AMERICAN INTELLIGENCE JOURNAL

THE MAGAZINE FOR INTELLIGENCE PROFESSIONALS

Intelligence Community Leadership: The Next Generation

NMIF

Vol. 37, No. 1, 2020

American Intelligence Journal

THE MAGAZINE FOR INTELLIGENCE PROFESSIONALS

Vol. 37, No. 1 *2020* ISSN 0883-072X

NMIF Board of Directors

LTG (USA, Ret) Mary A. Legere, Chair
Col (USAF, Ret) John R. Clark, President
Col (USAF, Ret) William R. Arnold, Vice President
Col (USAF, Ret) Michael Grebb, Treasurer

Ms. Natalie Anderson, Director
LTC (USAR, Ret) Christopher E. Bailey, SJD, Director
Col (USAF, Ret) Carla Bass, Director
CDR (USCG, Ret) Michael Bennett, Director
Mr. Don Bolser, Director
CDR (USNR, Ret) Calland Carnes, Director
SMSgt (USAFR) Kori L. Conoway
Mr. Dennis DeMolet, Director
LTC (USA, Ret) Ken Diller, Director
Lt Col (USAF, Ret) James Eden, Director
COL (USA, Ret) Sharon Hamilton, Director
COL (USA, Ret) David Hale, Director
LTC (USA, Ret) Steve Iwicki, Director
Mr. Bradley P. Moss, Esq., Director
CAPT (USNR) Rick Myllenbeck, Director
CW3 (USA, Ret) Todd Robinson, Director
Mr. (USSS, Ret) Robert A. Smith, Director
CDR (USNR) Louis Tucker, Director

Editor - COL (USA, Ret) William C. Spracher, Ed.D.
Production Manager - Ms. Debra Hamby-Davis

Brig Gen (USAF, Ret) Scott Bethel, Director Emeritus
MajGen (USMC, Ret) Michael Ennis, Director Emeritus
COL (USA, Ret) Michael Ferguson, Director Emeritus
Dr. Forrest R. Frank, Director Emeritus
Col (USAF, Ret) Owen Greenblatt, Director Emeritus
LTG (USA, Ret) Patrick M. Hughes, Director Emeritus
Col (USAF, Ret) William Huntington, Director Emeritus
COL (USA, Ret) Gerald York, Director Emeritus

The *American Intelligence Journal* (*AIJ*) is published by the National Military Intelligence Foundation (NMIF), a non-profit, non-political foundation supporting American intelligence professionals and the U.S. Intelligence Community, primarily through educational means. NMIF believes in the power of the intelligence mission to inspire young people to join the intelligence profession as a career of service to the nation. NMIF continuously engages current and future intelligence professionals, organizations, industry, and academic institutions to contribute to the overall sustainment of the U.S. military intelligence workforce.

Authors interested in submitting an article to the *Journal* are encouraged to send an inquiry—with a short summary of the text—to the Editor by e-mail at <aijeditor@nmif.org>. Articles and inquiries may also be submitted in hard copy to Editor, c/o NMIF, 256 Morris Creek Road, Cullen, Virginia 23934. Comments, suggestions, and observations on the editorial content of the *Journal* are welcomed. Questions concerning subscriptions, advertising, and distribution should be directed to the Production Manager at <admin@nmif.org>.

The *American Intelligence Journal* is published semi-annually. Each issue runs 100-200 pages and is distributed to key government officials, members of Congress and their staffs, and university professors and libraries, as well as to NMIF associates, *Journal* subscribers, and contributors. Contributors include Intelligence Community leaders and professionals as well as academicians, research fellows, students, and others with interesting and informative perspectives.

Copyright NMIF. Reprinting and copying by permission only.

AMERICAN INTELLIGENCE JOURNAL

Table of Contents

President's Message 1

Editor's Desk 3

In Memoriam..

Remembering David Moore: An Intellectual and Intelligence Teacher Extraordinaire
by LTC (USA, Ret) William A. Parquette 5

Hidden Warriors: The Effect of Espionage in Waging the Cold War
by Dr. Diana C. Gill 7

From China with Love? Analyzing the PRC's Shift to a "Foreign-Directed" Intelligence Collection Model
by Jimmy Z. Zhang 11

Assessment of Analytical Models Used within the Cox Report – People's Republic of China
by Robert Budahl 25

Examining Narratives on Chinese Strategic Ambitions
by MAJ (USA) Alex F. Oliver 30

The Paradox of Asymmetric Deterrence
by Samuel S. Chi 36

Improving Sources and Methods by Training Ethnic Slavs
by Mason C. Shuya 44

Russian Cyber Campaigns in Support of Military Operations
by John E. Arthur VI 49

Intelligence Reform: The Need for Empowerment of the Director of National Intelligence
by Kimbra L. Fishel 54

Operation MERKUR and the Battle for Maleme: Allied Failures in Intelligence
by Daniel L. Harris 62

Venezuela: A Case Study of Iran's Grand Strategy to Penetrate Latin America and the U.S. Response
by Dr. Magdalena Defort 73

Homeland Security: Advancing Intelligence-Led Policing in Confronting Jihadi-Salafism
by Bruno Brkic 80

Weaponizing Space: It Was Just a Matter of Time
by Lt Col (USAF, Ret) James J. Rooney 87

The Strategic Intelligence Implications of Circular Causality
by Jordan R. Beauregard 98

A Brief History of Cyber Intelligence: How Did Computer Data Evolve to Be Used for Intelligence Operations?
by Gueorgui Dimitrov 107

A New Hub for American Climate Security: Strengthening the Intelligence Community's Role in Meeting the Threat of Climate Change
by Diego H. Nuñez 115

Uncertainty Is What You Make of It: How It Affects Conflict and Perception in Intelligence
by Javier Martínez Mendoza 124

Russian Influence in Austria and Its Impact on the European Union
by Julia Girardi 133

AMERICAN INTELLIGENCE JOURNAL

Table of Contents *(Continued)*

Non-Democracies Prone to All Forms of Terrorism
by Sara Harmouch 146

Is the Coronavirus an Intelligence Failure? Lessons Learned for Intelligence Analysts in Pandemic
by Olivia M. Shumaker 154

From CIA to C(AI): Using Artificial Intelligence as a Shield and Sword in Cyberespionage
by Roman Kolodii 160

Window Dressing: Applying the RASCLS Framework in Foreign Policy
by Mason D. Goad 170

The Historical Evolution of Israeli Intelligence
by Admir Barucija 178

Understanding the Gray Zone: How Federal Law Enforcement Agencies Can Support SOF Operations Related to Counterterrorism Strategy
by Carvent L. Webb II 183

An Emerging Phenomenon: Private Military and Security Companies in Latin America
by SFC (USA) Sebastian Moreno 190

Porter's Four Corners: An Argument for Counterterrorism Analysis Utility
by Brianna Alverson 193

The Dilemma Between Morality and Intelligence Efficiency in the United States
by Tanguy Osman 197

In My View...

Seeking Help Is a Sign of Strength: Suicide Prevention within the Military
by Megan E. Connell-Cox 201

Profiles in Intelligence...

An Intelligence Community Leader: General Vernon Walters
by MSgt (USAF) Zachary S. McNair 206

The Transformational Leadership Approach of CIA Director John Brennan
by M. John Bustria 209

Counterintelligence Assessment of Jeffrey M. Carney, U.S. Air Force
by Lee E. Taylor II 213

NMIF Bookshelf

John William Davis' *Around the Corner: Reflections on American Wars, Violence, Terrorism, and Hope*
reviewed by MSgt (USAF) C. William Strong 217

Jason Fagone's *The Woman Who Smashed Codes*
reviewed by Avery G. Agostinelli 218

John E. Douglas' *Mindhunter: Inside the FBI's Elite Serial Crime Unit*
reviewed by Laurelyn Ostrowidski 219

Gino LaPaglia's *The Cultural Roots of Strategic Intelligence*
reviewed by Daniel P. Rich 221

Patricia O'Toole's *The Moralist: Woodrow Wilson and the World He Made*
reviewed by David A. Brock 222

Nikolaus Ritter's *Cover Name: Dr. Rantzau*
reviewed by MAJ (USA) Jeanette Chavez 224

The opinions expressed in these articles are those of the authors alone. They do not reflect the official position of the U.S. government, nor that of the National Military Intelligence Foundation, nor that of the organizations where the authors are employed.

President's Message

This volume of the *American Intelligence Journal* is the result of a labor of love—to dedicate a volume to student articles from across a broad array of students, subjects, countries, and universities. Vol. 37, No. 1, 2020, "Intelligence Community Leadership: The Next Generation," is primarily devoted to these articles. It is a multi-level task that requires a highly motivated student, an interested university professor, and an increased workload for the *AIJ* Editor. However, Dr. Bill Spracher and others transformed this dream into a concept, then planned the multiple inputs required, and now, finally—finished! As Dr. Spracher recounts in his "Editor's Desk," the idea goes back to David Moore, and their idea was embraced by the NMIF Board of Directors. Unfortunately, Mr. Moore has passed, but Dr. Spracher pursued the dream, and the results are one of the most diverse, informative, and interesting volumes of the *American Intelligence Journal* ever published.

The backstory of the *AIJ* "Student Volume" is NMIF support for intelligence and national security students through mentoring, publications, and scholarships. Years ago, the primary intelligence analysts were military, or former military. In fact, in the early 1980s about 80% of national intelligence agency personnel were military, and only about 20% civilian (to include former military). Now, the percentages are reversed, and the national agencies actively recruit college students. However, for students, the process for joining national agencies and other intelligence organizations can be very intimidating. To help prepare students, many universities now offer intelligence or national security curricula. Yet, there is a glitch in the form of a background investigation to obtain a national-level clearance, and the often extended time it takes to obtain the clearance. Many students must start work immediately and cannot afford the delay to obtain a clearance. Given these potholes, NMIF decided to assist students with opportunities to become published writers in a recognized, periodically published intelligence journal; hence, the *AIJ* student-only volume was born. This process equips students with the experience of thorough research of a selected intelligence topic or event, organizing the various aspects of the topic, and finally writing the article in accordance with the *AIJ* "Author's Guidelines." All agencies or organizations have similar processes, with internal variations. It is a rigorous task, but the students learn the process and become published authors, adding to their skillsets and their resumes.

Bringing the *AIJ* "Student Volume" to life has been an ongoing effort for several years, and student articles have been accepted previously, but this is the first *Journal* volume dedicated totally to students. As Dr. Spracher mentions in his "Editor's Desk," there are more than 20 universities involved with these articles, and at least 10 separate countries which the authors call home or are currently located in for their studies. To also assist the students achieve their goals, NMIF provides additional information to help guide them through the hiring process. Our congratulations to the students, their professors, and the universities for these fascinating articles! The number is amazing and the breadth of the topics is impressive, as are the articles themselves. Dr. Spracher and Dr. Bailey in their "Editor's Desk" comments provide more information on the development of this special volume. In addition, NMIF annually presents the Sherman Kent Award to the National War College student with the best paper. Although it takes a rewrite to fit the paper into the *American Intelligence Journal*, and also a release from the NWC and the student's parent organization, the last two winners of the Sherman Kent Award have had their papers selected for publication in the *American Intelligence Journal*, and a few others in past years too.

This year the National Military Intelligence Foundation has experienced many changes due to the COVID-19 pandemic. These restrictions led to many events and deadlines being postponed or cancelled. However, the core missions of NMIF continue, albeit on different timelines and form. Because of these new schedules, NMIF continued its core areas of support by proceeding with the national awards process and the NMIF 2020-21 Scholarships. In the past year, the *American Intelligence Journal* issues addressing HUMINT and MASINT have been published and the "Student Volume" finished. The unplanned delays allowed NMIF to add some details to its agenda for 2020 and institute some changes. The national awards for the Intelligence Community are now being finalized, and the 2020-21 NMIF Scholarships are in the final stage of selection and notification. Due to pandemic restrictions, the 2020 NMIF Awards Banquet was delayed twice, and finally transitioned to an upcoming virtual "Night of Heroes."

When it became quite obvious that the May 17, 2020, NMIF Awards Banquet would be impractical due to COVID-19 restrictions, it was postponed until October 18. However, the awards had to be presented in the early summer time

frame to reach all awardees before normal summer rotations. The national recognition at the Awards Banquet needed to be made, as these annual awards are timed to performance reviews, rotational assignments, and moves of government and service personnel. Therefore, NMIF worked with the national organizations and their staffs to identify award winners and plan for an internal, small recognition event at each organization. NMIF would proceed with preparing the plaques and citations, and the awards could be made within the restrictions. A second postponement of the Awards Banquet led to the decision to make it a virtual celebration of the top intelligence performers and their contributions. The planning for the NMIF "Night of Heroes" is continuing; it will be a virtual event to recognize the award winners, their organizations, and their contributions to intelligence careers. The timing will be in the fall, and the event will be held within the guidelines of COVID-19 restrictions. Planning information will be posted on the nmif.org website once finalized.

For the NMIF Scholarships, the student applications were being delayed by disruptions to academic schedules as universities shut down during their spring programs. In addition, student transcripts are normally submitted with applications to verify scholastic achievement, but the reduced manning at universities delayed applications even more. Consequently, because it was impossible to maintain the May award date, NMIF relaxed the deadline by over a month to allow for more applications. The NMIF Scholarship Committee then re-sent requests for student applications to the previous 40 universities, plus some additional ones. With the delay and additional prodding, the number of applications increased to 65, a record for the NMIF Scholarship Program. Three teams reviewed and evaluated applications, and another group did a down-select to the finalists. Another review by the Scholarship Committee was performed, and then 11 scholarships were proposed, which the NMIF Board approved. The NMIF 2020-21 Scholarships represent a total of $25,000 in awards. The NMIF Scholarships include the LTG James Williams Scholarship, three Col Bob Fectau Scholarships, one Col Scott St. Cyr Scholarship, two SOSi Scholarships, and four NMIF Scholarships. Because NMIF is an IRS Code 501(c)(3) charity, virtually any donation to the scholarship fund passes directly to the awardees—there is only one paid position at NMIF, and the administrative expenses come out of the general operating fund.

We are very appreciative of our donors and supporters. It has been an extremely challenging year for everyone, but especially for students. We will post updates on planning for events on the NMIF website as soon as timing matures. This particular issue of *American Intelligence Journal* is a quality statement to the talent and dedication of our intelligence and national security students. At NMIF, we often talk about the multi-generational aspect of our former "Intelligence Heroes," and the new generation of intelligence practitioners. From our vantage point, we will be in good hands!

John R. Clark

NMIF Corporate Partners

SOSi
CHALLENGE ACCEPTED

AMU

The Editor's Desk

Welcome to the Spring 2020 issue of *AIJ*. Even though spring is now over, and summer is flying by without our typical, close-knit family vacations to crowded places, given the crazy pandemic situation with which we're all coping it's difficult to track the seasons, the months, and the weeks. When one spends a good deal of time at home staring at the same walls, it's often a challenge even to remember what day it is!

Long before we knew what unique obstacles we would be facing this year, we made a decision to dedicate the first of two issues of the *Journal* to highlighting the work of students. As you will read in the memorial article about David Moore, producing such a special edition was the brainchild of this dearly departed colleague and frequent *AIJ* contributor, who passed away unexpectedly long before his time. Therefore, we commemorate David's legacy with this collection of thinkpieces by the best and brightest our schools have to offer. I intended to co-edit this edition with David, but the good Lord had other plans for him. Instead, I've called on fellow NMIF board member and NIU teaching colleague Dr. Christopher Bailey to stand in for David. Chris previously served the same role for an issue we put out on "Intelligence Leadership and Ethics" (Vol. 33, No. 1, 2016). He was indispensable this time around in recruiting several of the student authors and doing some editing of their work. I've asked Chris to say a little more about that at the end of this column.

This is the first issue of *AIJ* since we first began focusing on specific themes in 2011 in which the title on the cover refers to the writers inside and not to the topics being written about. After perusing many of the drafts submitted, I'm more convinced than ever that the future of the IC and its emerging leadership is in good hands. I was initially unsure I would be able to obtain enough solid articles to fill up a volume, as we normally do, but my fears were unfounded. The manuscripts came pouring in, and word of mouth from faculty to students and from students to fellow students obviously paid off. Perhaps being restricted to their homes and having to take classes virtually gave them more time to think and write! I'm also delighted and proud of the fact that, of the 65 NMIF scholarship applicants this year, three of them also published articles in this volume, and one of the three was a winner. That's not surprising; highly motivated students seek out all the benefits that come their way!

My admittedly unofficial count indicates that approximately 20 schools are represented in the pages of this issue, and not all of them in the United States. I always push to attract international scholars, and this issue was no different. I'm proud to say we have authors who hail from such diverse countries as Belgium, Bosnia and Herzegovina, Bulgaria, China, Lebanon, Mexico, the Philippines, Poland, Ukraine, and the United Kingdom, and attend schools in even more countries. All the authors and reviewers except one are students. I made an exception only for the author of the memorial piece devoted to Mr. Moore, Bill Parquette, a Penn State faculty member who for several years taught across the hall from me at the old site of what was then the Joint Military Intelligence College, later National Defense Intelligence College, and now NIU. David was one of Bill's students and a close friend. Both Bill and David were masters of denial and deception, and both were key in the issue of *AIJ* we did on that theme several years ago. In fact, David served as my co-editor (Vol. 32, No. 2, 2015).

Because the timeline to get an article drafted, submitted, approved, copy-edited, laid out, and published can extend for months, sometimes years, I knew that by the time this issue hit the street some of the authors would have graduated and no longer technically be students. Therefore, I arbitrarily made a rule that, as long as they produced their original handiwork while a student, they would be eligible. Many are still students, a few wrote as undergraduates and are now graduate students at other schools, and several recently graduated in 2019-20. Quite a few of the articles, as you might expect, are academic papers which were converted into articles. I always tell my students at NIU that's a great way to break into becoming a published author, i.e., take something they've already written for a course and turn it into an interesting journal article. That's what I did myself while in graduate school back in the late 1970s. For others, particularly undergraduates, I suggest getting their feet wet by first writing a book review and then, once they get the hang of it, moving on to feature articles. Many of the young people in the following pages have taken that advice well. I must confess some of them are not as young as you might think. Nowadays, we are blessed with an abundant crop of what I like to call "adult learners." We have them well represented in these pages too. A couple

already had "Dr." in front of their names before becoming master's students again. Now that takes real dedication to lifelong learning!

Sometimes in past Editor's Desks I would tick off the articles one by one and give a short snippet of their content. Because of the inordinate number of articles in this issue, and the diversity of their subject matter, I've decided to pass on that exercise and just let the reader leaf through the pages to see what's inside. As always, I'm pleased that some of the more contentious hotspots in the world are explored, such as China, Russia, Iran, Venezuela, and Syria. Many of the disparate fields of intelligence are also well covered, such as espionage, cyber, artificial intelligence (nice intro to the theme of our Fall 2020 issue), homeland security, climate security, space, intelligence reform, counterterrorism, ethics and morality, and a couple of historical pieces. One article in particular is very timely given the current #1 preoccupation of the entire world, COVID-19, and questions as to whether its infectious spread was an intelligence failure. I think we also broke the record, at least on my editorial watch, with three offerings in the "Profiles in Intelligence" section. The lone entry for the "In My View" section doesn't deal with intelligence per se, but it does sensitively discuss a problem all military units are coping with these days—rampant suicide—which is now increasingly affecting our police forces and other first responders who have been overtaxed with responses to the pandemic and protest activities in recent months.

I will quickly list board-approved themes for upcoming issues of *AIJ*, and encourage you readers to get on the bandwagon and contribute, before turning the pen over to Chris to say a few words:

Fall 2020 – "Artificial Intelligence: Ramifications for Collection and Analysis" (due 15 Oct)
Spring 2021 – "Law Enforcement Intelligence and Homeland Security" (due 15 Apr)
Fall 2021 – "Countering Transnational Threats" (due 15 Oct)

Feel free to tackle these themes or, if you prefer, just write on anything at all related to intelligence or international/national security and we'll give it strong consideration. Thank you for supporting your *Journal*, for cheering on the students we showcase in the following pages, and for championing the future of intelligence in general and military intelligence in particular.

Now, Chris, over to you. . .

NIU has teamed up with several local universities over the past two years to form an Intelligence Studies Consortium (ICS), as an informal, collaborative effort among educational institutions involved in intelligence education. In general terms, we have defined our purpose as promoting intelligence research and publication by students and faculty, as well as facilitating outreach and engagement among institutions with similar goals. On April 25, 2019, the ICS successfully conducted its first student-oriented symposium at Marymount University in Arlington, Virginia. The inaugural symposium, hosted by Marymount and sponsored by the Intelligence and National Security Alliance (INSA), offered each university the opportunity to present its expertise and distinctive contributions in topics such as terrorism, social computing, cyber, analysis, and policy issues of governance and accountability. We then began planning for a second symposium that would also feature student research, this time to be hosted by Georgetown University on April 16, 2020, but—like so many other things over the past several months—that event had to be cancelled because of the COVID-19 shutdown. Fortunately, many of the students who had been preparing for the 2020 symposium have been able to submit their materials for publication and some applied for NMIF scholarships. We take great pleasure in supporting student research and publishing through the *AIJ*, and a sampling of that work is represented here in this edition.

Dr. Bill Spracher
Dr. Chris Bailey

Interested in publishing an article in the *American Intelligence Journal*?

Submit a manuscript for consideration to the editor
<aijeditor@nmif.org>

Remembering David Moore: An Intellectual and Intelligence Teacher Extraordinaire

by LTC (USA, Ret) William A. Parquette

David Moore as a young professional, circa 1970s

I first met David Moore when he became a student in the Denial and Deception Advanced Studies Program (DDASP) at the National Intelligence University (NIU). The DDASP was a graduate certificate program sponsored by the Foreign Denial and Deception Committee (FDDC) of the National Intelligence Council (NIC) and I was its course director. David's biography says he was a senior intelligence professional and educator at the National Security Agency, the Central Intelligence Agency, the National Geospatial-Intelligence Agency, and the Office of the Director of National Intelligence. He was much more. He was the author of two groundbreaking books published by the then-National Defense Intelligence College Press (now NI Press), *Critical Thinking and Intelligence Analysis* and *Sensemaking: A Structure for an Intelligence Revolution*. He was also the author or co-author of a number of scholarly journal articles. He graduated from Washington and Lee University and the Joint Military Intelligence College (now National Intelligence University).

Once David graduated from the DDASP, we brought him back to lecture and contribute throughout the years. He was at his best when interacting with students and was always eager to mentor master's thesis students. David made a significant contribution to the D&D community by volunteering to co-edit a volume of the *American Intelligence Journal* dedicated to the theme "Denial and Deception." He wrote an excellent article in that volume and contributed several other thought-provoking pieces to *AIJ* over the years.

Always the educator, he worked with the editor of *AIJ*, Bill Spracher, to develop a special student-only issue, which David volunteered to co-edit. Not only did he conceive this edition but he recruited some of the contributing authors.

David defined "sensemaking," whereby intelligence professionals would work with executive decision-makers to explain data that are "sparse, noisy, and uncertain," requiring an interpreter and experienced champion to bring about a practicable understanding and acceptance of the concept among intelligence practitioners. David Moore ably accomplished that feat.

Mark Lowenthal, in his foreword to David's monograph *Critical Thinking and Intelligence Analysis*, wrote, "In addition to his duties as an intelligence officer at the National Security Agency, David Moore has devoted many fruitful hours to the intellectual underpinnings of intelligence, especially to what makes analysts and what makes better analysts." Intelligence officers are engaged in an intellectual pursuit. They are trying to solve puzzles, resolve uncertainties, and discover the nature and meaning of things that others would keep secret. They must have the tools to help them identify the problem, and to assess what is known and what is unknown. David spent his professional life trying to make the analyst's environment easier.

Stephen Marrin, in an article for the journal *Intelligence and National Security*, wrote about the creation of intelligence centers. Titled "Intelligence Studies Centers: Making Scholarship on Intelligence Analysis Useful," Steve states, "Intelligence analysis involves the interpretation of information about the adversary or environment for purposes of assisting decision-making.

There are many different kinds of intelligence analysts in many different domains, from civilian national security to military to law enforcement and to business." Intelligence analysis as a professional discipline has practitioners across the entire world, some of whom join professional intelligence analysis-related associations and explore the nature of the discipline in conferences and workshops, contribute to the growing dedicated literature on intelligence analysis, and even take college and university courses dedicated exclusively to exploring the nature and practice of intelligence analysis. This is where David Moore thrived; this was his environment.

David exercising in his kayak, circa 2000s

In the last few years after I became the deputy, then chairman, of the FDDC, David would call about once a week to chat and wanted to engage in many different activities. I would call them his "what abouts." He would ask what about this or that. I miss his calls and would love to chat about this or that again.

David Moore's significant contributions to the fields of intelligence analysis and denial & deception will be felt for many years.

[Editor's Note: I first got to know David well through the International Association for Intelligence Education (IAFIE), though I already knew his reputation through his periodic interactions with JMIC's (later NDIC and NIU) Center for Strategic Intelligence Research/JMIC Press, where I first worked as an editor over 16 years ago. David was a stimulating conversation partner, as Bill Parquette notes, always asking those contentious "what about?" or "what if?" questions to get others' blood flowing. Copies of his first book on critical thinking were distributed gratis to all attendees of the first-ever IAFIE conference. David never earned a dime from that book or his second one on sensemaking, as they were U.S. government publications free for anyone to read and use, whether inside or outside the Beltway. Without David's prompting me over the phone while at a conference at his alma mater surrounded by students, this special issue of *AIJ* would never have been realized. I was counting on having David's astute editing of these articles, and recruiting even more authors, as he had done a few years ago for the issue that explored the fascinating subject of D&D. His physical presence is sorely missed today, and always will be, but thankfully his spirit is still with us every step of the way.]

David relaxing as a seasoned veteran of the Intelligence Community, circa 2010s

LTC (USA, Ret) William A. Parquette is an Assistant Teaching Professor in the College of Information Science and Technology (IST), The Pennsylvania State University. He is the former Chairman of the Foreign Denial and Deception Committee (FDDC) of the National Intelligence Council (NIC), which is under the Office of the Director of National Intelligence (ODNI). Bill served with the FDDC for 17 years and prior to that was an active duty Army officer with the Field Artillery for 22 years. He has worked in the Denial and Deception discipline for 23 years.

Hidden Warriors:
The Effect of Espionage in Waging the Cold War

by Dr. Diana C. Gill

On February 22, 1946, an American *charge d'affaires*, stationed in Moscow, sent an extraordinary telegram to the U.S. Department of State. Known as the "Long Telegram," George Kennan's document analyzed the Soviet ethos which dictated "that with the US there can be no permanent *modus vivendi* [and that the USSR believed it]…desirable and necessary that the internal harmony of our society be disrupted, our traditional way of life be destroyed, the international authority of our state be broken, if Soviet power is to be secure."[1]

Kennan's analysis of the USSR as being anti-American was later codified as the basis for both the Truman Doctrine and the U.S. policy of communist containment.

Kennan was doubtless influenced by the Soviet Premier's speech less than two weeks before. At the opening of the Soviet Party Congress on February 9, Joseph Stalin blamed World War II on "present day monopolistic capitalism" whose nature tended to result in "catastrophic wars." Kennan's analysis of the USSR as being anti-American was later codified as the basis for both the Truman Doctrine and the U.S. policy of communist containment. The "Long Telegram" also served as a symbol of the ideological divide between the two superpowers; their political antipathy quickly spawned open hostility with the proliferation of atomic bombs, weapons that neither dared to use in a hot conflict. To defuse fears of the other, each created or retooled national intelligence agencies to "gather information about threats, whether external or internal, and to warn leaders about perils facing the homeland."[2]

This article examines how espionage, as a subset of such national intelligence, became a force multiplier in the Cold War dynamic, helping to direct its course while gathering relevant data. Espionage's influence was both direct and oblique. It was direct when operatives, singly or collectively, furnished "game-changing" information directly to policymakers. It was oblique in how the presence of spies contributed to the era's heightened tension via moral panic, and in how spies could provoke an aggressive, almost primal, response more expected in a central war.

DIRECT EFFECT BY HUMAN OPERATIVES

Up until the explosion of surveillance technology post-Sputnik, espionage stood as the preeminent form of state-run covert intelligence, its only competition being SIGINT (signals intelligence) initiated in the electronic form as early as the Second Boer War.[3] Conversely, espionage, using spies, was part of HUMINT (human intelligence) whose principal purpose was to reduce the likelihood of being "Pearl Harbored" or subjected to a surprise attack. Today, HUMINT competes within a "technophilic"[4] intelligence environment; other forms of intelligence include geospatial intelligence, imagery intelligence, measurement and signature intelligence, open source intelligence gathered from publicly available sources, and finally the modern-day version of SIGINT. In the early Cold War, however, it was largely espionage that provided Cold War leaders with knowledge of an opponent's strengths, weaknesses, and predilections, informing government leaders as to how to navigate a political environment in which they were making critical policy decisions concerning that opponent.

At its best, HUMINT gave policymakers what the future of surveillance technology could not. Richard Helms, a former CIA Director, spoke in support of human intelligence gathering when he stated during the Persian Gulf crisis that a satellite surveillance picture is "nice to have… But it doesn't tell you what's inside Hussein's head. It doesn't tell you what he is going to do… Even though you photograph [something] and can make some assessments from the photographs, that isn't the final word that you want."[5]

Cold War spies provided policymakers knowledge of an opponent's personal/political vulnerabilities, new technology, and military capacity. Their intelligence was

often, however, subject to political exploitation. U.S. policymakers frequently "manipulated…intelligence to reflect policy preferences,"[6] such as when the National Security Advisor, Henry Kissinger, who needed Congress to approve a large-scale anti-ballistic missile system to give Nixon a bargaining chip with the Soviets, backed the CIA into a corner with the 1969 debate over whether the SS-9 missile silo was a MRV or a MIRV.[7]

Espionage was also a slow investment. Gaining entrée into foreign governments was difficult for operatives to obtain. Consequently, American intelligence largely used "trusted locals…whether a lofty prime minister who may have been recruited to the U.S. espionage cause while a young student enrolled in an American university (won over with secret monthly financial stipends—beer money—and, later, by a growing dependence on secret payments); a prime minister's aide, mistress, or chauffeur; a diplomat; an intelligence officer; a colonel or, better yet, a general; a terrorist operative—anyone who might be able to put his or her hands on documents relevant to America's interests or attend a meeting in which schemes detrimental to the United States are being hatched."[8]

The Soviet use of sleeper agents or illegals showed even greater patience as Communist agents were inserted into American society to spend decades before they might acquire actionable intelligence.

Putting "the right guys in place" could take case officers years to arrange, however, and even then no substantive information might be forthcoming. The Soviet use of sleeper agents or illegals showed even greater patience as Communist agents were inserted into American society to spend decades before they might acquire actionable intelligence. Nevertheless, a select number of Cold War agents did prove the rule that "the right guy" in the right place could prove critical. Examples included Klaus Fuchs, a German physicist turned British citizen on the Manhattan Project, who secretly transmitted technical information to the Soviets that fast-tracked their own construction of an atomic bomb in 1949.[9]

Then there was Oleg Penkovsky, a double agent for the CIA who worked high up in the GRU (the military intelligence directorate of the Soviet Army General Staff of the Soviet Union 1918-1992). He personally kept the Cold War from going hot in 1962 over the Cuban missile crisis by providing the United States insight into Soviet medium-range ballistic missile capabilities which leveraged U.S. demands for their removal.[10]

Soviet aviation specialist Adolf Tolkachev, disillusioned by the "impassable, hypocritical demagoguery"[11] of the USSR, also provided the CIA top secret intelligence from 1979 to 1985. Smuggling to the West blueprints and circuit boards from his job at Phazotron, a Soviet radar design agency, Tolkachev's "product" (the raw data he transmitted that were evaluated and validated by the CIA) gave Israel an advantage over Palestine with its air force of Soviet-made planes[12] and saved the U.S. military "billions of dollars and up to five years of R&D time."[13] (Historian John Prados argues that stolen technology often affected Cold War tactics in "counter[ing] the enemy,"[14] citing U.S. procurement of Soviet tank improvements and new aircraft systems such as the FB-111, B-1, and next-generation stealth technology.[15])

Colonel Oleg Gordievsky, a disaffected KGB double agent for the British Secret Intelligence Service, was another operative who kept the Cold War from going hot. When in 1983, amid heightened tensions between the East and the West, a NATO command post exercise—code-named ABEL ARCHER 83—was initiated, the Soviet Union interpreted the exercise's heightened realism as camouflage for launching an actual attack on the USSR. Gordievsky provided his British contacts documented proof that the Russians were planning an armed response to the perceived threat.[16] Alerted then by the UK, which believed the threat to be genuine,[17] NATO amended the exercise to reduce its realism and thereby its appearance of menacing the Soviet Union.

Less dramatic, but no less influential to the course of the Cold War, were agents such as Miles Copeland, Jr., working for the Western Bloc under the hegemony of the United States and Larry Wu-tai Chin for the Eastern Bloc under the hegemony of the USSR. Copeland was credited with arranging the coup against Mohammad Mossadegh, the Prime Minister of Iran, in 1953, while Chin, a CIA agent working secretly for China, allegedly prolonged the Korean War through his job as interrogation translator of captured Chinese prisoners.[18] Later, as a case officer at CIA Headquarters, Chin influenced diplomacy between China and the U.S. by telling the former of Nixon's plans to pursue normalization.[19]

INDIRECT EFFECTS OF THE ENEMY WITHIN

Cold War goals for espionage were to gather enough information about an enemy to further national objectives. However, espionage had an unexpected by-product: a psycho-social effect, transforming it into a "secret war…fought in the mind."[20] By inserting spies into a hostile superpower, intelligence agencies effectively destabilized that superpower by challenging its sovereignty,[21] sparking, in many cases, bouts of "spy

mania"[22] or moral panic, a "quasi-collective psychosis,"[23] defined as "a form of collective behavior…sustained by many collective behavior processes: rumor, gossip, collective delusion, mass hysteria, [and] the conveyance of contemporary or urban legends."[24]

This was especially true of the United States, whose open society made it an easy espionage target. Fears of communists hiding literally next door triggered two major "Red Scares" in the United States, the first in 1919-1920, the second in 1946-1954 (the latter reputedly costing 10,000 to 12,000 Americans their jobs[25]). Robert Goldstein argues that between these two dates there were several "little" Red panics (with harbingers of McCarthyism on the horizon) that made the two major dates more a continuum of anxiety rather than discrete stops.[26] This dread of the enemy "other" (fed by such convicted Soviet spies as Ethel and Julius Rosenberg, Alger Hiss, Klaus Fuchs, and Morton Sobell) amplified American anger and its eagerness to accelerate the Cold War's arms race.

Soviet hypersensitivity to Western spies led to the unjustified arrests of American tourists and journalists such as Nicholas Daniloff and eventually to the shooting down of Korean Air Lines 007 in 1983, killing 269 innocent civilians.

Similar concerns fueled Soviet aggression while being mediated by the KGB or the military directly. Beginning in 1941, the USSR tried to avoid enemy infiltration by closing many of its borders to foreign travel.[27] By the 1950s, though, when Khrushchev relaxed travel bans, foreign visitors numbered 56,000; by 1963, 168,000 visitors; and "[b]y the early 1970s, the Soviet Union was receiving 4 million travelers yearly."[28] This influx triggered KGB suspicions of "tourists" as possible "ideological spies…[and] blatant anticommunists."[29] Soviet hypersensitivity to Western spies led to the unjustified arrests of American tourists and journalists such as Nicholas Daniloff and eventually to the shooting down of Korean Air Lines 007 in 1983, killing 269 innocent civilians.[30]

Espionage's final influence on the course of the Cold War involves global changes triggered by the mere presence of its operatives rather than their intelligence gathering (for example, when the Partial Nuclear Test Ban Treaty was adopted in 1963, the Kremlin much preferred verification by satellite reconnaissance, even over Soviet territory, as opposed to having Western inspectors physically on-site.)[31] This animosity toward possible infiltrators, highlighted by the shooting down of KAL 007, shared similarities with NATO's 1999 bombing of the Chinese embassy in Serbia for allegedly transmitting by radio military intelligence to the forces of NATO's adversary, Slobodan Milosevic.

Cold War espionage saw the beginnings of aggressive, sometimes irrational, 20th century intelligence and counterintelligence efforts. One example was FBI Director J. Edgar Hoover, who spent years conducting fruitless "invasive surveillance operations"[32] against civil rights icon Martin Luther King, Jr., and his organization, the Southern Leadership Conference, to prove communist involvement. Operations against such imagined internal enemies consumed more and more government resources on both sides of the Cold War as, increasingly, each superpower felt less secure. At the disbanding of the KGB in 1991, General Karbainov, its press secretary, stated that the KGB's budget had eventually reached 4.9 billion rubles annually, which translated at the time to $8.3 billion.[33] Additionally, 50 percent of the Soviet Union's total industrial output was devoted to the military protecting its borders from Western access in the 1980s.[34] U.S. defense spending was equally uncompromising in protecting itself against what President Reagan labeled the "evil empire." The CIA's budget in 1963, a year after the Cuban Missile Crisis, had been $550 million.[35] By the time the USSR dissolved in 1991, the U.S. intelligence budget was estimated at $30 billion.[36]

Spying's final effect was then the Cold War's greatest irony. Adherents of either communism or democracy professed their system to be the highest form of forward-looking modern governance, with espionage meant to state objectives further through the reasoned collection of an adversary's capabilities/intentions, diplomatic vulnerabilities, and weapons innovations. In the end, though, it was also the primitive terror of hidden enemies that added to the rage propelling the Cold War, increasing military border protections and spiraling intelligence costs which led eventually to the Soviet Union's dismantlement and the United States' brief unipolar moment of security.

NOTES

[1] "Long Telegram," *National Security Archive*, https://nsarchive2.gwu.edu//coldwar/documents/episode-1/kennan.htm, accessed April 3, 2020.

[2] Loch Johnson, "Evaluating Humint: The Role of Foreign Agents in U.S. Security," *Journal of Comparative Strategy*, October 4, 2010, https://www.tandfonline.com/doi/abs/10.1080/01495933.2010.509635?src=recsys&journalCode=ucst20#metrics-content, accessed April 4, 2020.

[3] Nigel West, *Historical Dictionary of Signals Intelligence* (Metuchen, NJ: Scarecrow Press, 2012), xix.

[4] Kristie Macrakis, "Technophilic Hubris and Espionage Styles During the Cold War," *Isis: A Journal of the History of Science Society*, Volume 101, Number 2, June 2010, https://www.journals.uchicago.edu/doi/full/10.1086/653104, accessed March 20, 2020.

[5] Loch K. Johnson, *The Threat on the Horizon: An Insider's Account of America's Search for Security After the Cold War*, Oxford, UK: Oxford University Press, 2011, 196.
[6] Joshua Rovner, "Intelligence in the Age of Twitter," in *Handbook of Terrorism and Counter-Terrorism Post 9/11*, edited by David Martin Jones, Paul Schulte, Carl Ungerer, and M.L.R. Smith (Cheltenham, UK: Edward Elgar Publishing, 2019), 101.
[7] Ray Locker, "The Appalling Story of the Nixon Administration's Decision to Bully the CIA into Distorting Intelligence," *History News Network*, December 2015, https:// historynewsnetwork.org/article/161464, accessed April 10, 2020.
[8] Loch Johnson, "Evaluating Humint: The Role of Foreign Agents in U.S. Security," *Journal of Comparative Strategy*, October 4, 2010, https://www.tandfonline.com/doi/abs/10.1080/ 01495933.2010.509635?src=recsys& journalCode= ucst20#metrics-content, accessed April 4, 2020.
[9] "Klaus Fuchs," *FBI Records: The Vault,* https://vault.fbi.gov/ rosenberg-case/klaus-fuchs, accessed April 12, 2020.
[10] Jerrold L. Schechter, "A Very Important Spy," *New York Review of Books*, June 24, 1993, https://www.nybooks. com/ articles/1993/06/24/a-very-important-spy/, accessed March 20, 2020.
[11] David E. Hoffman, "What Made This Man Betray His Country?" *The Atlantic*, August 8, 2015, https://www. theatlantic.com/international/archive/2015/08/adolf-tolkachev-cia-kgb/400769/, accessed April 6, 2020.
[12] Daniel Chalyan, "The CIA Paid This Soviet Traitor Millions, but Got Billions in Return," *Russia Beyond*, February 4, 2019, https://www.rbth.com/history/329940-soviet-american-cia-kgb-spy, accessed March 31, 2020.
[13] Milton Barden and James Risen, *The Main Enemy: The Inside Story of the CIA's Final Showdown with the KGB* (Novato, CA: Presidio Press, 2004 reprint), 37.
[14] John Prados, "Certainties, Doubts, and Imponderables: Levels of Analysis in the Military Balance," *Intelligence and National Security*, December 20, 2011, https://www.tandfonline.com/doi/ abs/10.1080/02684527.2011.619797, accessed April 4, 2020.
[15] Ibid.
[16] Ofer Aderet, "How Double Agent Oleg Gordievsky Changed the Course of History," *Haaretz Magazine*, September 21, 2019, https://www.haaretz.com/world-news/.premium.MAGAZINE-the-double-game-of-oleg-gordievsky-1.786 6186, accessed March 30, 2020.
[17] Len Scott, "Intelligence and the Risk of Nuclear War: Able Archer-83 Revisited," *Intelligence and National Security, no. 6, 2011,* https://www.tandfonline.com/doi/abs/10.1080/ 02684527.2011.619796*, accessed April 9, 2020.*
[18] Glenn P. Hastedt. *Espionage: A Reference Handbook* (Santa Barbara, CA: ABC-CLIO, 2003), 89.
[19] "Chinese Spy Cases," GlobalSecurity.org, https:// www.globalsecurity.org/intell/world/china/mss-ops-cases.htm, accessed April 10, 2020.
[20] Emmanuel Debruyne, "Espionage," *International Encyclopedia of the First World War*, October 2014, https://encyclopedia.1914-1918-online.net/article/espionage, accessed April 12, 2020.
[21] Daniela L. Caglioti, "Aliens and Internal Enemies: Internment Practices, Economic Exclusion and Property Rights during the First World War," *Journal of Modern European History*, Vol. 12, No. 4 (2014), https://www.jstor.org /stable/26266152?read-now=1&refreqid=excelsior%3Ac898669cc407656d46d7f54bb874cf41& seq=1 #pagescantabcontents, accessed April 14, 2020.
[22] Ibid.
[23] Ibid.
[24] Erich Goode and Nachman Ben-Yehuda, *Moral Panics: The Social Construction of Deviance* (Hoboken, NJ: Wiley-Blackwell, 2009), 140.
[25] Thomas C. Reeves, "Are You Now…," *The New York Times*, June 14, 1998, https://www.nytimes.com/1998/06/14/ books/are-you-now.html, accessed April 2, 2020.
[26] Robert Justin Goldstein, ed., *Little "Red Scares": Anti-Communism and Political Repression in the United States, 1921 to 1946* (New York: Routledge, 2016).
[27] "Restrictions on Foreign Travel in the USSR: Assessing Recent Changes," 2012, CIA Website, https://www.cia. gov/library/ readingroom/docs/CIA-RDP07C00121R001000280001-8.pdf, accessed April 2, 2020.
[28] Alex Hazanov, "Porous Empire: Foreign Visitors and the Post-Stalin Soviet State," PhD diss., University of Pennsylvania, 2016.
[29] Ibid.
[30] Michael R. Gordon, "Ex-Soviet Pilot Still Insists KAL 007 Was Spying," *The New York Times*, December 9, 1996, https:// www.nytimes.com/1996/12/09/world/ex-soviet-pilot-still-insists-kal-007-was-spying.html, accessed April 6, 2020).
[31] Laurence Nardon, "Cold War Space Policy and Observation," *Astropolitics Journal*, August 2007, https://www. tandfonline.com/ doi/10.1080/14777620701509280, accessed April 13, 2020.
[32] Kristine Phillips, "In the Latest JFK Files: The FBI's Ugly Analysis on Martin Luther King, Jr.," *The Washington Post,* November 4, 2017, https://www.washingtonpost.com/news/ retropolis/wp/2017/11/04/in-the-latest-jfk-files-the-fbis-ugly-analysis-on-martin-luther-king-jr-filled-with-falsehoods/, accessed April 10, 2020.
[33] David Wise, "Closing Down the KGB," *The New York Times*, November 24, 1991, https://www.nytimes.com/ 1991/11/24/ magazine/closing-down-the-kgb.html, accessed April 10, 2020.
[34] Thayer Watkins, "The Economic Collapse of the Soviet Union," San Jose State University website, Department of Economics, http://www.sjsu.edu/faculty/watkins/sovietcollapse.htm, accessed April 9, 2020.
[35] "CIA Budget Revealed – 42 Years Late," *DefenseTech*, April 2005, https://www.military.com/defensetech /2005/04/05/cia-budget-revealed-42-years-late, accessed April 12, 2020.
[36] James Risen, "An Extraordinary Link for Archenemies in Spying," *The Los Angeles Times*, December 31, 1997, https:// www.latimes.com/archives/la-xpm-1997-dec-31-mn-3817-story.html, accessed April 4, 2020.

Dr. Diana Clark Gill is the author of How We Are Changed by War: A Study of Letters and Diaries from Colonial Conflicts to Operation Iraqi Freedom*, published by Routledge in 2010. Having written much of this treatise on war-related personal documents for her doctoral dissertation in English from the University of Mississippi, Gill unexpectedly found a new academic interest in military conflict, and is currently working on a third master's degree (the first and second being in Social Work and English) in War Studies at King's College, London.*

From China with Love?
Analyzing the PRC's Shift to a "Foreign-Directed" Intelligence Collection Model

by Jimmy Zhang

OVERVIEW

Based on an analysis of nine Chinese espionage cases uncovered between 2012 and 2019, this article argues that, since Xi Jinping assumed the Chinese leadership, the PRC's human intelligence (HUMINT) collection doctrine has begun to shift from an "adapted internal security" model to a "Western/Russian foreign-directed model." Chinese case officers are increasingly (1) using sophisticated intelligence collection tradecraft, (2) running or recruiting agents in third countries outside of China, (3) recruiting non-ethnically Chinese agents, and (4) targeting high-ranking and experienced recruits with direct sensitive information access or reliable contacts in foreign governments of interest. This article's findings have two main implications for U.S. national security and foreign policy. First, policymakers, analysts, and law enforcement officials should be open to interpreting Xi-era Chinese HUMINT operations the same way as professional Eastern Bloc operations during the Cold War when coordinating counterintelligence strategies and operations. Second, enhanced Chinese foreign intelligence operations may drain Chinese internal stability maintenance and surveillance capabilities, potentially leading to strategic opportunities for the United States.

INTRODUCTION

At the 19th Chinese Communist Party Congress, General Secretary Xi Jinping described China as a "great power" or "strong power" 26 times and repeatedly stressed the importance of modernizing the People's Liberation Army, expanding Chinese leadership in international affairs, and countering Western influence in East Asia.[1] While Deng Xiaoping's *taoguangyanghui* foreign policy during the 1990s suggested that China should "bide its time, keep a low profile, and never take leadership," Xi's statements clearly demonstrated that China has finished "biding its time," no longer needs to "hide its capabilities," and is ready to seize a leadership role on the world stage.[2] As China's economic influence, military power, and foreign interests continue to expand, Chinese leaders must rely more heavily on external intelligence capabilities to gain knowledge of enemy intentions, acquire advanced foreign technologies, and launch "offensive counterintelligence operations" to disrupt foreign intelligence efforts.[3]

Despite improved electronic and signals intelligence capabilities, most Chinese civilian and military intelligence agencies still specialize in human intelligence (HUMINT).[4] Writing in 2011, Peter Mattis argued that Chinese human intelligence collection largely operates under the "adapted internal security" model, but the "Western, foreign-directed intelligence approach may be the future of [Chinese] intelligence" due to increased demands from policymakers and expanding Chinese foreign interests.[5] However, we do not yet know whether Chinese HUMINT operations have shifted toward the "foreign-directed" model and to what extent since Xi Jinping assumed the Communist Party leadership in November 2012 with a platform focused on promoting Chinese political, economic, and military primacy.[6] This article aims to fill the above gaps in the literature.

I begin this article by describing three possible conceptual models for Chinese HUMINT operations: the "mosaic" or "grain of sand" model, the "Western/Russian foreign-directed model," and Mattis' "adapted internal security" model. Next, I provide an overview of major Chinese espionage cases from 1949 to 2011, arguing that Chinese services largely employed the "adapted internal security" intelligence collection model during this period. Then, using data from court documents, newspaper articles, and other media reports, I analyze nine recent Chinese espionage cases uncovered between 2012 and 2019: Kun Shan CHUN, Candice Marie Claiborne, Kevin Patrick Mallory, WANG Tsung-Wu, HSIEH Chia-Kang, XU Yanjun, Ron Hansen, Xuehua PENG, and the attempted recruitment of an *Asia Sentinel* journalist. I argue that, since 2012, Chinese services have been, at the very least, employing elements of the "foreign-directed" intelligence collection model much more often, and these recent cases and events may mark the beginning of a shift in the PRC's HUMINT operational style. I conclude by evaluating implications for the United States and suggesting several areas for further study.

This article relies solely on open source information from the United States, Taiwan, China, and several European countries, and does not analyze the full universe of Chinese espionage cases, many of which are still classified and/or under investigation. However, authorities in the United States, Europe, and Taiwan have successfully prosecuted the Chinese agents in all cases cited, demonstrating that the actors in each case committed espionage in violation of the laws of each target country. Indeed, most public, successfully prosecuted cases in the United States and other countries offer reliable information about Chinese intelligence operations because attorneys and law enforcement officers have carefully vetted the facts and allegations in each case and the defendants' charges have held up in court under stringent legal standards. However, supplementing this analysis with classified information could reveal additional insights into new and emerging forms of Chinese intelligence tradecraft that may further confirm (or falsify) some of the theories in this article.

The article does not evaluate economic espionage cases in which the defendant provided information to Chinese government or intelligence services by his or her free will (the FBI's strict definition of "non-traditional collector"). Although most economic cases still constitute espionage, for this article I am interested only in cases in which a government or judicial authority established that a Chinese intelligence service deliberately recruited, developed, and/or directed an individual to collect foreign intelligence, because proven recruitment links can more effectively shed light on the motivations and operational styles of Chinese intelligence services.

THREE POTENTIAL CHINESE APPROACHES TO INTELLIGENCE COLLECTION

The current literature describes three possible Chinese approaches to intelligence collection: the "mosaic" or "grain of sand" model, the "Western/Russian foreign-directed model," and Peter Mattis' "adapted internal security model (2011)."

The "grain of sand" model originates from a quote by former U.S. Ambassador James Lilley:

> If the Russians want to get certain sand from a beach that's special, they'll have a submarine come in at night. They'll put a crew infiltration. They'll get a bucket full of sand, and they'll take it back to the submarine and leave. The Chinese will have 500 people having picnics on the beach, each picking up the sand in a small can [or, each picking up a grain of sand], and bringing it back.[7]

Under the "grain of sand" model, Chinese intelligence largely concentrates on recruiting and cultivating ethnic Chinese sources overseas, often appealing to patriotism, a shared cultural identity, or threats against family members still in China.

"Grain of sand" adherents believe that China employs a vast number of "amateur collectors" overseas who gather bits of data without regard to a larger intelligence picture.[8] The collected data is often "low grade, if not entirely unclassified."[9] Chinese intelligence officers then attempt to reassemble the "grains of sand" into a larger picture back in China.[10] Under the "grain of sand" model, Chinese intelligence largely concentrates on recruiting and cultivating ethnic Chinese sources overseas, often appealing to patriotism, a shared cultural identity, or threats against family members still in China.[11] Finally, the "grain of sand" model posits that China "does not use intelligence tradecraft familiar to Western services," if it employs tradecraft at all.[12] As Peter Mattis explains, the "grain of sand" view assumes that "PRC intelligence services [do not regularly] pay agents for sensitive information, employ covert technical or personal communications methods, [or use] age-old tools like dead drops."[13]

The more familiar "Western/Russian foreign-directed approach" to intelligence collection largely "focuses on foreigners" and "seeks to influence foreign entities by means not attributable to the acting government."[14] Although Russian intelligence priorities may have historically differed from Western priorities, Herman argues that Western and Russian intelligence services share close links to policymaking and view decision-making support to policymakers as a critical component of their mission.[15] According to Mattis, if Chinese intelligence operations functioned under the "foreign-directed approach," we may see "methods designed to hide government sponsorship, closely directed intelligence operations with top-down controls," clandestine tradecraft, and bases of operations overseas.[16] However, most Chinese espionage cases up to 2011 relied on a domestic operational base and were "dominated by internal security" considerations.[17]

Mattis developed the "adapted internal security" model in 2011 to better explain Chinese intelligence operations, as the bulk of Chinese intelligence cases do not fit neatly into the "grain of sand" or "Western/Russian foreign-directed" models. In the adapted internal security approach, Chinese

intelligence services maintain a domestic base of operations for conducting surveillance on possible topics, and proceed to foreign intelligence collection and source development only if opportunities emerge.[18] In contrast to the Western/Russian recruitment cycle, Chinese surveillance primarily "examines threats to the state and Party," and does not prioritize "examining the suitability and access of a potential agent to provide information of foreign intelligence value."[19]

Although the PRC is focused more on "internal security affairs than policymaking," Mattis argues that "[Chinese] intelligence concepts and methods resemble [Western/Russian concepts and methods], with minor variations."[20] While PRC intelligence services can employ Western/Russian tradecraft and launch operations abroad, under the "adapted internal security" model, China would still focus on internal security as the end goal of every operation, and resource limitations may prohibit significant foreign expansion.[21] Mattis explains that "case officers based in the PRC, underdeveloped overseas operations, and surveillance efforts preceding source development" would indicate operations under the "adapted internal security" model.

CHINESE HUMINT OPERATIONS FROM 1949 TO 2011

From 1949 to 2011, Chinese HUMINT operations largely employed the "adapted internal security" model and elements of the "grain of sand" model. Most cases involved the recruitment of ethnically Chinese (or PRC minority) agents within China. Additionally, while Chinese case officers may have used surveillance and other forms of tradecraft within China to recruit principal agents, Chinese case officers have rarely trained these agents in operational tradecraft.

Prioritizing Relationships over Direct Information Access

Directed access operations, in which PRC intelligence services "identify and assess" potential agents in China who can access foreign government or intelligence organizations when they travel abroad, are a hallmark of the "adapted internal security" approach to intelligence collection.[22] Peter Mattis argues that the "quality of [agents recruited in China] would largely be beyond the control of Chinese intelligence services, and relate to the kinds of people attracted to China as a place to live, study, and work."[23] Indeed, Chinese case officers recruited agents from within Chinese territory in almost all cases from 1949 to 2011,[24] and almost never operated from an overseas base (e.g., Chinese embassies abroad).

Recruited assets have included retired, professional Taiwanese intelligence officers, Chinese students or businessmen about to travel abroad, and foreign students studying abroad in China with no intelligence experience. However, most of these recruits had one thing in common—they did not usually have direct access to foreign government or intelligence information at the time of their recruitment.[25] Mattis argues that government or intelligence officials with direct access are often difficult recruitment targets because they do not usually "have routine contact with PRC society."[26] Mattis concludes that PRC services appeared to place higher importance on interpersonal relationships and information transmission than on "immediate informational requirements."[27] Chinese services may prefer to have a trustworthy source without direct information access than someone "on the inside" who cannot be fully trusted.

Between 1949 and 2011, PRC intelligence services recruited many Taiwanese businessmen and former government officials while they were abroad in Mainland China or Hong Kong. For example, on an unspecified date, Chinese intelligence services recruited Chen Chih-Kao, a former Taiwanese Ministry of Justice official, while he was abroad in Shanghai trying to start a magazine business.[28] In 2005, Chen in turn recruited a classmate and fellow Ministry of Justice official to help him collect intelligence on behalf of China.[29] Furthermore, in 2004, Taiwanese authorities arrested Tseng Chao-Wen, a former Taiwanese intelligence officer, for espionage.[30] Chinese intelligence officials recruited Tseng at an unspecified time during his post-retirement travels to China and Tseng "took advantage of his contacts in the Taiwanese intelligence community to collect information for Beijing."[31] Chinese officials paid Chen and Tseng handsomely for their services.[32]

Chinese intelligence services also recruited many Chinese emigrants about to go abroad for work or study. According to Mattis, the Chinese Ministry of State Security's organizational charts reveal the existence of a bureau dedicated solely to monitoring emigrants for possible recruitment, and intelligence services can likely access emigrants' passports and travel destinations to determine the highest-value targets. The Chi Mak case is a notable example of this type of directed access operation. Chinese services probably first recruited Chi Mak in the 1960s. Mak was already spying for the PRC and monitoring the movements of U.S. vessels in Hong Kong even before he left for the United States.[33] Chinese intelligence services probably gave Mak a long-term mission to infiltrate the U.S. defense and intelligence communities, as Mak "slept" for almost twenty years before making any significant movements.[34] Chinese patience finally paid off when Mak became a naturalized U.S. citizen in 1985, accepted a position with a defense contractor that specialized in advanced naval propulsion technology, and obtained a SECRET security clearance in 1996.[35]

Mak provided sensitive and classified information to his Chinese handlers relating to submarines and the DD(X) destroyer program.[36] Chinese handlers also provided tasking lists to Mak, requesting that he collect information about specific military technologies.[37] U.S. authorities finally arrested Mak in 2015 and ultimately sentenced him to 24½ years in prison.[38] Chinese authorities likely did not recruit Mak with a specific, long-term objective in mind. However, the PRC probably at least wanted to ensure that Mak obtained a sensitive position with access to classified U.S. government information. Once Mak gained access to the U.S. national security community, Chinese services could probably send him additional tasks to collect more specific information.

Larry Wu-Tai Chin, a turncoat CIA officer and one of the most notorious Chinese spies in the United States, was a U.S. government employee at the time he was recruited and did have direct access to information of interest.

Around 2004, Chinese authorities also recruited Glenn Duffie Shriver, an American student who was studying abroad in Shanghai.[39] Shriver responded to an advertisement, likely from the Chinese Ministry of State Security (MSS), soliciting papers on Sino-American relations in return for a payment of $120.[40] MSS case officers met with Shriver on several occasions and recruited him through a gradual, low-key approach.[41] Throughout several years, the MSS continued to pay Shriver in exchange for taking the U.S. Foreign Service exam and submitting applications to the Central Intelligence Agency (CIA) in an attempt to place Shriver in a position with access to classified information.[42] In 2010, during Shriver's final processing for a National Clandestine Service position, U.S. authorities detected inconsistencies in Shriver's background investigation statements and confronted him about his contact with Chinese government organizations.[43] Shriver was ultimately sentenced to four years in prison.[44]

On the other hand, Larry Wu-Tai Chin, a turncoat CIA officer and one of the most notorious Chinese spies in the United States, was a U.S. government employee at the time he was recruited and did have direct access to information of interest. Even so, sources state that Communist intelligence officers recruited Chin in 1944, even before the founding of the People's Republic of China, when Chin was still a translator for a U.S. Army liaison office in Fuzhou.[45] Chin probably had limited access to classified information, if any, as a translator at the time of his recruitment. Communist intelligence services probably directed Chin to seek out subsequent posts with enhance information access, which falls in line with the PRC's standard procedures for running agents in directed access operations. Chin became an interpreter at the U.S. consulate in Shanghai in 1948 and joined the CIA's Foreign Broadcast Information Service in 1952. In 1965, Chin became a U.S. citizen and passed a polygraph test to obtain a TOP SECRET clearance soon afterward, granting him access to classified information to send back to his Chinese handlers.[46]

Recruits Are Almost Always Ethnically Chinese

Almost all agents recruited by the Chinese intelligence services were ethnically Han Chinese or Chinese ethnic minorities. For example, in a survey of nine PRC-directed access operations against Taiwan between 1949 and 2011, Peter Mattis found that all recruited agents were ethnically Chinese.[47] Additionally, in all PRC espionage cases against the United States during this period, Glenn Duffie Shriver was the only non-ethnically Chinese agent employed.

Chinese intelligence services sometimes also employ ethnic minorities, like Mongolians and Uyghurs, for intelligence collection, especially against leaders of ethnic minority dissident groups based overseas. For example, Chinese intelligence services sent Gankhuyag Bumuutseren, a Mongolian citizen, to the United States to monitor Chinese ethnic dissidents in the 1990s.[48] However, Chinese authorities imprisoned and tortured Bumuutseren when they discovered that the Mongolian was a double agent who also reported to Mongolian intelligence.[49] In the early 2000s, Chinese officials most likely released Bumuutseren with the condition that he accept another mission to "monitor and photograph the leaders of a Chinese secessionist movement" in Canada.[50] Bumuutseren arrived in Canada in 2005, but Canadian authorities detected Bumuutseren's illegal activities soon afterward and commenced deportation proceedings.[51]

Glenn Duffie Shriver was the only publicly known, non-ethically Chinese agent directly recruited by Chinese case officers between 1949 and 2011. The Shriver case proved that China was willing and able to recruit non-ethnically Chinese assets, but may not have been completely comfortable with this approach due to cultural differences and the inability to appeal to patriotism and a shared Chinese identity. Even though Chinese agents use cash, blackmail, and coercion to recruit assets, just like Western services, elements such as cultural similarities and patriotism could likely supplement material incentives.

Some analysts argue that the Lin Hong case, which involved a Chinese spy ring in the late 1990s and early 2000s, may be another exception, as Lin Hong, a China-based spymaster, recruited two non-ethnically Chinese

agents, James Fondren and Gregg Bergersen.[52] Even so, the Chinese services did not recruit Fondren and Bergersen directly. Lin still recruited his principal agent, Kuo, an ethnically Chinese man, in China, and Kuo only later consulted the non-ethnically Chinese co-conspirators as secondary sources when he returned to the U.S.[53] Between 1949 and 2011, the Chinese services recruited only one publicly known, non-ethnically Chinese agent—Shriver—and his recruitment occurred in 2004, near the end of the period of analysis.

Lack of Professional Intelligence Tradecraft

According to retired FBI China expert Paul Moore, China normally does not pay money for intelligence. The Russians pay money, everybody pays money, but as a rule, the Chinese do not.[54] "China collects information from good people, people who don't have financial problems, don't have emotional problems, who are not motivated by revenge, not unsuccessful in their lives. Not someone who is lonely, needs a friend, needs a woman."[55] Moore is an analyst who almost exclusively subscribes to the "grain of sand" interpretation of Chinese intelligence operations.

Unfortunately, Moore is incorrect. Chinese intelligence services frequently pay money to Taiwanese recruits in exchange for collecting intelligence in Taiwan. Indeed, the Chinese intelligence services used cash as a recruitment incentive in all nine cases of Chinese-directed access operations against Taiwan analyzed by Peter Mattis.[56] The Chinese pay money to American recruits as well. The Ministry of State Security paid Glenn Duffie Shriver $30,000 to take the U.S. Foreign Service Exam and approximately $40,000 to pursue a CIA position.[57] Chinese services paid Larry Wu-Tai Chin more than $180,000 in exchange for his services (we cannot determine the total amount of money Chin received due to his skills in money laundering).[58] Finally, the Ministry of State Security and other organizations frequently employ "honey trap" operations to blackmail potential recruits, as in the case of a U.S. defense contractor in PACOM.[59]

However, Moore also mentions that "China does not use dead drops" and Chinese intelligence services do not employ "intelligence tradecraft" in the Western sense.[60] With respect to the 1949 to 2011 cases, Moore is largely correct. No public reports exist of any Chinese assets using professional, clandestine intelligence tradecraft, designed to conceal Chinese involvement, including chalk, dead drops, and eavesdropping devices, on the tactical or operational levels, outside of China to collect intelligence or arrange meetings with their handlers. Indeed, most Chinese handlers and case agents remain in China and very rarely meet with their agents overseas. Chi Mak had poor operational tradecraft, tearing the Chinese intelligence services' handwritten technology wish lists into small pieces which he deposited into the trash.[61] Later, U.S investigators were able to reassemble the lists which offered direct proof of Mak's illegal activities.[62] Additionally, Katrina Leung made no attempt to hide her finances fully, purchasing a house for $1.4 million in San Marino, Los Angeles, opening a Chinese language book store, and stashing funds in sixteen foreign bank accounts.[63] Leung also maintained affairs with two FBI agents, which a professionally trained intelligence officer would not even consider.[64] Larry Wu-Tai Chin may have been the exception to this rule due to his skills in money laundering. However, Chin was probably familiar with Western tradecraft because of his CIA experience, and not because Chinese case officers trained him in tradecraft when first recruiting him.

Peter Mattis implies that, while Chinese case officers may be trained in covert operations, surveillance, and targeting techniques inside of China, these officers rarely train their agents in these methods.[65] According to Mattis, "principal agents are not necessarily trained like professional intelligence officers or investigators, but, when trying to find sources with direct access, would look like case officers trying to recruit agents. Counterintelligence investigators operating against PRC intelligence only would see the principal agent, not the case officer."[66]

Agent Recruitment Outside China

From 1949 to 2011, Chinese intelligence services mostly recruited agents within China, prioritized relationships over direct information access, employed ethnically-Chinese agents, and did not extensively train principal agents in intelligence tradecraft. Chinese HUMINT operations during this period most clearly aligned with Peter Mattis' adapted internal security model. It may seem that Chinese intelligence services employed a risk-averse approach, conserving resources, recruiting agents with similar ethnicities to increase operational comfort, closely monitoring potential recruits and foreigners in China, and moving to recruiting sources only if an opportunity emerges, with internal security as the end goal in all instances. However, three publicly known cases are exceptions to these patterns.

In 1987 undercover FBI agents approached two Chinese diplomatic officials in a sting operation and offered to sell classified NSA documents to the Chinese officials.[67] The FBI caught the Chinese officials red-handed when they prepared to pay for the documents, and the State Department asked the diplomats to leave based on activities incompatible with their diplomatic status.[68] Still, this case may not be a true example of Chinese case

officers operating overseas, since the FBI made the first move in implementing the sting operation, and the Chinese diplomats did not make any effort to recruit agents while abroad in the United States. The Chinese diplomats would most likely not have spearheaded recruitment efforts had the FBI not proactively introduced them to the possibility of purchasing NSA documents.

In 2009 Swedish authorities arrested a Mandarin-speaking Uyghur and Swedish citizen who was gathering intelligence on the Swedish Uyghur community.[69] The man, Baibur Maihesuti, was a refugee who first entered Sweden in the 1990s, and was handled by a Chinese diplomat and journalist based in Sweden.[70] The Maihesuti case was the first publicly available espionage case in which Chinese case officers recruited and ran an agent from outside of China, probably from the Chinese Embassy in Sweden, resembling a "foreign-directed" intelligence collection approach. Nevertheless, we can argue that the Maihesuti case involved gathering intelligence on foreign-based ethnic minority communities to promote Chinese internal security. In this instance, the Chinese intelligence services may have had no other choice but to monitor Maihesuti closely from abroad to ensure he collected the most effective intelligence possible, with the goal of defusing foreign support to terrorist or dissident Uyghur organizations in China. Perhaps we can better explain this case as an instance of Chinese offensive counterintelligence, but with an end goal compatible with the adapted internal security model.

The 2011 case of Lo Hsien-Che, a Chinese spy in Taiwan, is another instance of Chinese case officers running an agent outside of China. After Lo's arrest, Taiwanese authorities learned that Chinese authorities recruited Lo in Thailand, where Lo was stationed as a Taiwanese military attaché between 2002 and 2005.[71] A Chinese case officer with an Australian passport reportedly recruited Lo in a honey trap operation, offering money and sex as incentives.[72] After Lo departed Thailand, he reportedly met his handlers in third countries, including the United States.[73] In contrast to the Baibur Maihesuti case, we cannot easily assess Chinese HUMINT operations in the Lo Hsien-Che case in the light of internal security. Additionally, the Maihesuti and Lo cases came to light at the end of this period, in 2009 and 2011 respectively. Writing in 2011, Mattis asked, "Why have PRC intelligence officers in widely disparate parts of the world started running clandestine agent operations entirely overseas?"[74] Mattis implied that China may have been testing certain elements of the "foreign-directed" model through the cases of Maihesuti and Lo, and the "Western, foreign-directed intelligence approach may be the future of [Chinese] intelligence."[75]

CHINESE HUMINT OPERATIONS POST-2011: ESPIONAGE IN THE ERA OF XI JINPING

I argue that Chinese intelligence operations had already begun shifting toward the "Western/Russian" foreign-directed intelligence collection model since Xi Jinping assumed Chinese leadership in 2012. The "foreign-directed" model can best explain Chinese HUMINT operational styles in nine recent Chinese espionage cases uncovered in the United States and Taiwan between 2012 and 2019: Kun Shan CHUN, Candice Marie Claiborne, Kevin Patrick Mallory, WANG Tsung-Wu, HSIEH Chia-Kang, XU Yanjun, Ron Hansen, Xuehua PENG, and the attempted recruitment of an *Asia Sentinel* journalist.

Kun Shan CHUN, Candice Marie Claiborne, and Kevin Patrick Mallory

In August 2016, Kun Shan CHUN, a naturalized U.S. citizen from China and a FBI electronics technician, pled guilty to "acting in the United States as an agent of the People's Republic of China, without providing prior notice to the Attorney General."[76] Although a Chinese company called Kolion probably first contacted CHUN when he travelled to China around 2005, Chinese government officials probably first recruited CHUN in either France or Italy. Kolion employees sent CHUN an email "that included information relating to hotels in France and Italy [which] stated, 'Five Star Hotel the entire way.'"[77] This email was likely an invitation for a paid vacation in exchange for performing services for Kolion, like obtaining U.S. information or technologies.[78] Some technologies that Kolion requested from CHUN, including solid state hard drives and remanufactured printer cartridges, were not highly sensitive.[79] However, Kolion officials likely used these simple consulting tasks to establish a relationship with CHUN and eventually arrange for CHUN to meet with Chinese intelligence officials.

According to a Department of Justice press release, Chinese nationals, likely from Kolion, introduced CHUN to a Chinese government official while he was abroad on the 2011 Kolion-sponsored trip to France and Italy.[80] The official asked CHUN about "sensitive, non-public FBI information," and CHUN allegedly also divulged the "identity and potential travel plans of an FBI agent."[81] In 2015 CHUN again met his Chinese government handler in Europe and maintained communication through WeChat, a mobile messenger application.[82] In January, 2017, CHUN was sentenced to 24 months in prison.[83]

In another 2017 case, U.S. authorities arrested Candice Marie Claiborne, a State Department employee with a TOP SECRET clearance, and charged her with "concealing extensive contacts with foreign agents."[84] Chinese intelligence officials from the Beijing and Shanghai State Security Bureaus reportedly recruited Claiborne while she was stationed with the State Department in China, and, from 2010 to 2014, provided gifts to her and her family (including a potential younger dependent) including cash, an iPhone and laptop computer, Chinese New Year gifts, meals, paid international vacations, tuition at a Chinese fashion school, a fully furnished apartment, and a monthly stipend.[85] According to a redacted Department of Justice affidavit, "when Claiborne was no longer in China and unable to meet face-to-face with [the co-conspirators, she told a witness] that she used a China-based social media application (possibly WeChat) to communicate with 'them, the China experts.'"[86] Chinese officials tasked Claiborne to "provide internal U.S. government analyses on a U.S.-Sino Strategic Economic Dialogue that just concluded," among other things.[87]

Finally, in June 2017, U.S. authorities arrested Kevin Patrick Mallory, a former CIA officer, for selling classified information to Chinese intelligence services. Mallory previously held a TOP SECRET clearance for most of his career but retired from the U.S. federal government around 2012.[88] According to the affidavit of a FBI agent investigating the case, a Chinese "recruiter" from the Shanghai Academy of Social Sciences (and probably the Shanghai State Security Bureau) first contacted Mallory on social media in February 2017 and introduced him to other potential Chinese "clients."[89] Mallory subsequently travelled to Shanghai separately in March and April of 2017 to meet with the Chinese contacts and their "boss."[90] Mallory then contacted several co-workers in the U.S. government (probably the CIA), most likely to obtain information to pass to his Chinese handlers.[91] Through unspecified means, Mallory obtained several documents classified at the TOP SECRET level and passed them to his Chinese handlers using a specially designed secure electronic communications device provided by the Chinese.[92] Mallory faces up to life in prison.

The CHUN, Claiborne, and Mallory cases differed from prior Chinese HUMINT operations in several ways. First, the CHUN case demonstrates that Chinese intelligence services have become increasingly comfortable meeting, and probably recruiting, sources abroad since 2011. Chinese government officials first met CHUN in France and Italy and most likely recruited him outside of China. Additionally, Chinese intelligence services have been more willing to initiate contact with agents through social media services, like WeChat. Mallory first received a social media solicitation from Chinese officials before he even travelled to China to meet with officers.

Chinese intelligence services are using increasingly sophisticated forms of Western-style tradecraft and offering tradecraft training to their recruits.

Second, Chinese intelligence services are using increasingly sophisticated forms of Western-style tradecraft and offering tradecraft training to their recruits. Mallory received an unspecified electronic "communications device" from his handlers while he was in Shanghai, which could move "from normal to secure messaging modes" and "required an SD card" to function.[93] The Chinese case officers taught Mallory how to use the device, and Mallory used the secure communications mode to pass classified documents to his handlers.[94] Mallory's messages provided further insights into the device's operation. On or about May 1, 2017, Mallory sent a secure message through the device stating, "We may need to go again step by step in my getting the document to become part [of this image]. Then sending it to you."[95] This information suggests that the device was capable of sending both text messages and images. The development of this device indicates that at least the Shanghai State Security Bureau, if not other Chinese intelligence agencies, were willing to invest resources to develop a high-tech, customized device, with two messaging modes, to ensure secure electronic communications with a source.

Third, the Claiborne and Mallory cases suggest that Chinese intelligence services are growing increasingly comfortable with recruiting non-ethnically Chinese sources. The intelligence collection activity in the Mallory case occurred in 2017, but Chinese sources may have recruited Claiborne as early as 2010. Clearly, Chinese case officers are increasingly using money as a core recruitment incentive, as shown in all three cases. For example, Chinese services paid Claiborne at least $60,000 for her services, and Claiborne noted in a journal that she could "generate 20K in one year" working with the Chinese agents.[96] For Chinese case officers, money may be becoming more effective than appeals to patriotism or shared cultural values for recruiting agents.

Most importantly, Chinese intelligence services recruited CHUN and Claiborne while they had direct access to sensitive and classified information of Chinese interest, representing a significant shift from the adapted internal security model's opportunistic (vice targeted) recruitment style, which prioritizes transmission, or maintaining a "reliable channel that minimizes distortions," over direct access to information.[97] According to Mattis, the "'foreign-directed' model would involve assessing the suitability of an

agent to provide valuable foreign intelligence, while the 'adapted internal security' model would examine threats to the state and party."[98] Mattis also explains that "targeted (non-opportunistic) operations (in line with the foreign-directed model) would imply the intelligence service will ignore potential agents irrelevant to policy objectives."[99]

...the Claiborne case was the first time the Chinese intelligence services recruited a non-ethically Chinese asset with direct information access, signaling that the Chinese are becoming bolder in their recruitment efforts.

Chinese authorities had very clear and specific intelligence collection goals in all three of these cases. A Chinese handler asked CHUN about the "internal structure of the FBI" and FBI surveillance technologies.[100] In response to these inquiries, CHUN passed to his handler an FBI organizational chart and photos of documents summarizing FBI surveillance technologies.[101] The Chinese government official who met CHUN in France and Italy knew CHUN was working for the FBI, and probably obtained this information from CHUN's prior Kolion contacts.[102] The CHUN case strongly suggests that the Chinese intelligence services had specific intelligence gaps concerning the FBI's organization and surveillance technologies. Indeed, Chinese services probably identified CHUN through his Kolion contacts and deliberately proceeded to recruit CHUN to fill these intelligence gaps.

The Chinese intelligence services also recruited Claiborne while she was still in her official capacity as a State Department employee, suggesting that the Chinese intelligence services had immediate intelligence needs. Indeed, the State Security officials gave Claiborne specific taskings, asking her for information about "internal evaluations on the U.S.-China Strategic and Economic dialogue, the types of pressures that the U.S. government wanted to place on China if certain expectations were unmet, and internal attitudes [of] high-level U.S. officials."[103] The "adapted internal security" model can explain many of Claiborne's taskings in light of Chinese internal economic stability but, at the very least, the Claiborne case was the first time the Chinese intelligence services recruited a non-ethically Chinese asset with direct information access, signaling that the Chinese are becoming bolder in their recruitment efforts.

The Mallory case also suggests that the Chinese intelligence services may be shifting toward more "Western, foreign-directed" targeting. Mallory was a natural-born United States citizen who had significant experience in the Central Intelligence Agency and the Diplomatic Security Service. Mallory may not have had direct access in his retirement state, but it would be difficult to imagine a better principal agent with contacts in the most sensitive U.S. government agencies. Mallory contacted CIA employees on behalf of the Chinese intelligence services and, through unspecified means, successfully obtained and transmitted to the Chinese at least three documents classified at the TOP SECRET and SECRET levels.[104] Although further details about the Mallory case are probably classified, the Chinese probably did not reach out to Mallory opportunistically. An official at the Shanghai Academy of Social Sciences deliberately initiated contact through social media, and Chinese officials probably gave Mallory specific taskings when he met with State Security officials in China.

WANG Tsung-Wu and HSIEH Chia-Kang

Two recent Chinese espionage cases in Taiwan further support the theory that Chinese intelligence services have become vastly more comfortable running or recruiting sources from bases outside of China. In September 2016, Taiwanese authorities sentenced Major Wang Tsung-Wu, a former Taiwanese intelligence officer, for espionage as a Chinese double agent.[105] Taiwanese officials first deployed Wang to gather intelligence in China more than 20 years ago, and Chinese intelligence officers turned Wang as a double agent in approximately 1995.[106] Wang retired in 2005 and continued working on behalf of China after his retirement.[107] In 2013 Wang recruited a retired colleague, Lin Han, to help him gather intelligence on behalf of China.[108] Wang met his Chinese handlers in Singapore and Malaysia during an unknown period of time and "disclosed the identities and missions of Taiwanese intelligence officials."[109]

The 2017 case of HSIEH Chia-Kang is an even more significant example of increasing Chinese HUMINT operations in third countries. HSIEH, the Deputy Chief of Taiwan's Army Command for the Defense of Matsu, had extensive knowledge and expertise about Taiwan's indigenous missiles, the Patriot PAC-3 batteries, and "newly developed projectiles which could hit Shanghai."[110] According to the *Taipei Times*, HSIEH traveled to Thailand and Malaysia, where he first met his Chinese handlers, possibly received financial rewards for passing classified military information, and agreed to "recruit other individuals to set up a spy ring in Taiwan."[111] Another Taiwanese army officer spying for the Chinese, HSIN Peng-sheng, may have first recruited HSIEH in Taiwan, but the sequence of recruitment is unclear.[112] Regardless, HSIEH first travelled to Thailand and Malaysia, not mainland China, to meet with his Chinese handlers.

The WANG and HSIEH cases, in combination with the LO Hsien-Che case, suggest that Chinese intelligence services may see Southeast Asian nations, like Thailand and Malaysia, as particularly attractive locations for case officers to meet with their agents, especially in espionage operations against Taiwan. Indeed, a Malaysian news article indicates that the Malaysian police have been in close contact with their Taiwanese counterparts regarding the WANG case, suggesting that Malaysia may have further information to share regarding Chinese agent recruitment activities in-country.[113] Although more specific information about Chinese intelligence activities in Thailand and Malaysia is unknown, we can speculate that Chinese intelligence services may be more comfortable operating from these nations than other Asian states due to established host-government contacts, resources, and intelligence infrastructure.

Additionally, the WANG case could indicate that Chinese intelligence services saw third country meetings as a benefit for operational security when running a double agent. When Chinese officials recruited WANG while he was stationed in China in 1995, Chinese officials may have suggested subsequent meetings in a third country because frequent travels to China may have raised red flags for a Taiwanese intelligence official. Although the WANG case is the most solid example of this theory, since WANG was a double agent, we can speculate that Chinese officials may also have preferred to meet with CHUN, LO, and HSIEH in third countries in Europe and Asia (under the guise of vacations, etc.) to decrease foreign government suspicion when running current government or military officials as assets. Chinese officials were probably aware of CHUN's need to report any foreign travel in his FBI security forms and on his SF-86 during periodic security clearance reinvestigations.[114] The LO, CHUN, WANG, and HSIEH cases suggest that China may be increasingly using "methods designed to hide government sponsorship" by establishing "overseas bases of operation," in line with the "Western, foreign-directed" model.

XU Yanjun, Ron Hansen, and Xuehua PENG

From at least December 2013 until his 2018 arrest, XU, a Deputy Division Director of the Chinese Ministry of State Security, conducted economic espionage against several U.S. and foreign aviation companies, including GE Aviation.[115] XU targeted employees of these companies and paid them to travel to China and share trade secrets, under the guise of asking them to deliver presentations at Chinese universities.[116] In April 2018, XU traveled to Belgium to meet with one of his sources, where he was arrested at the request of the United States, and he was later formally extradited to the United States to stand trial.[117]

In another recent case, Chinese intelligence services targeted Ron Hansen, a former U.S. Army Officer and DIA case officer who was fluent in Chinese, with extensive training in intelligence tradecraft.[118] Between 2006 and 2011, after retiring from the U.S. government, Hansen began working at a digital forensics company where he coordinated the company's business in Asia, and began travelling extensively to China.[119] According to the FBI investigation, from approximately 2013 to 2017 Hansen began attending conferences on behalf of the PRC intelligence services to collect information from prominent conference presenters who, in some cases, were still working in sensitive government positions.[120] Hansen also reestablished contact with several colleagues at DIA and attempted to recruit a current DIA case officer to sell classified national defense information to the PRC.[121] In total, Hansen received at least $800,000 from his handlers for his assistance in obtaining information at defense and national security conferences that the Chinese services found valuable, as well as his efforts to obtain classified information through other channels.[122]

Finally, Xuehua PENG was arrested in September 2019 for acting as an illegal foreign agent for the PRC.[123] The PENG case emerged from a U.S. government-coordinated double-agent operation targeting the Ministry of State Security. Around 2015, the U.S. government deployed a confidential human source to meet with MSS officers, provide them with classified information that was carefully selected to mitigate damage to U.S. national security, and receive financial payments.[124] MSS officers tasked the U.S. government's confidential source to travel to a Newark, California, hotel and prepared a "dead drop" package by adding classified information to an SD card, "placing the card in a book, wrapping the book in a bag," and leaving the bag at the hotel's front desk.[125] The FBI investigation revealed that PENG picked up the source's dead drop, and left additional dead drop packages for the source at other California hotels for delivery onward to China.[126] For each pick-up or delivery, PENG left the source approximately $10,000 or $20,000.[127]

These three recent cases from 2018 to 2019 provide further evidence that the Chinese intelligence services may be shifting to a "foreign-directed" intelligence collection approach. The XU case demonstrates that medium- or high-ranking MSS agents are increasingly willing to travel to third countries, even to U.S. allies like Belgium, to meet sources. Moreover, the Hansen case demonstrates that Chinese services are using a more tailored approach to recruit non-ethnically Chinese agents who are already established within target countries' national security organizations, like DIA. Most importantly, the PENG case conclusively demonstrates that the Chinese intelligence services are increasingly employing traditional HUMINT tradecraft, like "dead drops." The "grain of sand" model's assumption that "PRC

intelligence services [do not regularly] pay agents for sensitive information [or use] age-old tools like dead drops" has now been completely falsified.[128]

The *Asia Sentinel* Incident

The *Asia Sentinel* Incident provides excellent insights into how Chinese intelligence services recruit targets in practice. Chinese State Security officials contacted *Asia Sentinel* journalist Nate Thayer via social media in September 2014 to recruit him as a potential agent, and Thayer documented his full recruitment experience over the course of two years in a 2017 article, offering valuable play-by-play insights into the Chinese agent recruitment process.[129]

Thayer first received a LinkedIn message from a Shanghai State Security Bureau front organization, praising Thayer as a "renowned international journalist" and asking for "cooperation opportunities."[130] After Thayer decided to play along, the State Security officials sent him another message seeking very specific, targeted information about the Kyaukpyu Port project in Burma.[131] Specifically, the Chinese officials wanted to know "how the U.S. assesses the Kyaukpyu Port project, the latest unrevealed talks between the U.S. and Burma on the project, and what measures the U.S. would take concerning the project."[132] The Chinese offered a payment of between $500 and $1,000 and sent further messages, asking for information about "secret talks between the US and North Korea held in Singapore in January 2015," and requested that Thayer use his "Washington government social circles in the State Department and National Security Council" to pass them "information not available on the internet."[133]

Thayer ultimately discontinued contact with the State Security officials, but the *Asia Sentinel* Incident demonstrates that Chinese intelligence services are employing very direct, targeted pitches to individuals on social media. Peter Mattis commented on this incident, stating that "the Chinese intelligence services usually cast a 'wide net.' The MSS comes to people like you. You said no, a friend of mine said no, but Mallory said yes. If they get one in 10 or one in 20 to bite, that works for them."[134] However, I argue that, rather than opportunistically reaching out to prospective recruits without access like Shriver using unfocused, public advertisements, Chinese officers are now closely mining social media for important contacts that suggest potential access to valuable information and sending out tailored, personal messages. Rather than casting a "wide net" for all potential recruits, Chinese intelligence services are narrowing their search to only the highest-quality "fish" in the ocean of national security who have the most effective potential connections and access, demonstrating a certain level of targeting in line with the "foreign-directed model."

CONCLUSION

The Chinese intelligence services have not yet completely shifted to a "foreign-directed" intelligence collection approach, but Chinese services have, at the very least, employed elements of the "foreign-directed" model much more often in espionage operations since Xi Jinping assumed the Chinese leadership in 2012. Indeed, I argue that, collectively, the cases of Kun Shan CHUN, Candice Marie Claiborne, Kevin Patrick Mallory, WANG Tsung-Wu, HSIEH Chia-Kang, XU Yanjun, Ron Hansen, and Xuehua PENG, and the 2014 *Asia Sentinel* recruitment attempt demonstrate that Chinese HUMINT collection styles have already begun to shift to a "foreign-directed" approach due to increased political, economic, and military demands overseas, and the need for increased foreign intelligence to inform Chinese decision-making.

Moreover, the number of Chinese espionage cases in the United States that demonstrate a "foreign-directed" approach have increased exponentially, with three relevant cases uncovered between 2018 and 2019 alone. Importantly, in December 2019, *The New York Times* reported that the United States secretly expelled two Chinese diplomats who were stationed at the Chinese Embassy in Washington, DC, after they attempted to infiltrate a sensitive military facility near Norfolk, Virginia, by driving through the security checkpoint.[135] The U.S. government believes that at least one of the diplomats was a Chinese intelligence officer operating under diplomatic cover (the alternative explanation advanced by some Taiwanese analysts is improbable).[136] If true, this incident suggests that the Chinese intelligence services have not only started recruiting sources from overseas bases, but also started engaging in overt and covert operations potentially designed to test the security of U.S. military facilities, representing an almost complete shift toward a "foreign-directed," professional intelligence collection model.[137] Just a few years ago, in 2013 or 2014, a Chinese intelligence officer directly employed by a Chinese intelligence service (not a proxy) engaging in operational work from an overseas base would probably have been unthinkable.[138] U.S. policymakers and analysts should note that the Chinese HUMINT operations are changing in four main ways.

First, Chinese case officers and agents are becoming much more professional. The Mallory case demonstrates that Chinese case officers are willing to develop customized, secure electronic communications devices and train sources on how to use these devices to establish secure communication channels. The PENG case also provides conclusive evidence that Chinese services are extensively employing traditional HUMINT tradecraft, like dead drops.

Second, Chinese case officers are becoming increasingly comfortable with running or recruiting agents in third countries outside of China. Chinese operational styles in the LO and Maihesuti cases are now no longer the exception, given recent third-country meetings in the CHUN, WANG, HSIEH, and XU cases. In the future, Chinese case officers may also begin to establish more operational bases in the target country itself like in the Baibur Maihesuti case. Chinese intelligence services may be taking more care to conceal state involvement in espionage operations by meeting sources in third countries.

Third, the Claiborne, Mallory, Hansen, and *Asia Sentinel* cases indicate that anyone with potential foreign government contacts or sensitive information access is now a potential target for China, ethnically Chinese or not. Chinese intelligence services are now more often appealing to traditional recruitment incentives, including money and sex, than patriotism or Chinese cultural affinity.

Finally, Chinese case officers are increasingly targeting high-ranking and experienced recruits with direct sensitive information access or reliable contacts in foreign governments of interest. The Mallory, Hansen, and *Asia Sentinel* cases indicate that Chinese targeting is no longer as opportunistic as it used to be, and Chinese officials do a considerable amount of research to narrow down the number of high-value targets before making recruitment pitches. In the future, Chinese services are likely to be more aggressive and proactive when recruiting and may value direct information access far more than interpersonal relationships or information transmission. Chinese services will probably no longer post public advertisements for papers to lure any unsuspecting students like in the Shriver case, and instead make personalized recruitment pitches to specific targets.

This article's findings have two main implications for U.S. national security and foreign policy. First, the "grain of sand" model of Chinese intelligence operations was never completely accurate from 1949 to 2011 in the "adapted internal security" era, and it certainly is not true now. Policymakers, analysts, and law enforcement officials should be open to interpreting Chinese HUMINT operations the same way as traditional, professional Eastern Bloc operations during the Cold War when coordinating counterintelligence strategies and operations. Of course, some "grain of sand" elements may remain, likely as part of a "dual-track" intelligence collection approach as Chinese intelligence services continue their shift to a "foreign-directed" doctrine. Nevertheless, solely viewing Chinese intelligence collection through the "grain of sand" or "adapted internal security" models may lead to an incomplete picture of Chinese intelligence collection methods and goals.

Second, if China is indeed shifting to a "foreign-directed" intelligence collection model, U.S. policymakers and intelligence analysts should also closely monitor how China attempts to balance its internal and external intelligence demands in the future. China's resources are finite; enhanced Chinese foreign intelligence operations will drain internal stability maintenance and surveillance capabilities, which already have significant maintenance costs in Hong Kong and Xinjiang. In a hypothetical future crisis with relentless foreign intelligence demands, such as a Taiwan invasion scenario, China may shift its resources outward, revealing internal vulnerabilities that can be exploited. The United States must be prepared to take advantage of such strategic opportunities if they arise.

The U.S. Intelligence Community should commission a classified study to determine if additional cases support or refute some of the theories in this article. U.S. policymakers could also recruit contractors and academics to compile a comprehensive database of Chinese intelligence operations for quantitative analysis, which may shed additional insight into Chinese operational patterns. This article's limited analysis of successfully prosecuted Chinese espionage cases in the United States, Europe, and Taiwan provides background information to analysts that would likely inform both of these research projects.

NOTES

[1] Chris Buckley and Keith Bradsher, "Xi Jinping's Marathon Speech: Five Takeaways," *The New York Times,* October 18, 2017, accessed November 24, 2019, https://www.nytimes.com/2017/10/18/world/asia/china-xi-jinping-party-congress.html?_r=0.

[2] Yan Xuetong, "From Keeping a Low Profile to Striving for Achievement," *Chinese Journal of International Politics* 7, no. 2 (2014): 153-184, accessed November 24, 2019, https://academic.oup.com/cjip/article/7/2/153/438673.

[3] Peter Mattis, "Chinese Intelligence Operations Reconsidered: Toward a New Baseline," master's thesis, Georgetown University, 2011 (available at Georgetown University), 7; "Conduct Offensive (Strategic) Counterintelligence Operations in Furtherance of National Security Policy Initiatives" (declassified), Central Intelligence Agency, July 5, 1997, accessed November 24, 2019, https://www.cia.gov/library/readingroom/docs/DOC_0000112364.pdf; Del Quintin Wilber, "The Saga of the Chinese Spies and the Stolen Corn Seeds: Will it Discourage Economic Espionage?" *The Los Angeles Times,* October 31, 2016, accessed November 24, 2019, http://www.latimes.com/nation/la-na-seeds-economic-espionage-20161031-story.html; Peter Mattis, "Beyond Spy vs. Spy: The Analytic Challenge of Understanding Chinese Intelligence Services," *Studies in Intelligence* 56, no. 3 (September 2012): 47-57, Center for the Study of Intelligence, Central Intelligence Agency, accessed November 24, 2019, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-56-no.-3/pdfs/Mattis-Understanding%20Chinese%20Intel.pdf.

[4] Devlin Barrett, "Chinese National Arrested for Allegedly Using Malware Linked to OPM Hack," *The Washington Post,* August 24, 2017, accessed November 24, 2019, https://

www.washingtonpost.com/world/national-security/chinese-national-arrested-for-using-malware-linked-to-opm-hack/2017/08/24/746cbdc2-8931-11e7-a50f-e0d4e6ec070a_story.html?utm_term=.568eb907ed53; Mattis, "Chinese Intelligence Operations Reconsidered," 20. HUMINT-focused Chinese intelligence organizations include the Ministry of State Security (MSS), the Ministry of Public Security (MPS), the Second Department of the People's Liberation Army's General Staff Department (2PLA), and the Liaison Office of the People's Liberation Army General Political Department (LO/GPD). 2PLA is also responsible for imagery intelligence and tactical reconnaissance, but its focus remains human intelligence. See Mattis, "Beyond Spy vs. Spy," 52. The People's Liberation Army's Strategic Support Force (PLASSF) is largely responsible for Chinese technical intelligence collection, consolidating cyber espionage capabilities, electronic support measures, and space-based ISR. Also see Elsa Kania, "The PLA Strategic Support Force: The 'Information Umbrella' for China's Military," *The Diplomat,* April 1, 2017, accessed November 24, 2019, https://thediplomat.com/2017/04/pla-strategic-support-force-the-information-umbrella-for-chinas-military/.

[5] Mattis, "Chinese Intelligence Operations Reconsidered," 55.

[6] "The Resistible Rise of Xi Jinping," *Foreign Policy,* October 19, 2017, accessed November 24, 2019, http://foreignpolicy.com/2017/10/19/the-resistible-rise-of-xi-jinping/.

[7] Dan Stober, "Frontline: China Is Different," *PBS,* January 15, 2004, accessed November 24, 2019, http://www.pbs.org/wgbh/pages/frontline/shows/spy/spies/different.html. Multiple versions of this quote, with slight variations, have circulated through intelligence circles.

[8] "Special Report: Espionage with Chinese Characteristics," *STRATFOR,* March 24, 2010, accessed November 24, 2019, 2; Mattis, "Chinese Intelligence Operations Reconsidered," 8.

[9] Mattis, "Beyond Spy vs. Spy."

[10] Mattis, "Chinese Intelligence Operations Reconsidered," 8.

[11] Ibid.

[12] Mattis, "Beyond Spy vs. Spy."

[13] Mattis, "Chinese Intelligence Operations Reconsidered," 8.

[14] Matthew Crosston, "Bringing Non-Western Cultures and Conditions into Comparative Intelligence Perspectives," *International Journal of Intelligence and CounterIntelligence* 29 (2016): 110-131, accessed November 24, 2019, http://www.tandfonline.com/doi/abs/10.1080/08850607.2015.1083337.

[15] Michael Herman, "Intelligence and Diplomacy," in *Intelligence Services in the Information Age* (Abingdon, UK: Frank Cass Publishers, 2001): 29-49.

[16] Mattis, "Chinese Intelligence Operations Reconsidered," 10.

[17] Mattis, "Chinese Intelligence Operations Reconsidered," 11-55.

[18] Mattis, "Chinese Intelligence Operations Reconsidered," 11.

[19] Ibid.

[20] Mattis, "Chinese Intelligence Operations Reconsidered," 55.

[21] Ibid.

[22] Mattis, "Chinese Intelligence Operations Reconsidered," 50.

[23] Ibid.

[24] Chinese case officers have recruited agents abroad (outside of China) only in three cases during this period: HOU Desheng et al., Baibur Maihesuti, and LO Hsien-Che. I treat these three cases as potential exceptions to the adapted internal security model and analyze them in detail at the end of this section.

[25] Mattis, "Chinese Intelligence Operations Reconsidered," 46,

[26] Mattis, "Chinese Intelligence Operations Reconsidered," 50.

[27] Mattis, "Chinese Intelligence Operations Reconsidered," 46-47.

[28] "Jail Sought for MJIB Agents on Spying for China," *China Post,* November 21, 2007, accessed November 24, 2019, https://chinapost.nownews.com/20071121-121399.

[29] Ibid.

[30] Brian Hsu, "Two People Detained over Suspected Spying for China," *Taipei Times,* November 14, 2003, accessed November 24, 2019, http://www.taipeitimes.com/News/taiwan/archives/2003/11/14/2003075777.

[31] Ibid.

[32] Ibid.; "Jail Sought for MJIB Agents."

[33] Yudhijit Bhattacharjee, "How the FBI Cracked a Chinese Spy Ring," *The New Yorker,* May 12, 2014, accessed November 24, 2019, https://www.newyorker.com/news/news-desk/how-the-f-b-i-cracked-a-chinese-spy-ring.

[34] Joby Warrick and Carrie Johnson, "Chinese Spy 'Slept' in United States for Two Decades," *The Washington Post,* April 3, 2008, accessed November 24, 2019, http://www.washingtonpost.com/wp-dyn/content/article/2008/04/02/AR2008040203952.html.

[35] Ibid.

[36] Bhattacharjee.

[37] Ibid.

[38] Ibid.

[39] David Wise, "Mole-In-Training: How China Tried to Infiltrate the CIA," *The Washingtonian*, June 7, 2012, accessed November 24, 2019, https://www.washingtonian.com/2012/06/07/chinas-mole-in-training/.

[40] Ibid.

[41] Ibid.

[42] Ibid.

[43] Ibid.

[44] Ibid.

[45] David Wise, *Tiger Trap: America's Secret Spy War with China* (New York: Harcourt, 2011), 203.

[46] Ibid.

[47] Mattis, "Chinese Intelligence Operations Reconsidered," 44.

[48] Stewart Bell, "When a Toronto Church Gave Sanctuary to a Man Facing Deportation, It Unwittingly Harbored a Child Molester," *National Post,* updated January 25, 2015, accessed December 18, 2015, http://nationalpost.com/news/when-a-toronto-church-gave-sanctuary-to-a-man-facing-deportation-it-unwittingly-harbored-a-child-molester.

[49] Ibid.

[50] Ibid.

[51] Ibid.

[52] Pauline Arrillaga, "How a Networking Immigrant Became a Spy," *The San Diego Union-Tribune,* May 8, 2011, accessed November 24, 2019, http://www.sandiegouniontribune.com/sdut-how-a-networking-immigrant-became-a-spy-2011may08-story.html.

[53] Ibid.

[54] Ibid.

[55] Wise, *Tiger Trap*, 16.

[56] Mattis, "Chinese Intelligence Operations Reconsidered," 44.

[57] Wise, "Mole-In-Training."

[58] Stephen Engelberg, "Spy for China Found Suffocated in Prison, Apparently a Suicide," *The New York Times,* February 22, 1986, accessed November 24, 2019, http://www.nytimes.com/1986/02/22/us/spy-for-china-found-suffocated-in-prison-apparently-a-suicide.html.

[59] "U.S. Intelligence Worker Caught in Chinese Honey Trap Scheme," *The New York Post,* March 19, 2013, accessed November 24, 2019, https://nypost.com/2013/03/19/us-intelligence-worker-caught-in-chinese-honey-trap-spy-scheme/.
[60] Wise, *Tiger Trap*, 12.
[61] Bhattacharjee.
[62] Ibid.
[63] Wise, *Tiger Trap*, 39.
[64] Wise, *Tiger Trap*, 41.
[65] Mattis, "Chinese Intelligence Operations Reconsidered," 50.
[66] Ibid.
[67] Jim Mann and Ronald J. Ostrow, "U.S. Ousts Two Chinese Envoys for Espionage," *The Los Angeles Times,* December 31, 1987, accessed November 24, 2019, http://articles.latimes.com/1987-12-31/news/mn-7581_1_diplomats.
[68] Ibid.
[69] Peter Mattis, "Five Ways China Spies," *The National Interest,* March 6, 2014, accessed November 24, 2019, http://nationalinterest.org/commentary/five-ways-china-spies-10008; "Sweden Jails Uyghur Chinese Man for Spying," *Reuters,* March 8, 2010, accessed November 24, 2019, https://www.reuters.com/article/us-sweden-china-spy/sweden-jails-uighur-chinese-man-for-spying-idUSTRE6274U620100308; Paul O' Mahony, "Pensioner Indicted Over Chinese Spy Scandal," *TheLocal.Se*, December 15, 2009, accessed November 24, 2019, https://www.thelocal.se/20091215/23864.
[70] Ibid.
[71] "Taiwan Spy Case: General Lo Hsien-Che Jailed for Life," *BBC News,* July 25, 2011, accessed November 24, 2019, http://www.bbc.com/news/world-asia-pacific-14273191; "Ð™•n˜[áTÿ…nâŒòTÐ™ðl^—Ð™•n [*Zhumei Guanyuan: Luo Xianzhe Zhutai Fei Zhumei*] [Official Posted in America: Lo Hsien-Che Was Posted in Thailand, Not America]," *NTDTV.com (Taiwan),* February 8, 2011, accessed November 24, 2019, http://www.ntdtv.com/xtr/b5/2011/02/09/a490289.html; "Taiwan Spy Case: General Lo Hsien-Che Jailed for Life."
[72] "Sex Lured Taiwan General to become Chinese Spy," *RNW Archives,* 2011, accessed November 24, 2019, https://www.rnw.org/archive/sex-lured-taiwan-general-become-china-spy.
[73] Ibid.
[74] Mattis, "Chinese Intelligence Operations Reconsidered," 54.
[75] Mattis, "Chinese Intelligence Operations Reconsidered," 55.
[76] "FBI Employee Pleads Guilty in Manhattan Federal Court to Acting in the United States as an Agent of the Chinese Government," U.S. Department of Justice press release, August 1, 2016, accessed November 24, 2019, https://www.justice.gov/usao-sdny/pr/fbi-employee-pleads-guilty-manhattan-federal-court-acting-united-states-agent-chinese.
[77] United States District Court for the Southern District of New York, United States of America v. Kun Shan Chun, a/k/a "Joey Chun," *Affidavit of Special Agent Jason Levitt of the Federal Bureau of Investigation,* https://www.justice.gov/opa/file/881161/download, 8 (accessed November 24, 2019).
[78] Ibid.
[79] Ibid.
[80] Ibid.; Benjamin Weiser and Megan Jula, "FBI Agent Pleads Guilty to Acting as an Agent of China," *The New York Times,* August 1, 2016, accessed November 24, 2019, https://www.nytimes.com/2016/08/02/nyregion/fbi-employee-pleads-guilty-to-acting-as-an-agent-of-china.html?_r=0.
[81] Ibid.
[82] *Affidavit of Special Agent Jason Levitt*, 10-12.
[83] "Former FBI Employee Sentenced in Manhattan Federal Court to 24 Months in Prison for Acting as an Agent of China," U.S. Department of Justice press release, January 20, 2017, accessed November 24, 2019, https://www.justice.gov/usao-sdny/pr/former-fbi-employee-sentenced-manhattan-federal-court-24-months-prison-acting-agent.
[84] "State Department Employee Arrested and Charged with Concealing Extensive Contacts with Foreign Agents," U.S. Department of Justice press release, March 29, 2017, accessed November 24, 2019, https://www.justice.gov/opa/pr/state-department-employee-arrested-and-charged-concealing-extensive-contacts-foreign-agents.
[85] Ibid.
[86] United States District Court for the District of Columbia, In the Matter of an Application for Criminal Complaint and Arrest Warrant for Candace Marie Claiborne, *Affidavit of Special Agent Kellie O'Brien of the Federal Bureau of Investigation,* https://www.justice.gov/opa/press-release/file/953321/download, 9 (accessed November 24, 2019).
[87] "State Department Employee Arrested and Charged."
[88] Rachel Weiner, "Former CIA Officer Accused of Selling Top Secret Information to China," *The Washington Post,* June 22, 2017, accessed November 24, 2019, https://www.washingtonpost.com/local/public-safety/ex-dod-employee-accused-of-selling-top-secret-governments-to-china/2017/06/22/3ec3a706-576f-11e7-a204-ad706461fa4f_story.html?utm_term=.c8dd710af55e.
[89] United States District Court for the Eastern District of Virginia, United States of America v. Kevin Patrick Mallory, *Affidavit of Special Agent Stephen Green of the Federal Bureau of Investigation,* https://www.justice.gov/opa/press-release/file/975671/download, 7-8 (accessed November 24, 2019); Weiner.
[90] Ibid.
[91] Weiner.
[92] *Affidavit of Special Agent Stephen Green,* 12-13.
[93] *Affidavit of Special Agent Stephen Green,* 8-10.
[94] Weiner.
[95] *Affidavit of Special Agent Stephen Green,* 11.
[96] "State Department Employee Arrested and Charged."
[97] Mattis, "Chinese Intelligence Operations Reconsidered," 51.
[98] Mattis, "Chinese Intelligence Operations Reconsidered," 11.
[99] Mattis, "Chinese Intelligence Operations Reconsidered," 3.
[100] "FBI Employee Pleads Guilty in Manhattan Federal Court."
[101] Ibid.
[102] Ibid.
[103] *Affidavit of Special Agent Kellie O'Bryan,* 8.
[104] *Affidavit of Special Agent Stephen Green,* 12.
[105] "Taiwan 'Double Agent' gets 18 Years for Spying for China," *The Straits Times,* September 23, 2016, accessed November 24, 2019, http://www.straitstimes.com/asia/east-asia/taiwan-double-agent-gets-18-years-for-spying-for-china; "‹s—[fkqQÜŠHh: $RR18t^š[•‹ [*Wang Zongwu Gongdiean: Panxing 18 Nian Dingyan*] [Wang Tsung-Wu PRC Spy Case: Sentenced to 18 Years]," *Liberty Times,* April 2, 2017, accessed November 24, 2019, http://news.ltn.com.tw/news/focus/paper/1091006.
[106] Ibid.
[107] Ibid.
[108] Ibid.
[109] Ibid.
[110] Matthew Strong, "Taiwan Major General Suspected of Handing Missile Secrets to China," *Taiwan News,* May 9, 2017,

accessed November 24, 2019, https://www.taiwannews.com.tw/en/news/3159429.

[111] Jason Pan, "Second Suspect Investigated in Spy Case," *Taipei Times,* May 11, 2017, accessed November 24, 2019, http://www.taipeitimes.com/News/taiwan/archives/2017/05/11/2003670361.

[112] Ibid.

[113] Kamles Kumar, "Cops in Contact with Taiwan over Convicted China Spy," *Malay Mail Online,* September 23, 2016, accessed November 24, 2019, http://www.themalaymailonline.com/malaysia/article/cops-in-contact-with-taiwan-over-convicted-china-spy.

[114] *Affidavit of Special Agent Jason Levitt.*

[115] "Chinese Intelligence Officer Charged with Economic Espionage Involving Theft of Trade Secrets from Leading U.S. Aviation Companies," U.S. Department of Justice press release, October 10, 2018, accessed November 24, 2019, https://www.justice.gov/opa/pr/chinese-intelligence-officer-charged-economic-espionage-involving-theft-trade-secrets-leading; United States District Court for the Southern District of Ohio, *Grand Jury Indictment of Yanjun XU,* accessed November 24, 2019, https://www.justice.gov/opa/press-release/file/1099876/download; United States District Court for the Southern District of Ohio, *Affidavit of FBI Special Agent Bradley D. Hull,* https://www.justice.gov/opa/press-release/file/1099881/download.

[116] Ibid.

[117] Katie Benner, "Chinese Officer Is Extradited to U.S. to Face Charges of Economic Espionage," *The New York Times,* October 10, 2018, accessed November 24, 2019, https://www.nytimes.com/2018/10/10/us/politics/china-spy-espionage-arrest.html.

[118] United States District Court for the District of Utah, United States vs. Ron Rockwell Hansen, *Felony Complaint,* accessed November 24, 2019, https://www.justice.gov/opa/press-release/file/1068176/download; Mike Ives, "U.S. Army Veteran Tried to Spy for China, Officials Say," *The New York Times,* June 5, 2018, accessed November 24, 2019, https://www.nytimes.com/2018/06/05/world/asia/spy-arrest-china-ron-rockwell-hansen.html.

[119] Ibid.

[120] Ibid.

[121] Ibid.

[122] Ibid.

[123] "Northern California Resident Charged with Acting as an Illegal Agent," U.S. Department of Justice press release, September 30, 2019, accessed November 24, 2019, https://www.justice.gov/opa/pr/northern-california-resident-charged-acting-illegal-agent.

[124] United States District Court for the Northern District of California, United States vs. Xuehua PENG, *Affidavit of FBI Special Agent Spiro Fokas,* https://www.justice.gov/opa/press-release/file/1205776/download.

[125] Ibid.

[126] Ibid.

[127] Ibid.

[128] Mattis, "Chinese Intelligence Operations Reconsidered," 8.

[129] Nate Thayer, "China Spy," *The Asia Sentinel,* July 4, 2017, accessed November 24, 2019, https://www.asiasentinel.com/politics/china-spy/.

[130] Ibid.

[131] Ibid.

[132] Ibid.

[133] Ibid.

[134] Ibid.

[135] Edward Wong and Julian E. Barnes, "U.S. Secretly Expelled Chinese Officials Suspected of Spying after Breach of Military Base," *The New York Times*, December 15, 2019, accessed December 15, 2019.

[136] An alternative explanation of this incident advanced by some Taiwanese analysts portrays the Chinese officials as tourists who simply took a wrong turn and inadvertently stumbled into the military checkpoint. The Taiwanese analysts support this explanation by arguing that two Chinese couples were involved in the incident. If the Chinese intelligence services wanted to collect intelligence on the Norfolk base's security posture, why would they willingly compromise two Chinese diplomatic officials? One Chinese intelligence officer would be sufficient to carry out the operation. However, the timing of the incident, combined with the U.S. government's judgment that at least one of the officials was a Chinese intelligence officer operating under diplomatic cover, indicates that the incident was intentional, as a Chinese intelligence officer would not likely be involved otherwise. The other Chinese diplomatic couple may have been used as cover. Therefore, in the author's judgment, the alternative explanation above is unlikely. Author's discussion with Paul Huang, Taiwanese Independent Analyst, December 16, 2019, Arlington, VA.

[137] Ibid.

[138] Ibid.

[Author's Note: I would like to thank Peter Mattis and Kevin O'Connell for their mentorship and for taking the time to provide feedback on this article. All statements of fact, analysis, or opinion are the author's and do not reflect the official policy or position of the Department of Justice, Department of Homeland Security, Department of Defense, any of their components, or the U.S. government at large.]

Jimmy Zhang is a detailee in the Department of Homeland Security's Office of Counterterrorism Policy where he is exploring programmatic solutions to counter foreign adversaries and hostile nation states more effectively. Prior to joining DHS, he served in the Department of Justice's Office of International Affairs for two years where he helped coordinate and execute international extradition and mutual legal assistance requests to East Asian and West African countries. Outside of work, he is the Director of National Security Programs for Embolden, a non-profit organization providing tuition-free leadership and career development programs in business, journalism, and national security to high school students from low-income families and diverse communities in the Washington, DC, metropolitan area. He graduated Magna Cum Laude from the College of William and Mary, holds an MA degree in Security Studies from Georgetown University, and is currently pursuing another master's degree from an accredited Department of Defense institution.

Assessment of Analytical Models Used within the Cox Report — People's Republic of China

by Robert Budahl

INTRODUCTION

Although it was written over 20 years ago in 1999, the findings of the Cox Report are more relevant today than in 1999. In 1995 a "walk-in" operative divulged to the U.S. Intelligence Community the vast extent of the damage caused by espionage perpetrated by the Chinese. This included information and know-how on the W-88 nuclear warhead, which was the most advanced weapon the United States had at the time.[1] The Cox Report involved a comprehensive informational and damage assessment of the espionage conducted by the Chinese against the U.S.

Along with my findings pertinent to the Cox Report, in this article I discuss the relevant structured analytic techniques (SATs)[2] that intelligence agencies typically utilize to improve the quality of their intelligence and conclusions. The most common are structured brainstorming, key assumptions check, analysis of competing hypotheses, and indicators.

(1) Structured brainstorming—a group discussion process used for generating new ideas and concepts often used to kick off analysis of especially complex or controversial issues.
(2) Key assumptions check—a systematic effort to make explicit assumptions that guide an analyst's interpretation of evidence and reasoning about any particular problem.
(3) Analysis of competing hypotheses (ACH)—the identification of a complete set of alternative hypotheses, the systematic evaluation of each through the examination of evidence and data that applies to them all, and the selection of the most explanatory or best-fitting hypothesis (or hypotheses) by focusing on information that tends to disconfirm weaker hypotheses.
(4) Indicators—a pre-established set of observable phenomena that are periodically reviewed to help track events, spot emerging trends, and warn of unanticipated changes.

SATs provide analysts with clear, often step-by-step, guidance for conducting analysis of intelligence issues. By providing greater structure to the analytic process, they reduce subjectivity and add both rigor and transparency to analysis.[3]

During the 1970s and 1980s the U.S. held the belief that a strong and more advanced China was a countermeasure to Russia's influence.

There are three types of analytical models included within the CIA's *Tradecraft Primer* which include diagnostic methods, contrarian methods, and imaginative thinking.[4] Utilizing the intelligence agencies to the utmost provided the Cox Report with in-depth and relevant findings and recommendations. Within this article I describe the SATs, their use, and what benefit they may provide.

As new focus has again shifted to major power struggles,[5] the importance of maintaining technological superiority over our adversaries is crucial. During the 1970s and 1980s the U.S. held the belief that a strong and more advanced China was a countermeasure to Russia's influence.[6] The U.S. fostered and assisted China's military and technological modernization.[7] As detailed within the Cox Report, its espionage targeted against U.S. intelligence, defense, space, and other secrets now moves China closer to parity on thermonuclear warheads. It could begin producing advanced nuclear weapons in the next decade, which was first reported in 1999.[8] The Chinese are closing the gap in many systems and technological know-how. Can the U.S. now constrain China from achieving parity at this late stage of the latter's modernization, militarism, and new offensive capability?

The "Report of the Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China" details in depth the seriousness of the threat from the PRC regarding its targeting the intelligence, defense, and corporate sectors of the U.S. The PRC is shown to have achieved a great deal of success in

acquisition of technologies from the U.S. and through third countries/parties. Some of the examples, methods of analysis, and results are included in this article.[9]

Use of SATs has increased since the intelligence failures regarding WMD in Iraq. There has been a focus on qualitative and quantitative analysis to improve the accuracy of findings.

The Intelligence Community has increased the use of structured analytic techniques in an attempt to conduct rigorous analysis, reduce the failure of the intelligence produced, and improve transparency of the analysts' reasoning to the audience.[10] SATs are utilized to stimulate and organize thinking regarding the intelligence issue. They also provide an approach that specifically deals with a certain problem or issue.[11] In addition, SATs indicate the level of confidence one should have in his/her judgment. Use of SATs has increased since the intelligence failures regarding WMD in Iraq. There has been a focus on qualitative and quantitative analysis to improve the accuracy of findings.[12] I follow this with explanations and details of the espionage conducted by the PRC against the U.S. and how these methods may provide a guideline to follow in an analyst's intelligence assessment.

ASSESSMENT

Almost damaging event transpired during 1995 when a "walk-in" operative of the PRC presented design information on the W-88 nuclear warhead program, which is the U.S.'s most advanced nuclear weapon.[13] It is a MIRV (multiple independently targetable reentry vehicle) and is carried on the "Trident D-5" missile, which is deployed on submarines. It is highly destructive with multiple, individually targeted, nuclear warheads. The PRC operative also had information on a dozen or so U.S. nuclear warheads and reentry vehicles. Included in the information gleaned was design of a "neutron" or high-radiation nuclear device which subsequently has been tested by China. Also obtained was a secret record from the PRC on the D-5 missile and other nuclear warheads, and it stated that these were what the PRC should gauge their own weapons program against. In other words, it was clear the PRC was now competitive and moving from a defensive nuclear stance to a potential offensive one. These technological advances will put the PRC on par with the U.S., and the report estimated they could be emplaced within 10 years, bringing Chinese nuclear weapons into the next generation. The MIRV warheads greatly affect the effectiveness of defensive ICBM systems. High-performance computers are already within the PRC and their use magnifies the nuclear weapons program greatly as well as other aspects.[14]

Since the acquisition of the stolen technology from the U.S. labs, the PRC has established additional silo-based ICBMs which can target the U.S. It has been determined that the U.S. counterintelligence programs in place at the research labs fall short of effectively negating the threat.

"At the urging of the Cox panel, an assessment of the damage done by Chinese nuclear espionage was made by the U.S. intelligence community, which was subsequently reviewed by an independent panel led by retired Admiral David Jeremiah." Released on April 21, the Intelligence Community's damage assessment, with which the Jeremiah panel concurred, concluded that classified information obtained by China "probably accelerated its program to develop future nuclear weapons."[15] Nevertheless, the assessment concluded that, so far, Chinese nuclear espionage "has not resulted in any apparent modernization of their deployed strategic force or any new nuclear weapons deployment." While China had acquired "classified U.S. nuclear weapons information," the Intelligence Community assessment noted that "we do not know whether any weapon design documentation or blueprints were acquired."[16] This conclusion, based on information gleaned from the "walk-in" agent and assumptions made by intelligence officials, can be described as a predictive analytical method but also explanatory in nature. A conclusion was also made that the top secret national research laboratories had been compromised for as long as several decades and were probably still penetrated. The primary focus of intelligence gathering seemed to be centered on the well-known labs of Sandia, Lawrence Livermore, Los Alamos, and Oak Ridge. Since the acquisition of the stolen technology from the U.S. labs, the PRC has established additional silo-based ICBMs which can target the U.S. It has been determined that the U.S. counterintelligence programs in place at the research labs fall short of effectively negating the threat.[17]

Efforts have been increased since the Cox Report and other illuminating events that export policies have reduced U.S. transfer of technology, which may be militarily beneficial. Changes have been made in oversight of satellite licensing requirements which had aided the PRC, but now changes have been made with removal of oversight from the Commerce Department. We have to be well aware of dual-use technologies which the PRC will exploit to its advantage, if at all possible.[18]

ANALYSIS

An important element in successfully understanding the consequences and effects of the espionage committed by the PRC is that quality intelligence analysis is needed. It is the norm within intelligence to utilize structured analytic techniques. As explained by RAND, "The Intelligence Community (IC) is strongly emphasizing the use of structured analytic techniques (SATs) to promote rigorous analysis, lessen the risk of intelligence failure, and make analysts' reasoning more transparent to consumers."

A key part of reducing subjectivity in analysis requires identifying cognitive bias and reducing it. Chief among such biases often seen in intelligence analysis are:

> A. Confirmation bias—a tendency to search for or interpret information in ways that confirm preconceptions, preferences, and assumptions, while downplaying or discrediting alternative or less agreeable explanations that tend not to confirm the preferred explanation or interpretation of events.
> B. Mirror imaging—an inclination to assume that foreign leaders would behave pretty much as we imagine our own leaders would behave in similar circumstances, especially when the stakes are high if major errors are made in "rational" decision-making.
> C. Anchoring—a tendency to "anchor" analysis in the first or earliest important piece of information considered, so that later changes in judgments are typically small and rarely stray far from the initial judgment.
> D. Groupthink—a usually subconscious preference for group consensus favoring agreement among group members and subtly discouraging alternative views and interpretations, which are often seen as efforts to disrupt the consensus the other members desire."[19]

Debate often occurs, though, on whether or not it is worth the effort to implement SATs. However, the Intelligence Community has increased use of SATs after the debacle of the Iraq WMD case. The method I place the greatest value upon is ACH or analysis of competing hypotheses, although some studies have shown it only helps those who lack a professional intelligence background. One must consider that, even without using these methods, strong intuition-based perceptions at times can be effective should the operative be a seasoned professional.

Given the findings of the Cox Report, I recommend a manual based on the CIA *Tradecraft Primer,*[20] which details several analysis methods. One method suggested to be the beginning point in this analysis is described as a "key assumptions check." Also, an "analysis of competing hypotheses" safeguards against one single opinion or conclusion. Since the loss of top secret information has occurred, the intelligence services must determine damage assessment and possible outcome scenarios. The "high impact/low probability" is a contrarian method of analysis and may bring awareness to scenarios. China has long held a defensive military posture but with the information gained from the U.S. it can obtain an offensive strategic capability. Becoming offensive may seem unlikely to most observers. However, it presents the case that through a regime change the attitude becomes overtly militarily hostile toward the U.S. and contemplates a first-strike nuclear attack. By postulating the unthinkable it may bring out possible triggers and events that may give notice to a change of course. In this case, improving from a nuclear deterrent to full offensive systems is something that must be considered. Red-team analysis in some cases gives a perspective, but regarding the PRC it would not be beneficial as our cultures, government structures, political systems, and economic systems are so vastly different, unless we can utilize a very unorthodox free thinker.

There are three types of analytical methods:

> (1) Diagnostic methods attempt to formulate arguments, assumptions, or intelligence gaps.
> (2) Contrarian methods challenge the current thinking.
> (3) Imaginative thinking broadens the scope to try to reach insight or a different perspective.

In an explanation of analysis methods, which include the diagnostic method umbrella, is a "key assumptions" method which provides a quick insight to the scenario. The quality of information check does as it describes. Indicators of signpost of change watches behavior keep track of events, target monitoring, watching for emerging trends and alert of unanticipated change. Another method is ACH, in which alternative hypotheses are identified, which in turn can disconfirm instead of confirm the principal hypothesis.

Contrarian methods include "devil's advocacy." This questions a widely held belief. Team A/Team B uses separate teams to compare two different hypothesis. High impact/low probability brings attention to what would happen to policy if the unexpected were to occur. "What if" analytics assumes that a positive or negative event happened and examines its impact.

Imaginative thinking methods include "brainstorming," in which a group will try to come up with new ideas or scenarios. "Outside in" identifies forces, factors, and trends that indirectly form an issue. "Red-team" analytics involve trying to put one's self in the adversary's position and to think as it does. "Alternative futures analysis" is when the

situation does seem too complicated or not likely to occur; hence, alternative outcomes should be considered.[21]

Results: As a result of the Cox Report it is suggested:

1. The President brief Congress at least every six months.
2. The Department of Energy immediately institute a counterintelligence program.
3. Review the program to make sure it is successful.
4. Conduct a complete damage assessment of the actions completed by the PRC.
5. Legislate counterintelligence.
6. Hold a five-department assessment to see whether scientific exchange is a security/intelligence risk to the U.S.
7. Decide on whether or not the Department of Energy will remain in charge of nuclear weapons responsibility, which I hold it should.
8. Ensure compliance with the National Security Act.
9. Take the necessary international enforcement steps needed, including preventing Russia from providing nuclear weapons system knowledge to China.
10. Safeguard satellite launches.
11. Devise the appropriate policy on HPC (high-performance computers) so as to not allow military application.
12. Export legislation revision.[22] The findings within the Cox Report show the importance of sound logic and reasoning utilizing SATs to aid in the analysis of the subject matter.

CONCLUSION

The consequences of the acquisition of the vast amount of top secret information which China gleaned is staggering and the consequences may not be realized yet, but in the future we may face a direct threat resulting from the PRC advancing to the level of its nuclear posture becoming offensive rather than defensive. A very frightening, but possible, scenario is that should in the future the U.S. become involved in armed conflict or war with North Korea, China may assist or directly respond to or attack U.S. forces or the homeland. The policy in the 1970s and 1980s of using China as a buffer to Russia is now clearly shown to be a mistake. China may become the U.S.'s top adversary rather than Russia.

An example of the unthinkable is the premise of a "Thucydides Trap," which basically is a theory that emerging powers instill a sense of fear in the established power which may result in war. While the premises of this theory can be debated, the findings point to conditions in which war is avoidable and not inevitable. Now it is conceived that war is avoidable and not inevitable. However, research completed at Harvard University used 16 cases of emerging powers challenging established powers and in 12 of 16 cases war resulted. It is also theorized that nuclear weapons may have ended the possible consequences of a "Thucydides Trap." I do believe this is true.[2]

NOTES

[1] U.S. National Security and Military/Commercial Concerns with the People's Republic of China. (1999). Report of the Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China. Submitted by Mr. Cox of California, Chairman, 105th Congress, 2nd Session, House of Representatives, Report 105-851, January 3, 1999. Declassified May 25, 1999, pp. IV, 1-232. http://www.gpo.gov/fdsys/pkg/GPO-CRPT-105hrpt851/content-detail.html. Accessed September 7, 2018.

[2] Artner, Stephen, Richard S. Girven, and James Bruce, Assessing the Value of Structured Analytic Techniques in the U.S. Intelligence Community. Santa Monica, CA: RAND.

[3] Artner, Stephen, Richard S. Girven, and James Bruce, Assessing the Value of Structured Analytic Techniques in the U.S. Intelligence Community. Santa Monica, CA: RAND Corporation, 2016. https://www.rand.org/pubs/research_reports/RR1408.html, pp.1-3. Accessed September 9, 2018.

[4] *A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis* (2009). Prepared by U.S. Government. March, 2009, p. 1-38. Located on INTL409 D001Sum 18 Resources link. https://edge.apus.edu/portal/site/370402/tool/f0793a7f-a9c2-4982-8777-f516eb42ca56. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf. Accessed September 8, 2018, and July 23, 2019.

[5] Cancian, Mark F. 2018. Avoiding Coping with Surprises in Great Power Conflicts. Center for Strategic and International Studies. February 2018, p. 1. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180227_Cancian_CopingWith Surprise_wAppen_Web.pdf?0rD 0fcMI7gGXNLM1AYJWoVsNT_xSxOiu. Accessed July 27, 2019.

[6] Pollack, Jonathan D. 1999. "The Cox Report's 'dirty little secret'." *Arms Control Today* 29, no. 3: 26-27+, https://search-proquest-com.ezproxy2.apus.edu/docview/211219435?accountid=8289.

[7] Pollack, Jonathan D. 1999. "The Cox Report's 'dirty little secret'." *Arms Control Today* 29, no. 3: 26-27+, https://search-proquest-com.ezproxy2.apus.edu/docview/211219435?accountid=8289. Accessed uly 27, 2019.

[8] U.S. National Security and Military/Commercial Concerns with the People's Republic of China. (1999). Report of the Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China. Submitted by Mr. Cox of California, Chairman, 105th Congress, 2nd Session, House of Representatives, Report 105-851, January 3, 1999. Declassified May 25, 1999, pp. IV, 62, 1-232. http://www.gpo.gov/fdsys/pkg/GPO-CRPT-105hrpt851/content-detail.html. Accessed September 7, 2018.

[9] U.S. National Security and Military/Commercial Concerns with the People's Republic of China. (1999). Report of the Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China. Submitted by Mr.

Cox of California, Chairman, 105th Congress, 2nd Session, House of Representatives, Report 105-851, January 3, 1999. Declassified May 25, 1999, pp. III, 1-232. http://www.gpo.gov/fdsys/pkg/GPO-CRPT-105hrpt851/content-detail.html. Accessed September 7, 2018.

[10] Artner, Stephen, Richard S. Girven, and James Bruce, Assessing the Value of Structured Analytic Techniques in the U.S. Intelligence Community. Santa Monica, CA: RAND Corporation, 2016. https://www.rand.org/pubs/research_reports/RR1408.html. pp.1-3. Accessed September 9, 2018, and July 27, 2019.

[11] Artner, Stephen, Richard S. Girven, and James Bruce, Assessing the Value of Structured Analytic Techniques in the U.S. Intelligence Community. Santa Monica, CA: RAND Corporation, 2016. https://www.rand.org/pubs/research_reports/RR1408.html. P.1-3. Accessed September 9, 2018, and July 27, 2019. p. 2.

[12] Artner, Stephen, Richard S. Girven, and James Bruce, Assessing the Value of Structured Analytic Techniques in the U.S. Intelligence Community. Santa Monica, CA: RAND Corporation, 2016. https://www.rand.org/pubs/research_reports/RR1408.html. pp.1-3, 3. Accessed September 9, 2018, and July 27, 2019.

[13] U.S. National Security and Military/Commercial Concerns with the People's Republic of China. (1999). Report of the Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China. Submitted by Mr. Cox of California, Chairman, 105th Congress, 2nd Session, House of Representatives, Report 105-851, January 3, 1999. Declassified May 25, 1999, pp. IV, 1-232. http://www.gpo.gov/fdsys/pkg/GPO-CRPT-105hrpt851/content-detail.html. Accessed September 7, 2018.

[14] U.S. National Security and Military/Commercial Concerns with the People's Republic of China. (1999). Report of the Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China. Submitted by Mr. Cox of California, Chairman, 105th Congress, 2nd Session, House of Representatives, Report 105-851, January 3, 1999. Declassified May 25, 1999, pp. XXIX, 1-232. http://www.gpo.gov/fdsys/pkg/GPO-CRPT-105hrpt851/content-detail.html. Accessed September 7, 2018.

[15] U.S. National Security and Military/Commercial Concerns with the People's Republic of China. (1999). Report of the Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China. Submitted by Mr. Cox of California, Chairman, 105th Congress, 2nd Session, House of Representatives, Report 105-851, January 3, 1999. Declassified May 25, 1999, pp. IV, 1-232. http://www.gpo.gov/fdsys/pkg/GPO-CRPT-105hrpt851/content-detail.html. Accessed September 7, 2018.

[15] Diamond, Howard. 1999. "Cox panel charges China with extensive nuclear espionage." *Arms Control Today* 29, no. 3: pp. 37, 48. https://search-proquest-com.ezproxy2.apus.edu/docview/211230803?accountid=8289. Accessed September 8, 2018.

[16] "Cox Report overview." 1999. *Arms Control Today* 29, no. 3: 17-22. https://search-proquest-com.ezproxy1.apus.edu/docview/211230568?accountid=8289, p. 18. Accessed September 8, 2018.

[17] U.S. National Security and Military/Commercial Concerns with the People's Republic of China. (1999). Report of the Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China. Submitted by Mr. Cox of California, Chairman, 105th Congress, 2nd Session, House of Representatives, Report 105-851, p. XXVII, 1-232. January 3, 1999. Declassified May 25, 1999. http://www.gpo.gov/fdsys/pkg/GPO-CRPT-105hrpt851/content-detail.html. Accessed September 7, 2018.

[18] Artner, Stephen, Richard S. Girven, and James Bruce, Assessing the Value of Structured Analytic Techniques in the U.S. Intelligence Community. Santa Monica, CA: RAND Corporation, 2016. https://www.rand.org/pubs/research_reports/RR1408.html, pp. 1-2. Accessed September 9, 2018.

[19] *A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis*. (2009). Prepared by U.S. Government. March, 2009, pp. 1-38. Located on INTL409 D001 Sum 18 Resources link. https://edge.apus.edu/portal/site/370402/tool/f0793a7f-a9c2-4982-8777-f516eb42ca56. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf. Accessed September 8, 2018, and July 23, 2019.

[20] *A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis* (2009). Prepared by U.S. Government March, 2009, pp. 1-38. Located on INTL409 D001 Sum 18 Resources link. https://edge.apus.edu/portal/site/370402/tool/f0793a7f-a9c2-4982-8777-f516eb42ca56. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf. Accessed September 8, 2018, and July 23, 2019.

[21] U.S. National Security and Military/Commercial Concerns with the People's Republic of China. (1999). Report of the Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China. Submitted by Mr. Cox of California, Chairman, 105th Congress, 2nd Session, House of Representatives, Report 105-851, January 3, 1999. Declassified May 25, 1999, pp. 166-177, 1-232. http://www.gpo.gov/fdsys/pkg/GPO-CRPT-105hrpt851/content-detail.html. Accessed September 7, 2018.

[22] Bulkeley, Emily. 2017. "Destined for War: Can America and China Escape Thucydides's Trap?" *Washington Journal of Modern China* 13 (September): 122-124. http://search.ebscohost.com.ezproxy2.apus.edu/login.aspx?direct=true&AuthType=ip&db=aph&AN=131014544&site=ehost-live&scope=site, pp.122, 123. Accessed July 27, 2019.

Robert Budahl graduated in 2019 from American Military University with the designation Omicron Sigma Sigma *in the Counterintelligence certificate program. That same year he was inducted into the Order of the Sword and Shield National Honor Society. In 2005 he earned a BA degree from Bethel University and in 2001 graduated from Colorado State University-Pueblo with a Paralegal Studies certificate. He is currently licensed in real estate and affiliated with a firm in Reston, Virginia. He is also a licensed life and health insurance provider. Previously, he managed a bank in Las Vegas and was a financial associate, team leader, and security/fraud investigator. In 2017 Bob received a life-saving liver transplant and now is enjoying good health while actively pursuing a career in a new field.*

Examining Narratives on Chinese Strategic Ambitions

by MAJ (USA) Alex F. Oliver

INTRODUCTION

Over the course of the past 20 years, the People's Republic of China has undergone a transformation from an inwardly-focused emerging economy to a great power rivaling the United States. China's economy has grown at an average real annual rate of 9.5 percent since 1979, which has contributed to 800 million Chinese rising from poverty.[1] Observers, particularly in the West, speculate with trepidation that China will seek to dominate the international geopolitical system. John Mearsheimer, among other experts, depicts such dominance as an imperative rather than a choice.[2] In contrast, the Constructivist school of international relations (IR) theory rejects the notion that China (or any actor) is compelled by structural power dynamics to pursue specific interests or exhibit specific behaviors, and are instead guided in action by their shared understanding of themselves and the world around them—their identity.[3] This article attempts to determine: *What elements of Chinese identity are most relevant to the understanding of China's strategic ambitions?*

The primary contention of this article is that China's view of its role in the world is influenced by competing, and sometimes conflicting, narratives that cast it as an aggrieved victim of Western colonialism, a culturally superior ancient civilization, a repressive authoritarian regime with profound inequity, and global economic power generating prosperity domestically and, through trade, around the world. The extent to which each of these narratives, or combination of narratives, about China's past and present prevails in the discourse will undoubtedly shape how China proceeds in the future. This article concludes that, when China focuses on its rich history and economic potential, it tends toward cooperation. On the contrary, when it focuses on past misdeeds and current critiques of its authoritarian regime, it tends toward competition (and potentially hostility). This is in line with the sentiment and conclusions of Chinese academic Yong Deng.[4]

This article proceeds in two directions. First, the author briefly reviews the important theoretical arguments of Constructivism, in particular the sources of identity formation. Then the author examines three primary areas for evidence of Chinese identity formation; history and culture, elite rhetoric, and external discourse. In a brief conclusion, the author proposes a range of future trajectories for China, based on the prevailing narratives about its past and present. The goal of this article is simply to propose a framework for analysis. Future work could apply methods such as content and discourse analysis to determine the relative prevalence of each narrative—an endeavor of much greater depth.

THE FORMATION OF IDENTITY IN CONSTRUCTIVIST THEORY

This article examines three primary sources for evidence of China's collective identity: First and foremost, from the history and culture of the society; second, from the rhetoric of national leaders, who often draw on symbols and events important in the national culture; and finally from the perceptions and behaviors of outside actors, because external discourse about China very much impacts the state's image of itself.

Broadly defined, *cultures* are "collectively held ideas, beliefs, and norms."[5] There are several cultural categories, including political, organizational, and strategic cultures. Critics argue that this broad epistemology challenges operationalization for empirical study but, for the purposes of this analysis, a broad definition of culture helps ensure a full appreciation of the evidence available. Because identity formation is a process that is iterative in nature over time, events in an actor's history and the shared meaning of those events with other actors evolve. Peter Katzenstein argues that the prevailing domestic attitude of a society will affect the state's preferences regarding the use of national power.[6] Alternatively, Martha Finnemore argues that global norms, through the process of socialization, constrain and indoctrinate states into normative convention.[7] Put another way, states tend to adhere to international norms, or attempt to rationalize or conceal when they deviate. In the context of strategic decision making, Alastair Johnston argues that national security elites do not always exhibit pure rationality, and that their shared notions about the role of war in interstate relations and its efficacy form a strategic culture.[8]

Jutta Weldes argues that elites have a particularly important role to play in steering the discourse on national identity. In particular, Weldes points to the importance leaders place on historic symbols and analogies as indicators of the direction in which they are steering the country.[9] One might imagine that elite rhetoric would be particularly impactful in a society, such as China, where individual freedom of the press is so heavily curtailed and the CCP has an outsized voice compared to countries with a free press.

To appreciate fully the trajectory of Chinese identity we need to consider also the way other states treat China.

No discussion of identity formation is complete without considering the perceptions of *the other*. As discussed above, the process of identity formation is *intersubjective*, meaning it is derived from the perceptions of all participants. As Alexander Wendt states, it is these relationships "which structure the interactions" between actors.[10] Put another way, again by Wendt, it "is collective meanings that constitute the structures which organize our actions."[11] This means to appreciate fully the trajectory of Chinese identity we need to consider also the way other states treat China.

The preceding section briefly explained three sources from which nation-states derive collective identity provided in the literature. The literature on this topic is vast, and this summary is deliberately reductionist. The next section will use these criteria to find evidence for a better understanding of Chinese identity.

EVIDENCE OF CHINESE IDENTITY

The Chinese culture is complex; China's national history is long. These facts are constituent in the Chinese identity in and of themselves, but also serve to complicate crafting a parsimonious description of Chinese identity. As William Callahan notes, "To understand China's present and future" authors look to the past, "[but] which past?"[12]

China, as Henry Kissinger explains, does not view itself as a country that was *founded,* like the United States in 1776. In Chinese historical lore, it is a constant: something that always was—*Eternal China.* In dynastic history, spanning centuries, China conceives of itself as *Zhong Guo,* or the Middle Kingdom: the place where heaven meets earth. For centuries, this is how China conceived of relations with those beyond its environs—as vassals who paid tribute to the closest earthly point to the divine. Martin Jacques, in his widely read *When China Rules the World*, contends that this tributary system ("Tianxia") is China's preferred international order, and China's rise portends the demise of the Westphalian system with it, a notion that others dispute.[13] Today, Chinese foreign policy experts characterize this concept as a "benevolent" China bringing harmony and civilization to the world.[14] This Sino-centric sense of cultural superiority pervaded even through invasions and occupations in its early history, when Chinese doctrine was to absorb and assimilate, and ultimately enlighten, the "barbarian" invaders.[15]

The Tianxia approach to foreign relations served many dynasties of China well, until it encountered the West. Initially treating Western diplomats and emissaries as vassals seeking to pay tribute, with little to offer China culturally, technologically, or otherwise, China realized too late that the West had the coercive capability to exert its will even from as far afield as Europe. It was China's unwillingness to recognize the military and technological superiority of the West that led to the Opium Wars of the 1860s, which resulted in colonial occupation and subjugation of parts of China, and essentially an end to the ancient Middle Kingdom paradigm.[16] Thus began the Century of Humiliation, which many argue pervades the modern Chinese mind with distrust and resentment of the West.[17]

It was China's unwillingness to recognize the military and technological superiority of the West that led to the Opium Wars of the 1860s, which resulted in colonial occupation and subjugation of parts of China, and essentially an end to the ancient Middle Kingdom paradigm.

Determined to emerge from the "Century of Humiliation," Mao Zedong set forth to rejuvenate China when he took power. The impact of Mao and his communist Cultural Revolution on Chinese identity in the post-war era cannot be understated. The conventional wisdom is that Mao's legacy in China is one of domestic populism. Programs such as the Great Leap Forward and the Cultural Revolution caused such domestic upheaval and strife that they are simultaneously credited with stifling and spurring structural change. Unlike dynastic and colonial China, the tribulations of the Mao era had a direct formative impact on today's Chinese Communist Party (CCP) elites, sometimes referred to as the fifth generation of leaders. For example, about a quarter of current Politburo members received education during the Cultural Revolution which was curtailed or otherwise disrupted, including Xi Jinping himself.[18] Having traced the important events and symbols of China's past—a key to

understanding Chinese identity—this article examines how Chinese leaders' rhetoric co-opt and evoke these events and symbols.

The rhetoric of this generation of leaders, in particular President Xi, is the second source of insight into Chinese identity. In China, as in many authoritarian states, individual leaders carry great power, particularly with regard to foreign relations. Lucian Pye notes that the "Confucian tradition of rule by men…and the Marxist-Leninist doctrine of the preciousness of the Party, when combined…have produced a heightened glorification of the concept of the infallible leader, the indispensable figure."[19] At the moment, and for the foreseeable future, Xi is that figure.

The overall tenor of Xi's discourse, with descriptors such as "national rejuvenation," raises the prospect that China is operating from a desire to restore past injustices.

Xi Jinping's public commentary of China's core interests has expanded substantially from his predecessor's, reflecting the more assertive and confident identity of China as a rising global power. The overall tenor of Xi's discourse, with descriptors such as "national rejuvenation," raises the prospect that China is operating from a desire to restore past injustices. Avery Goldstein recognizes that references to the Century of Humiliation have diminished from CCP official discourse in the "last decade" while also contending that the real or perceived injustices of the past by the West remain explanatory in China's security mindset.[20] Still, themes of national restoration and empowerment through all means, including violence, continue to feature prominently in Xi's rhetoric.[21]

At the same time, Xi claims that hegemony is not China's ambition (though one might suspect it would not be politic to admit if it were).[22] At times, Chinese leaders go to great pains to soften their rhetoric, emphasizing China's peaceful ambitions. For example, State Council Information Officer Wang Guoqing said, "Our top agenda [item] is to…tell China's story and help the international community understand China."[23] Elites have claimed that China's goal is not coercion, but "win-win" cooperation, rooted in mutual gains.[24] Therefore, as with history, elite rhetoric is split between fiery calls for a return to glory and more measured discussion of China leading the world to prosperity. However, the world has things to say about China, too.

Chengxin Pan argues that the way in which Western policymakers and scholars characterize China is not an exercise in the objective description of reality but a "normative, meaning-giving practice" that can turn fears of the "China Threat" into a socially constructed reality.[25] Much of the discourse around China, in terms of its meteoric economic rise, focuses on the potential of an accompanying security challenge for other countries.[26] In addition to material capability, some authors selectively point to turbulent periods of Chinese history as evidence of future hostile proclivity.[27] Still other Western observers claim there are intrinsic ethnic and cultural reasons for hostility, such as China's relatively ethnic homogeneity.[28]

By contrast, Western scholarship with a positive outlook on China (sometimes under the moniker "peaceful China rising") is less available and more nuanced. Some scholars base their positive outlook on their personal experiences. One well-known example is *On China*, by Henry Kissinger, which covers the breadth of Chinese history (not including the Xi Jinping era), but focuses on the period of the U.S. opening to China, in which he played a large part. Thematic in Kissinger's book is the potential present in China, and the hope of individual Chinese leaders such as Zhou Enlai.[29] Other scholars take a more empirical approach, arguing that the costs of militarism far outweigh the potential benefits of additional territorial gains.[30] Still other China watchers look at precedent, arguing that since its emergence as a nation-state China has worked within the rules-based international order, and that incentives exist for China to continue to do so.[31] In sum, as with history and elite rhetoric, the view of China from the outside is mixed between fear and optimism.

This section presented three perspectives of the impact of Chinese identity on its strategic ambitions. The evidence gathered provides conflicting views of China's history, the current system state, and China's ambitions. The next section considers the evidence and offers a model for thinking about China's future trajectory.

IMAGINING (AND IMAGING) CHINA'S TRAJECTORY

This article set out to determine which element(s) of Chinese identity might be important in understanding China's strategic ambitions for its role in the world. The evidence has shown that there are dichotomies in the prevailing views of both China's past and present. I propose that using these viewpoints as polemics provides some structure to imagine how a range of ambitions for the future might look. This is not an alternative futures analysis, and these models are not intended to be predictive—they are intended to help articulate the narrative about Chinese identity as it relates to strategic ambitions.

Prevailing Perspective in Historical Narrative			
Prevailing Perspective on Current Behavior		Century of Humiliation	Middle Kingdom
	Insular Autocracy	Mao's Legacy	Win-Win'ism
	Emerging Superpower	China Rising (China Threat?)	China Dream

Figure – Framing Future Identity Based on Perceptions of Past and Present

Mao's Legacy. The colonial occupation that resulted from the 19th century Opium Wars, at the onset of the Century of Humiliation, is still highly visible in China today. One example of this is visible through the "one country, two systems" regime in Hong Kong.[32] This allows Hong Kong to administer justice in accordance with its own legal system and to vote for political representation. The CCP views these vestiges of colonialism as a threat and is committed to eliminating them over time.[33] This campaign to homogenize and purge Western influence is very reminiscent of Mao's Cultural Revolution where any symbol not consistent with communist ideals was destroyed. If we carry this image of Chinese identity into the future, one might imagine a scenario in which the CCP grows ever less tolerant of not just Hong Kong but any non-Han, non-communist ethnic or political discourse in China, and even less tolerant of the diffusion of Western cultural symbols in Chinese society.

When China feels that its pursuit of economic prosperity is threatened, or impeded, it tends to take measures to secure those interests militarily.

China Rising (China Threat). It is unlikely, though, that China will remain focused internally under Xi Jinping. China's need for natural resources, and access to markets, is central to Xi's plan for a "moderately prosperous society" by 2020.[34] When China feels that its pursuit of economic prosperity is threatened, or impeded, it tends to take measures to secure those interests militarily. For example, China has established overseas military installations, contributed to peacekeeping (not traditionally favored by the CCP), and conducted non-combatant evacuations, all arguably tied to securing international commerce.[35] This foreshadows China adopting a neo-imperialist approach, albeit somewhat constrained by modern institutions and norms surrounding sovereignty.[36] Carried forward, this is the worst scenario for China, and the world. When China views itself as surrounded and under threat once again from its former colonial overlords, prospects for cooperation dwindle and the security dilemma becomes most prominent.

Win-Win'ism. When China focuses on mutual, rather than absolute gains, and cooperation rather than pure competition, Chinese rhetoric reflects a more positive tone. The concept of "win-win" economic development has featured prominently in the Chinese public branding.[37] This concept is born out of traditional, Middle Kingdom-era Chinese principles of external non-interference and respect for the sovereignty of other states. The phrase carries the connotation that trade and cooperation is not connected to domestic reform, a direct juxtaposition to U.S. policy that often makes trade and economic development assistance contingent on governance or civil liberties reform. Carrying this image forward, one can imagine a fairly palatable future in which China, while not necessarily doing much to support the proliferation of human rights and democracy, is engaging in the world where it feels there is value to be had. This is perhaps the most beneficial frame from the U.S. perspective.

China Dream. At the opening of the 19th Communist Party Congress, Xi Jinping announced that "to achieve great dreams there must be a great struggle."[38] Xi clearly envisions the path to great power status, and symbols of the Middle Kingdom within his national rejuvenation rhetoric abound.[39] The principal distinction between this narrative, and the China Rising narrative discussed above, is that there is substantially less emphasis on correcting past misdeeds, and on Chinese victimization, and more focus on assuming China's "rightful" place at the center of the international order. Chinese leaders and

academics claim that China will be a "new type of superpower," which seeks to cooperate with, not supplant, the United States.[40] This image most clearly aligns with China's ideal-type international order—Tianxia—and is probably the most preferable from a Chinese perspective. Carrying this image forward to the future, one might imagine a world in which China leads an orderly and cooperative Asia-Pacific region, and has influence and reach in Africa, the Middle East, and potentially even South America.

The world must recognize that vilifying and attempting to isolate China only serves to exacerbate China's own fears about the world.

The four images, or frames, presented above are not discreet or mutually exclusive. They exist together, often in conflict, sometimes in unison. This article argues that when the narrative of one image dominates over the others, it will affect the subjectively shared meaning of Chinese identity in China, and throughout the world. The world must recognize that vilifying and attempting to isolate China only serves to exacerbate China's own fears about the world. China, for its part, must go beyond rhetoric in reassuring the international community that its pursuit of prosperity is benign in the sense that it will occur within the confines of the existing rules-based international order.

NOTES

[1] Wayne M Morrison, "China's Economic Rise: History, Trends, Challenges, and Implications for the United States," Congressional Research Service (February 5, 2018): i.

[2] John J. Mearsheimer, *The Tragedy of Great Power Politics* (New York: Norton, 2001), 402.

[3] Ted Hopf, "The Promise of Constructivism in International Relations Theory," *International Security* 23, no. 1 (1998): 173, accessed January 27, 2020, www.jstor.org/stable/2539267.

[4] Yong Deng, "The Chinese Conception of National Interests in International Relations," *The China Quarterly*, no. 154 (1998): 308-311, 328, http://www.jstor.org/stable/655893.

[5] Michael C. Desch, "Culture Clash: Assessing the Importance of Ideas in Security Studies," *International Security* 23, no. 1 (1998): 151, accessed January 28, 2020, www.jstor.org/stable/2539266.

[6] Peter J. Katzenstein, "Norms and the Japanese State," in *Cultural Norms and National Security: Police and Military in Postwar Japan* (Ithaca, NY: Cornell University Press, 1996), 33-58, accessed January 28, 2020, www.jstor.org/stable/10.7591/j.ctv5rdzdm.7.

[7] Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," *International Organization* 52, no. 4 (1998): 896, accessed January 27, 2020, https://www.cambridge.org/core/product/identifier/S0020818398440608/type/journal_article.

[8] Alastair Iain Johnston, "Thinking about Strategic Culture," *International Security* 19, no. 4 (1995): 46, accessed January 28, 2020, www.jstor.org/stable/2539119.

[9] Jutta Weldes, *Cultures of Insecurity: States, Communities, and the Production of Danger* (Minneapolis: University of Minnesota Press, 1999), 10-11. Cited in Hoyoon Jung, "The Evolution of Social Constructivism in Political Science: Past to Present," *SAGE Open* 9, no. 1 (January 1, 2019), accessed November 5, 2019, https://doi.org/10.1177/2158244019832703.

[10] (U) Alexander E. Wendt, "The Agent-Structure Problem in International Relations Theory," *International Organization* 41, no. 3 (1987): 338, accessed January 27, 2020, www.jstor.org/stable/2706749.

[11] (U) Alexander E. Wendt, "Anarchy Is What States Make of It: The Social Construction of Power Politics," *International Organization* 46, no. 2 (1992): 397.

[12] William A. Callahan, "Sino-Speak: Chinese Exceptionalism and the Politics of History," *The Journal of Asian Studies* 71, no. 1 (2012): 43, http://www.jstor.org.proxyaua.wrlc.org/stable/41350049.

[13] Ibid., 37.

[14] Yan Xuetong, "The Rise of China in Chinese Eyes," *Journal of Contemporary China* 10, no. 26 (February 2001): 33-39, http://search.ebscohost.com/login.aspx?direct=true&db=a2h&AN=4009301&site=ehost-live.

[15] Henry Kissinger, *On China* (London: Penguin Books Limited, 2011), 51-56. As Callahan notes, Kissinger and others tend to offer a selective recollection of Chinese history to support their accounts, omitting important counterfactual events, such as the Qing Dynasty's extermination (rather than assimilation) of the Mongols. See Callahan, "Sino-Speak: Chinese Exceptionalism and the Politics of History," 42.

[16] Kissinger, *On China*, 45-48.

[17] For example, Matt Schiavenza, "How Humiliation Drove Modern Chinese History," *The Atlantic*, last modified October 25, 2013, https://www.theatlantic.com/china/archive/2013/10/how-humiliation-drove-modern-chinese-history/280878/, and David Shambaugh, *China Goes Global: The Partial Power* (Cary, NC: Oxford University Press, 2013), 17, http://ebookcentral.proquest.com/lib/dialibrary-ebooks/detail.action?docID=1113182.

[18] Bo Zhiyue, "China's Fifth Generation Leaders: Characteristics of the New Elite and Pathways to Leadership," in *China in the Era of Xi Jinping: Domestic and Foreign Policy Challenges*, eds. Robert S. Ross and Jo Inge Bekkevold (Washington, DC: Georgetown University Press, 2016), 8-9.

[19] Lucian W. Pye, *The Mandarin and the Cadre: China's Political Cultures*, Michigan Monographs on Chinese Studies 59 (Ann Arbor: University of Michigan Press, 1988), 135. Cited in Benjamin Ho, "Understanding Chinese Exceptionalism: China's Rise, Its Goodness, and Greatness," *Alternatives: Global, Local, Political* 39, no. 3 (2014): 169, http://www.jstor.org.proxyaua.wrlc.org/stable/24569474.

[20] Avery Goldstein, "Parsing China's Rise: International Circumstances and National Attributes," in *China's Ascent: Power, Security, and the Future of International Politics*, eds. Robert S. Ross and Zhu Feng, Cornell Studies in Security Affairs (Ithaca, NY: Cornell University Press, 2008), 75.

[21] Jamie Fullerton, "Xi Jinping Says China Willing to Fight 'Bloody Battle' to Regain Rightful Place in the World, in Blistering Nationalist Speech," *The Telegraph*, March 20, 2018, accessed September 29, 2019, https://www.telegraph.co.uk/news/2018/03/20/xi-jinping-says-china-willing-fight-bloody-battle-regain-rightful/.
[22] Xi Jinping, "Speech in Nazarbayez University, Kazakhstan," 2013; Katherine Wong, "'Cooperate or Stop Criticising', China Says as Belt and Road Summit Nears," *South China Morning Post*, last modified April 19, 2019, accessed November 18, 2019, https://www.scmp.com/news/china/diplomacy/article/3006893/cooperate-or-stop-criticising-chinas-foreign-minister-wang-yi.
[23] Shambaugh, *China Goes Global: The Partial Power*, 11, 21.
[24] Angang Hu, "The Belt and Road: Revolution of Economic Geography and the Era of Win-Winism," in *China's Belt and Road Initiatives: Economic Geography Reformation*, 2018, 15-32.
[25] Chengxin Pan, "The 'China Threat' in American Self-Imagination: The Discursive Construction of Other as Power Politics," *Alternatives* 29, no. 3 (June 1, 2004): 308, accessed January 27, 2020, https://doi.org/10.1177/030437540402900304.
[26] See, for example, the central premise of Allison's argument, based largely on Power Transition theory, which casts competition between rising powers and status quo powers as an inevitable occurrence that more often than not results in conflict. Graham T. Allison, *Destined for War: Can America and China Escape Thucydides's Trap?* (New York: Houghton Mifflin Harcourt, 2017).
[27] See, for example, the historical analogy threaded throughout Pillsbury's argument, which compares modern Chinese decision making to the maxims of the Warring States period of Chinese history. Michael Pillsbury, *The Hundred-Year Marathon: China's Secret Strategy to Replace America as the Global Superpower* (Washington, DC: Griffin, 2016).
[28] Warren I. Cohen, "America's Response to China: An Interpretative History of Sino-American Relations," *The American Historical Review* (1972): 3. Cited in Pan, "The 'China Threat' in American Self-Imagination: The Discursive Construction of Other as Power Politics," 309. See also, for example, the intractable conflict of cultures thematic in Samuel P. Huntington, "The Clash of Civilizations?" *Foreign Affairs* 72, no. 3 (January 1993): 22-49.
[29] Kissinger, *On China*.
[30] M. Taylor Fravel, "International Relations Theory and China's Rise: Assessing China's Potential for Territorial Expansion," *International Studies Review* 12, no. 4 (2010): 507, http://www.jstor.org/stable/40931355.
[31] Alastair Iain Johnston, "Is China a Status Quo Power?" *International Security* 27, no. 4 (2003): 5-56, http://www.jstor.org/stable/4137603.
[32] Ming K. Chan, "The Challenges of 'One Country, Two Systems' Disequilibrium in China's Hong Kong SAR, 1997-2017," *Chinese Law & Government* 50, no. 1 (January 2, 2018): 8, https://doi.org/10.1080/00094609.2018.1445337.
[33] Mark Sharp, "What Colonial Symbols Might They Target after Hong Kong's Royal Postboxes?" *South China Morning Post*, last modified October 13, 2015, accessed January 30, 2020, https://www.scmp.com/lifestyle/article/1866866/what-colonial-symbols-might-they-target-after-hong-kongs-royal-postboxes.
[34] Jo Kim, "So Much for a Rough Year: China Is Set to Achieve Its First Centennial Goal in 2020," *The Diplomat*, accessed January 30, 2020, https://thediplomat.com/2020/01/so-much-for-a-rough-year-china-is-set-to-achieve-its-first-centennial-goal-in-2020/.
[35] Patricia Kim, "Understanding China's Military Expansion," Hearing on China's Worldwide Military Expansion, 2018, accessed January 30, 2020, https://www.pacificcouncil.org/newsroom/understanding-china%E2%80%99s-military-expansion; Joel Wuthnow, *Securing China's Belt and Road Initiative: Dimensions and Implications* (Washington, DC, 2018), accessed September 8, 2019, https://www.uscc.gov/sites/default/files/Wuthnow_USCC%20Testimony_20180123.pdf.
[36] Anthony Kleven, "Belt and Road: Colonialism with Chinese Characteristics," The Lowery Institute, last modified May 6, 2019, accessed January 30, 2020, https://www.lowyinstitute.org/the-interpreter/belt-and-road-colonialism-chinese-characteristics.
[37] Brenda Goh and Ryan Woo, "China President Xi Says Goal of Belt and Road Is Advance 'Win-Win Cooperation,'" *Reuters*, last modified April 25, 2019, accessed January 30, 2020, https://www.reuters.com/article/us-china-silkroad-xi/china-president-xi-says-goal-of-belt-and-road-is-advance-win-win-cooperation-idUSKCN1S205Z.
[38] Charlie Campbell, "China's Xi Jinping Vows 'National Rejuvenation' at Congress," *Time*, October 18, 2017, accessed January 30, 2020, https://time.com/4986999/xi-jinping-china-19th-congress-ccp/.
[39] Daniel Blumenthal, "The Unpredictable Rise of China," *The Atlantic*, last modified February 3, 2019, accessed January 30, 2020, https://www.theatlantic.com/ideas/archive/2019/02/how-americans-misunderstand-chinas-ambitions/581869/.
[40] Cheng Li, "Introduction: A Champion for Chinese Optimism and Exceptionalism," Brookings Institution, xix, accessed November 21, 2019, https://www.brookings.edu/wp-content/uploads/2016/07/chinain2020_chapter.pdf.

MAJ (USA) Alex F. Oliver is a member of the Military Intelligence branch. He is currently assigned as an autonomous systems program manager at the Defense Innovation Unit in Silicon Valley, California. His previous assignments include a variety of units within the U.S. Special Operations Command and the Intelligence Community. In addition to a Master of Science of Strategic Intelligence degree from NIU, which he was awarded in 2020, he holds an MA in International Relations from American University's School of International Service. Alex graduated with distinction from the Virginia Military Institute in 2009.

The Paradox of Asymmetric Deterrence

by Samuel S. Chi

Untethered from the rational choice moorings of its Cold War theory, deterrence is experiencing a renaissance.[1] With the more belligerent Russia and the continuing ascendance of China as a strategic competitor, the three-way standoff between the United States (U.S.) and its near-peer nuclear armed rivals has garnered much attention. Yet, the focus on this trio risks ignoring the strategic implications of smaller nation-states and non-state actors that seek to obtain weapons of mass destruction (WMD). Smaller regional powers, aspiring states,[2] and non-state actors are increasingly seeing WMD as a force equalizer. Their apparent willingness to threaten to use WMD (and in some cases actually use them), destabilizes global strategic security.[3] Against this backdrop, it is unclear how effective traditional deterrence practices will fare against aspiring state and non-state actors who seek to pursue or even flaunt WMD capabilities.

Smaller regional powers, aspiring states, and non-state actors are increasingly seeing WMD as a force equalizer.

In some ways, these smaller entities pose an enhanced threat to U.S. security and international stability because their relative weakness makes them more likely than traditional powers to construct, spread, acquire, and use WMD. Despite the disparity in apparent power and military capability, the relationship between an established major power and smaller entities reveals a paradoxical deterrence dynamic. Ostensibly the larger, more powerful nation-state should be able to deter the smaller, seemingly weaker entity; yet, larger nation-states seem to fail to deter weaker ones from acquiring or outfitting WMD. More often, the stronger power appears to be deterred by the weaker one. In these asymmetric deterrence relationships, the presence of WMD (especially nuclear weapons) serves as a confounding factor. The apparent success of these asymmetric deterrence efforts may encourage other conventionally weak states to nuclearize. This article will describe situations in which weaker actors can deter stronger powers, the risks associated with such asymmetric dynamics, and the implications of the paradox for the counter-WMD effort.

DETERRENCE

Deterrence is essentially the act of preventing someone or something from committing specific actions by inducing fear of consequences, by diminishing probabilities of success, or even by persuading them to accept alternative incentives. Deterrence operates along a continuum—from dissuasion to denial and then to threat.[4] In a rational sense, deterrence works by convincing the adversary that the expected costs of a potential action outweigh the expected benefits.[5]

Deterrent measures involve holding something valuable to the other party at risk.[6] The classic use for deterrent measures is preventing an adversary from changing its behavior or discouraging it from initiating an action.[7] Consequently, effective deterrence requires credibly communicating both the will and capability to imperil what the adversary holds dear. Clear and credible threats, if properly calibrated for the particular actor and the circumstances, often will encourage rational, risk-averse opponents to retreat.[8] Conversely, threats that lack credibility will not deter.[9]

In addition to overt threats, such as those involving retaliating with force or other military intervention (deterrence by punishment),[10] or imposing economic sanctions or higher costs on the attacker (deterrence by cost imposition),[11] deterrence can take more subtle forms, such as thwarting an opponent's goals or reducing the expected benefits of an attack (deterrence by denial).[12] Deterrence by denial involves largely defensive measures to increase an attacker's risks or probability of failure, though alternative models can incorporate influence theory to account for an actor's perceptions and behavioral motivations.[13] The ability to discourage attacks depends on the attacker's appetite for risk, its capacity to bear the costs of failed attempts, and its perception of the opponent's effectiveness.[14]

Other forms of deterrence also take aim at an actor's subjective behavioral motivations. Deterrence by dissuasion is arguably a more passive deterrent, involving public opinion, public diplomacy, propaganda, or offering a benefit to maintain the status quo.[15] Similarly, deterrence by counter-narrative or deterrence by delegitimization involves convincing an actor or its supporters that some activities are so heinous that even like-minded entities and followers would condemn them.[16] For instance, because using a nuclear or biological weapon may provoke a severe public backlash among its citizens, a nation-state may refrain from conducting such an attack despite tactical or strategic advantages.[17]

The potential irrationality of actors, however, as well as their ability to adapt or make multiple attacks, implies that deterrence carries a palpable risk of failure.[18] Accordingly, to mitigate those risks, an effective deterrence posture requires a mix of deterrent strategies. Would-be deterrers cannot rely solely on threatening adverse repercussions or improving defenses. They should also simultaneously impose costs on potential attackers and undermine attackers' sources of support.[19]

Successful deterrence also requires that the participants send clear, robust communications to each other. Yet, achieving effective communication is challenging for nation-states engaged in strategic competition and even more difficult between nation-states and adversarial non-state actors. The rise of globalization and social media allows different segments of society to express divergent opinions about international events and fosters the propagation of false information, potentially adding noise that undermines the credibility of threats or obfuscates other deterrent signals.[20] Non-state actors motivated by ideological goals may ignore or discount messaging attempts or even use the threats delivered to them to rally their bases of support.[21] Adversaries that do not share a common cultural lexicon, social institutions, public mores, or individual values may have no way to convey or comprehend fully the deterrent messages.[22] Engagements between non-state groups and nation-states face other challenges. The nation-state may deny that an organized group exists, refuse to acknowledge the legitimacy of the group's grievances, or dismiss such a group as an unlawful terrorist or criminal organization. Such actions eliminate both the opportunity for effective communication and the basic peer recognition necessary for meaningful dialogue.

Poor communications may increase uncertainty, allowing adversaries to manipulate both real and perceived risks.[23] "Fake news" currently plagues elections in the U.S. and other parts of the world.[24] Wikileaks and illicit disclosures of state secrets have undermined trust and greater intelligence sharing between allies.[25] Against the ambiguity and instability inherent within the age of social media, Therese Delpech notes that "those who now risk being overwhelmed by complexity and paralyzed by ambiguity are the Western powers, not their adversaries."[26]

COERCION

In contrast to deterrence, which seeks to maintain the status quo between a deterrer and a target, coercion seeks to make an adversary change behavior, i.e., either do something new or stop doing something. Echoing Thomas Schelling, Robert Art and Patrick Cronin use the term "compellence" to describe a range of coercive actions, including applying pressure or inducements as "coercive attempts" or by threatening or actually employing a demonstrative use of military force as "coercive diplomacy" or "forceful persuasion."[27] Beyond threats, coercive diplomacy can encompass (1) "exemplary uses" that communicate intent to intensify adverse consequences and (2) "limited uses" that involve military actions which stop short of the threshold of war.[28] From the point of view of a would-be deterrer, coercive diplomacy represents a belligerent escalation relative to deterrent strategies.[29]

Some coercive actions, however, may contravene international law. Article 2(4) of the United Nations (UN) Charter contains a general prohibition on threats of force or the use of force.[30] Unless a use of armed force is authorized by the UN Security Council or otherwise constitutes a legitimate act of self-defense under customary international law or pursuant to Article 51 of the UN Charter,[31] the use of armed force against the "territorial integrity" or "political independence" of a nation-state may be unlawful.

In practice, deterrence and compellence often become intertwined counterpoints. Whether an action is perceived as a deterrent or as coercion often depends on who benefits from the status quo. Efforts to maintain the status quo will be characterized by the advantaged party as deterrence, yet the target will perceive such actions as coercive.[32] If deterrence fails, however, carrying out the communicated threat is an inherently coercive action, and when deterrent measures are weak a deterrer may employ coercive tactics to maintain the status quo.[33] The failure of coercive diplomacy leaves a nation-state with a set of binary options: either to "back down or wage war."[34]

THE DETERRENCE TRAP: THE WEAK DETERRING THE STRONG

Theoretically, simply possessing nuclear weapons should make a nation secure enough to obviate the need to engage in geopolitical rivalries.[35] In other words, nuclear arms as the ultimate weapon should provide an "existential deterrence," such that a nation-state ought to

be able to deter conflict even with small nuclear forces.[36] In reality, though, nation-states which possess nuclear weapons continue to engage in rivalries and security competitions,[37] even waging overt kinetic hostilities (e.g., 1999 Kargil War between Pakistan and India).

Similarly, radically asymmetric nuclear competitions should be fundamentally unstable, because nascent arsenals should be unable to deter larger, more established arsenals.[38] Moreover, improvements in counterforce capability—the ability to engage in attacks aimed at disarming the enemies' nuclear forces—should allow larger arsenals to render small nuclear arsenals even more vulnerable.[39] Yet, North Korea and nuclear-enabled regional powers, such as India and Pakistan, have shown that stronger powers are often unable to deter the actions of a relatively weaker actor effectively, even when the stronger nation-state is a major world power. Aspiring states such as North Korea, with less to lose, seem to understand how to manipulate risks better than Western powers.[40] Regardless of whether the stronger power threatens retaliation or abstains from threats to appease the weaker actor, the weaker power's unwelcome behavior continues.[41] The major power's attempts at overt deterrence fall into a self-defeating prophecy, a so-called "deterrence trap."[42]

When caught in a deterrence trap, weaker actors may leverage the beliefs, values, and motivations of the stronger state to elicit a violent response or inaction, both of which help the weaker entity.[43] Western democracies, which believe that human life has intrinsic value, generally work to avoid violent escalation; they assume that the advantages of peace and the value of their ideals are universal and self-evident, such that all actors would be willing to compromise to preserve their lives.[44] This fundamental bias for preserving human life forms the basis for Western powers' approach to deterrence.[45] Yet, acting on the belief that everyone shares this risk-averse propensity for peace and compromise is the source of a key weakness in Western deterrence strategy.

Opponents (such as terrorists) may not share key Western ideological tenets. Succumbing to such cognitive biases of projection and mirror-imaging can have tragic results, as aspiring states like North Korea that are willing to subject significant numbers of their population to death by starvation do not appear to hold human life as precious. Malicious non-state actors may instead utilize the West's valuation of human life to fashion human shields against the stronger nation's threats of force.[46] Without any mutual sense of the intrinsic value of human life or other shared ideals, there is little chance to hold anything the target values at risk and no basis for achieving meaningful concessions. Despite their opponents' provocations, risk-averse Western powers are unwilling to use force and are locked into a prison of self-restraint.

This deterrence trap can foster asymmetric escalations of armed force. Instead of the gradual, proportionate responses to hostile actions, e.g., symmetrically matching conventional uses of force with comparable conventional uses of force, a weaker nation immediately goes to its trump card and readies nuclear arms as an initial response to any provocation. Unlike Cold War deterrence strategies based on second-strike capabilities to assure the destruction of an attacker, actors who employ asymmetric escalation brandish their WMD (especially nuclear) capabilities to threaten them as weapons of immediate resort. Asymmetric nuclear escalation potentially sets a new global norm that seems to tolerate an offensive posture for nuclear weapons, which undermines the use of international agreements or other fora that encourage compliance using cooperative, problem-solving approaches.[47] Instead, the community of nation-states may be left with coercive or punitive mechanisms as the sole means of countering the proliferation of WMD.

ASYMMETRIC ESCALATION BETWEEN NATION-STATES

Pakistan has employed what Vipin Narang describes as "a credible first use nuclear posture" to deter asymmetrically both Indian conventional and nuclear attacks.[48] Pakistan has essentially goaded India into a deterrence trap by communicating its intent to use tactical nuclear weapons against an attack by India's greater conventional forces, while keeping the remainder of its arsenal protected from an Indian retaliatory strike.[49] This deterrence trap has ostensibly enabled Pakistan to engage in hostile actions against India, as well as allow armed groups based in Pakistan to conduct terrorist attacks, without significant fear of Indian retaliation.[50]

To maintain this credible first use posture, Narang notes that Pakistan is believed to keep the components of both its warheads and delivery mechanisms geographically close together, possibly in the same facilities, to enable extremely rapid assembly and deployment.[51] Pakistan has also made doctrinal changes that essentially delegate launch controls of its tactical devices to field commands.[52] Instead of splitting nuclear launch and assembly authorizations between the central command and lower levels of command, launch codes are kept with the devices and split between the base commander and the unit commander.[53] This distributed authorization guards against communication outages between bases and the capital during crisis situations, but reduces the control that central political authorities have over the use of nuclear weapons, increasing the chances of accidental or unauthorized use of WMD.[54]

By keeping devices in a state of near-launch readiness, Pakistan risks a dangerous end game. Despite Pakistan's insistence that the first-strike weapons would be used

against military targets in only a limited setting, any use of nuclear weapons is likely to be met by an Indian nuclear response. An Indian nuclear strike would likely engender an additional retaliatory strike from Pakistan, setting off a spiral of coercive escalation. Ultimately, India will likely use its larger nuclear arsenal to launch a full assault against Pakistan, and it is uncertain whether Pakistan will be able to maintain its second-strike capability. This end game will likely motivate Pakistan to use the full complement of its nuclear weapons early on, diminishing the chances for only a tactical or limited nuclear exchange between the two regional combatants.

To avoid this end game, yet preserve domestic political support, India and Pakistan have kept their hostilities to limited skirmishes with conventional weapons. The use of nuclear weapons is a tipping point[55] that both India and Pakistan are apparently reluctant to cross, which appears to encourage the parties to de-escalate after each of these skirmishes. Most recently, in response to a deadly February 14, 2019, suicide bombing against Indian paramilitary forces in the disputed Kashmir region, India launched an airstrike on February 26 against a target in Pakistan.[56] The Indian airstrike, which was the first time India had used aircraft to strike a target in Pakistan in nearly five decades, inflicted very little damage.[57] News reports suggest that "India was making a calculated bet to assuage public anger but minimize the risk of a major Pakistani military response."[58] On February 27, Pakistan shot down an Indian fighter plane, capturing its pilot.[59] In what it called a "good will gesture," Pakistan released the captured pilot two days later, apparently gaining favorable publicity in the process.[60] Although the likelihood of a major conflict has eased somewhat, tensions on each side are likely to remain on edge until the end of April when Indian elections occur.[61]

Aspiring regimes, such as North Korea, are also developing WMD and long-range missile capabilities; in addition, North Korea has demonstrated a willingness to spread these technologies.[62] North Korea seeks to use its WMD to guarantee regime survival and gain influence over South Korea, Japan, and the U.S.[63] In the event kinetic hostilities break out, North Korea would likely launch nuclear arms against U.S. and allied bases in the Pacific to cripple the impending U.S. attack.[64] Yet, U.S. attempts to denuclearize North Korea and deter it from pursuing WMD and advanced delivery mechanisms have not been successful, despite the apparent disparity in military capabilities between the U.S. and North Korea. The continued advances of North Korea's nuclear and missile programs seem to show that it is achieving some success in deterring the U.S.

As Pakistan does with India, North Korea is likely to employ asymmetric escalation to use nuclear devices both in fending off invasion and simultaneously threatening U.S. or allied cities in order to deter a preemptive nuclear strike.[65] North Korea's efforts to "stave off an invasion with a limited nuclear attack on a U.S. military target is not irrational, although it is clearly risky and terrifyingly tragic."[66]

The U.S. is not India, however. The U.S. has advanced counterforce capabilities.[67] In the event of war, the U.S. will likely try to find and neutralize all of North Korea's nuclear systems.[68] However, because of its dearth of weapons and the vulnerability of its arsenal, North Korea will need to launch an extensive nuclear strike first; accordingly, any credible threat of major hostilities against North Korea will risk a nuclear exchange.[69]

NON-STATE ACTORS

Non-state actors also threaten U.S. national security with increasingly sophisticated capabilities. The 2018 National Defense Strategy notes that terrorists continue to pursue WMD,[70] but non-state actors pose unique deterrence challenges. There are many kinds of non-state actors, each having different motivations, grievances, and objectives. Richard Shultz categorizes non-state actors[71] as insurgents,[72] terrorists,[73] militias,[74] and criminal organizations.[75] The variation between these groups complicates deterrence strategies and precludes a "one size fits all" posture for them. However, Shultz describes six common elements: (1) non-state actors challenge a nation-state's "authority, power, and legitimacy;" (2) they use violence and force in unconventional and asymmetric ways to achieve their objectives; (3) technological advances and decentralized structures allow them to operate both locally and globally; (4) they operate on a "conspiratorial and clandestine" basis, often hiding their methods, members, and targets; (5) they face both internal factional and political rivalries as well as competition with other entities; and (6) they do not adhere to Western values such as democracy and the rule of law.[76]

Would-be deterrers need to take a more nuanced look at each non-state actor and see it in the context of its geopolitical surroundings, socioeconomic milieu, and motivations.[77] For instance, a stable and flourishing criminal group has likely achieved some measure of accommodation, either tacit or overt, with the relevant authorities.[78] Such a group may be more amendable to deterrence because it seeks to protect its revenue streams. In contrast, non-state actors motivated by religion or committed to armed revolt are unlikely to be deterred by mere threats of force.

Unlike a nation-state that will seek to protect its sovereignty, non-state actors often lack a "clearly identifiable center of gravity" or other fundamental asset that can be targeted and held at risk.[79] Emanuel Adler asserts that "using force against asymmetrically weaker adversaries or exhibiting self-restraint will achieve the same result: the materially stronger

state stands to lose."[80] Moreover, uses of force designed for what Rupert Smith calls "interstate industrial war," in which militaries of similar strength engage each other on delineated theaters of operation, will often fail when deployed against non-state actors that employ unconventional modes of warfare.[81] To win an industrial war, a nation-state will seek to destroy its opponent's military forces, and thereby eliminate the opponent's ability to wage war.[82] Without the means to defend against armed force, the opponent's government cannot protect itself or its people. Hence, the government will capitulate.[83] In contrast, when a weaker entity fights a stronger nation-state, it will seek to whittle away the warfighting resources of the nation-state and, over the long term, break the will of its government and people in order to debilitate the nation-state's capacity for war.[84] Rational non-state groups recognize that they may be unable to win decisive military victories against stronger foes; instead, they will focus on causing disruptions to undermine their opponent's ability to govern or achieve political goals.[85]

Weaker actors will attack stronger targets only when it is to their advantage; a rational actor will avoid other confrontations during asymmetric warfare. Accordingly, non-state armed groups will present tactical targets only because they will avoid engaging stronger military powers with the bulk of their forces.[86] Threats and use of force will hold little sway against a non-state actor because it simply has less to lose, yet the smaller non-state group can force the stronger power into protracted engagements that sap the stronger power's resources and will to fight.

Armed interventions to prevent terrorism seem to galvanize public sympathy for the terrorists, thereby undermining deterrent efforts and encouraging terrorists to continue to try to put U.S. interests in jeopardy.[87] Because general threats of force are largely ineffective when directed against insurgents, terrorists, and militias, deterrers should employ a broader deterrence strategy that simultaneously targets the group's individual members, the nation-states where the group resides or operates, and the group's international sources of support.[88] For instance, hardening potential targets (e.g., installing checkpoints at airports) and improving intelligence collection may help thwart terrorist attacks, thereby enhancing deterrence by denial.[89] Propaganda and influence campaigns can dissuade likely recruits, as well as win the hearts and minds of the surrounding population.[90] Applying resources and political pressure on the government may ameliorate an insurgent group's grievances within its host country.[91] At an international level, choking off sources of support and sympathy will weaken hostile non-state actors. Over time, nation-states banding together to suffocate sources of funding will likely disrupt an international criminal group's efforts.[92]

In practice, though, implementing such targeted deterrence schemes has proven difficult. Although the U.S. government developed a framework for tailoring forms of deterrence, U.S. policymakers largely abandoned this approach in the real world; instead, policymakers have resorted to hinting at severe but unspecified threats.[93] Failure to follow up on such threats undermines the credibility of deterrent efforts.

IMPLICATIONS

Engagements with asymmetric opponents and the associated potential to be ensnared in a deterrence trap have significant implications for counter-WMD and non-proliferation efforts. The traditional threats involving use of force are unlikely to deter aspiring states and malicious non-state actors from trying to develop and use WMD.

Rather than simply issuing threats, counter-WMD efforts against non-state actors should couple deterrent messages with forceful persuasion. For instance, decentralized criminal groups that rely on modern communications networks to coordinate disparate cells may be vulnerable to cyber engagement and sanctions that disrupt their ability to communicate or generate funds. Although outright uses of armed force that infringe upon the sovereignty of nation-states may violate international law, employing subtle measures below the threshold of armed conflict may still be effective. Moreover, given reckless uses of force may escalate hostilities, softer deterrence tactics tailored to the specific circumstances that address the roots of the actors' motivations and sources of support may often be more effective than simplistic threats of military force.[94]

Deterrence can fail; therefore, those issuing threats and taking other deterrent actions need to ensure that sufficient political will and proper resources are available to follow through, as necessary. Strategists need to understand that engagements against weaker entities may take the form of a protracted series of tactical actions, such that outright military victory at the strategic level may be unattainable in the short term. Unlike adversaries engaged in conventional industrial war, non-state groups are not protecting people or even trying to achieve outright military dominance. Because they emphasize tactical actions over strategic objectives, non-state actors can adjust their approach and quickly exploit weaknesses in defenses.

Nation-states and their intelligence services need to discern the effectiveness of their deterrent communications amid the fog of uncertainty. That is, did the correct recipient receive the correct message? Moreover, intelligence efforts will need to place greater emphasis on clarifying an adversary's intentions and motivations, as well as prioritizing the mitigation

of strategic surprise. Western nation-states reflect many potential vulnerabilities. Since it may be easier to prevent the formation of new non-state groups than to neutralize existing ones, intelligence efforts in support of deterrence strategies should include efforts to find "incipient indicators" for terrorists, insurgents, and militias, in addition to looking for ways to address the underlying grievances of the relevant population.[95] Non-state actors which are unfettered by international norms and lack home territories or institutions to defend are more likely to utilize tactics and take actions that are unpredictable, even foolhardy, because they have less to lose and may not need to achieve outright victories against a major power to make gains.[96]

The rise of potentially irrational actors requires deterrence strategists to account for behavioral aspects such as an attacker's perceptions and its subjective motivations. Policymakers should also avoid projecting Western democratic values or their own decision calculus on non-state actors and aspiring regimes. Adversaries which do not believe human rights or their lives are particularly valuable are unlikely to be deterred by threats of force. The American bias toward a "technical or engineering approach to solving political problems"[97] may blind policymakers from understanding that emotions, anger, betrayal, and shame are more likely to sway these actors than any cold cost-benefit calculations.[98] Asymmetric contestants may appear to act irrationally by our standards, but they will act rationally with regard to their own values and objectives.

CONCLUSION

The current geopolitical balance is complex and unstable. There are few, if any, non-violent alternatives to deterrence.[99] Coercive diplomacy, full-scale use of military force, or the actual use of WMD carry serious downsides. Understanding an attacker's perceptions and behavioral motivations can yield more effective deterrence strategies against non-state actors and aspiring nation-states, alleviating the risk of falling into a deterrence trap.

Forms of deterrence other than threatening the use of force may be more effective against the destabilizing behavior of non-state actors and aspiring regimes. In contrast to the mindset of industrial war, in which militaries will destroy their opponent's ability to fight in order to achieve a political end, small forces engaging larger ones will conduct tactical actions to attenuate the control of political authorities, to rally members, and to cultivate new recruits and support from allies.[100] Policymakers need to understand the balance and interplay between deterrence and compellence. Simple Cold War-era rational choice strategies fail to account for the nuances of each actor and of each situation and thus carry high risks of failure.[101] Yet, despite its limitations, deterrence remains an important tool in the non-proliferation effort.

NOTES

[1] Michael Ruhle, "Deterrence: what it can (and cannot) do," *NATO Review*, accessed October 7, 2018, http://www.nato.int/docu/review/2015/Also-in-2015/deterrence-russia-military/EN/index.htm.

[2] A more pessimistic person would refer to aspiring states as "rogue states."

[3] "Dissuading, preventing, or deterring state adversaries and non-state actors from acquiring, proliferating, or using weapons of mass destruction" is a key national defense objective. Jim Mattis, "Summary of the 2018 National Defense Strategy," 3.

[4] Adam B. Lowther, "How Can the United States Deter Nonstate Actors," in *Deterrence: Rising Powers, Rogue Regimes, and Terrorism in the Twenty First Century*, ed. Adam B. Lowther (New York: Palgrave Macmillan, 2012), 172; Ibid., 165. Citing Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, "Deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counter actions."

[5] DSB Task Force on Cyber Deterrence, *Final Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence* (Washington, DC: Defense Science Board, February 1, 2017), 5, accessed May 15, 2018, http://www.dtic.mil/docs/citations/AD1028516.

[6] Jeffrey W. Knopf, "Use With Caution: The Value and Limits of Deterrence Against Asymmetric Threats," last modified June 11, 2013, accessed October 7, 2018, https://www.worldpoliticsreview.com/articles/13006/use-with-caution-the-value-and-limits-of-deterrence-against-asymmetric-threats.

[7] Robert J. Art and Patrick M. Cronin, *The United States and Coercive Diplomacy* (Washington, DC: U.S. Institute of Peace Press, 2003), 8.

[8] Therese Delpech, *Nuclear Deterrence in the 21st Century* (Santa Monica, CA: RAND Corporation, 2012), 50. Well-tailored deterrent efforts "oblige the opponent to take sides in a gamble known to be highly dangerous," such that rational actors (ones who are able to distinguish gains from losses and then act to maximize gains) will back down.

[9] Lowther, "How Can the United States Deter Nonstate Actors," 167.

[10] Ruhle, "Deterrence."

[11] DSB Task Force on Cyber Deterrence, *DSB Cyber Deterrence Report*, 5.

[12] Ruhle, "Deterrence"; DSB Task Force on Cyber Deterrence, *DSB Cyber Deterrence Report*, 5.

[13] Paul K. Davis, "Toward Theory for Dissuasion (or Deterrence) by Denial: Using Simple Cognitive Models of the Adversary to Inform Strategy" (January 2014): 2; Lowther, "How Can the United States Deter Nonstate Actors," 166. Davis describes "dissuasion by denial," a variation of deterrence by denial, as "deterring an action by having the adversary see a credible capability to prevent him from achieving potential gains adequate to motivate the action."

[14] Davis points out that defenses may fail to deter because an attacker may (1) underestimate the defense if its more effective elements are hidden from the attacker, (2) have enough resources to try numerous times, (3) benefit even if attack "fails" because the attempt will motivate supporters to garner favorable publicity, and (4) get lucky and succeed even if the defense is relatively effective. In the latter case, "a rogue state trying to deter intervention by the United States

and allies, the rogue's ability to deliver even a single nuclear weapon against an allied capital or the U.S. homeland might have great value even if defenses could intercept most weapons." Davis, "Toward Theory for Dissuasion (or Deterrence) by Denial: Using Simple Cognitive Models of the Adversary to Inform Strategy," 4.
[15] Lowther, "How Can the United States Deter Nonstate Actors?" 166.
[16] Knopf, "Use With Caution: The Value and Limits of Deterrence Against Asymmetric Threats."
[17] Ibid.
[18] Therese Delpech observes that "Deterrence is not only about influencing adversaries' behavior but also about taking risks." Delpech, *Nuclear Deterrence in the 21st Century*, 28.
[19] DSB Task Force on Cyber Deterrence, *DSB Cyber Deterrence Report*, 5; Davis, "Toward Theory for Dissuasion (or Deterrence) by Denial: Using Simple Cognitive Models of the Adversary to Inform Strategy," 5.
[20] Koichi Arie, "Complex Deterrence Theory and the Post-Cold War Security Environment," *NIDS Journal of Defense and Security* 17, no. 1 (December 2016): 27.
[21] Lowther, "How Can the United States Deter Nonstate Actors," 175.
[22] Emanuel Adler, "Complex Deterrence in the Asymmetric-Warfare Era," in *Complex Deterrence: Strategy in the Global Age*, eda. T.V. Paul, Patrick M. Morgan, and James J. Wirtz (Chicago: University of Chicago Press, 2009), 99.
[23] Delpech, *Nuclear Deterrence in the 21st Century*, 48.
[24] See, for example, Paul Mozur and Mark Scott, "Fake News in U.S. Election? Elsewhere, That's Nothing New," *The New York Times*, November 17, 2016, sec. Technology, accessed February 24, 2019, https://www.nytimes.com/2016/11/18/technology/fake-news-on-facebook-in-foreign-elections-thats-not-new.html.
[25] Lowther, "How Can the United States Deter Nonstate Actors," 176.
[26] Delpech, *Nuclear Deterrence in the 21st Century*, 18.
[27] Art and Cronin, *The United States and Coercive Diplomacy*, 7; Thomas C. Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966), 69. Art and Cronin differentiate coercive diplomacy from coercive attempts, stating that the "coercive diplomacy must involve the threat or limited use of force, even though it can also include…other types of coercive actions." They credit Alexander George for the term "forceful persuasion," citing Alexander L. George, *Forceful Persuasion: Coercive Diplomacy as an Alternative to War* (Washington, DC: U.S. Institute of Peace Press, 1991), 5.
[28] Art and Cronin, *The United States and Coercive Diplomacy*, 10.
[29] Ibid., 7.
[30] United Nations, "United Nations Charter," October 24, 1945, accessed March 18, 2019, http://www.un.org/en/sections/un-charter/un-charter-full-text/. Art. 2(4): "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."
[31] Ibid. The text of Art. 51: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security."
[32] Art and Cronin, *The United States and Coercive Diplomacy*, 8. "In a deterrent situation, if the threat has to be carried out, then, by definition, the adversary has changed its behavior and deterrence has failed. In contrast, because compellence can entail both threats and actual use of force, compellence has not necessarily failed if the threats are carried out."
[33] Ibid.
[34] Ibid., 7.
[35] Keir A. Lieber and Daryl G. Press, "The New Era of Counterforce: Technological Change and the Future of Nuclear Deterrence," *International Security* 41, no. 4 (Spring 2017): 10.
[36] Vipin Narang, "Deterring Unequally: Regional Power Nuclear Postures and International Conflict" (presented at the International Security Colloquium, Charlottesville, VA, 2011), 10, http://politics.virginia.edu/wp-content/uploads/2015/11/Narang-VISC.pdf.
[37] Lieber and Press, "New Era of Counterforce," 10.
[38] Jan Ludvik, *Nuclear Asymmetry and Deterrence: Theory, Policy and History* (London, UK: Routledge, 2016), 8.
[39] Lieber and Press, "New Era of Counterforce," 9.
[40] Delpech, *Nuclear Deterrence in the 21st Century*, 48.
[41] Arie, "Complex Deterrence Theory and the Post-Cold War Security Environment," 26-27.
[42] Adler, "Complex Deterrence in the Asymmetric-Warfare Era," 85.
[43] Ibid., 86.
[44] Delpech, *Nuclear Deterrence in the 21st Century*, 1; Ibid., 17.
[45] Ibid., 97.
[46] Adler, "Complex Deterrence in the Asymmetric-Warfare Era," 100.
[47] Abram Chayes and Antonia Handler Chayes, *The New Sovereignty: Compliance with International Regulatory Agreements* (Cambridge, MA: Harvard University Press, 1998), 3. Chayes and Chayes argue that a "managerial model" of cooperative problem solving may prove to be a better way to foster compliance with international treaties than the traditional "enforcement model" of sanctions and punitive measures.
[48] Vipin Narang, "Posturing for Peace? Pakistan's Nuclear Postures and South Asian Stability," *International Security* 34, no. 3 (Winter 2009): 45.
[49] Ibid., 57.
[50] Ibid., 39, 64.
[51] Ibid., 67.
[52] Ibid., 39.
[53] Ibid., 67-68.
[54] Ibid., 39.
[55] Malcolm Gladwell, *The Tipping Point: How Little Things Can Make a Big Difference* (Boston, MA: Little Brown and Company, 2002), 7. Gladwell's eponymous tipping point has become the vernacular way to label situations that are at the cusp of change.
[56] Maria Abi-Habib and Austin Ramzy, "Indian Jets Strike in Pakistan in Revenge for Kashmir Attack," *The New York Times*, February 26, 2019, sec. World, accessed March 16, 2019, https://www.nytimes.com/2019/02/25/world/asia/india-pakistan-kashmir-jets.html; Sameer Yasir and Maria Abi-Habib, "Kashmir Suffers From the Worst Attack There in 30 Years," *The New York Times*, February 15, 2019, sec. World, accessed March 11, 2019, https://www.nytimes.com/2019/02/14/world/asia/pulwama-attack-kashmir.html. Jaish-e-Muhammad, a group that the U.S. Treasury Department has listed as a terrorist organization, claimed responsibility for the suicide bombing, which killed more than 40 Indian soldiers.

[57] Abi-Habib and Ramzy, "Indian Jets Strike in Pakistan in Revenge for Kashmir Attack"; Maria Abi-Habib, "After India's Strike on Pakistan, Both Sides Leave Room for De-Escalation," *The New York Times*, February 27, 2019, sec. World, accessed March 11, 2019, https://www.nytimes.com/2019/02/26/world/asia/india-pakistan-kashmir-airstrikes.html.
[58] Abi-Habib and Ramzy, "Indian Jets Strike in Pakistan in Revenge for Kashmir Attack."
[59] Jeffrey Gettleman, Maria Abi-Habib, and Salman Masood, "Imran Khan Says Pakistan Will Release Indian Pilot, Seizing Publicity in Showdown," *The New York Times*, March 1, 2019, sec. World, accessed March 11, 2019, https://www.nytimes.com/2019/02/28/world/asia/pakistan-india-pilot-kashmir.html.
[60] Jeffrey Gettleman and Suhasini Raj, "Pakistan Frees Indian Pilot Who Was Beaten by a Mob and Then Served Tea," *The New York Times*, March 2, 2019, sec. World, accessed March 16, 2019, https://www.nytimes.com/2019/03/01/world/asia/india-pakistan-plane-abhinandan-varthaman-india.html; Gettleman, Abi-Habib, and Masood, "Imran Khan Says Pakistan Will Release Indian Pilot, Seizing Publicity in Showdown."
[61] Jeffrey Gettleman, Vindu Goel, and Maria Abi-Habib, "In India's Election Season, an Explosion Interrupts Modi's Slump," *The New York Times*, March 11, 2019, sec. World, accessed March 11, 2019, https://www.nytimes.com/2019/03/11/world/asia/modi-india-election.html; Sameer Yasir and Jeffrey Gettleman, "'We Will Always Live in Fear': What Life Is Like for Civilians in Kashmir," *The New York Times*, March 2, 2019, sec. World, accessed March 16, 2019, https://www.nytimes.com/2019/03/01/world/asia/kashmir-india-pakistan.html.
[62] Mattis, "Summary of the 2018 National Defense Strategy," 3.
[63] Ibid., 2.
[64] Vipin Narang, "Perspective: Why Kim Jong Un Wouldn't Be Irrational to Use a Nuclear Bomb First," *The Washington Post*, last modified September 8, 2017, accessed October 7, 2018, https://www.washingtonpost.com/outlook/why-kim-jong-un-wouldnt-be-irrational-to-use-a-nuclear-bomb-first/2017/09/08/a9d36ca4-934f-11e7-aace-04b862b2b3f3_story.html.
[65] Ibid. "Faced with the prospect of a U.S.-led invasion, Pyongyang's conventional inferiority requires it to degrade the United States' ability to sustain the attack against it."
[66] Ibid.
[67] Lieber and Press, "New Era of Counterforce."
[68] Narang, "Perspective: Why Kim Jong Un Wouldn't Be Irrational to Use a Nuclear Bomb First."
[69] Ibid.
[70] Mattis, "Summary of the 2018 National Defense Strategy," 3.
[71] Richard H. Shultz, Jr., "The Era of Armed Groups," in *The Future of American Intelligence*, ed. Peter Berkowitz, 1st edition. (Stanford, Calif: Hoover Institution Press, 2005), 10. Shultz uses the term "Non-State Armed Groups."
[72] Ibid., 11. Shultz describes insurgents as groups that use irregular military forces and political organizations to gain political control over the territory of their target country.
[73] Ibid., 15. Terrorists use violence to instill fear for political purposes, sometimes in favor or against current governments. Terrorists differ from insurgents in tactics, targeting and motivation. Insurgents use tactics other than terrorism.
[74] Ibid., 17. Shultz describes post-Cold War militias as an amorphous category that involves a "recognizable irregular armed force operating within the territory of a weak or failing state." Members tend to be economically disadvantaged young males who see membership as a path to money, power, or security, though some members are coerced into joining.
[75] Ibid., 23. Shultz distinguished criminal organizations as possessing "a clandestine hierarchical structure and leadership whose primary purpose is to operate outside the law in a particular criminal enterprise." In contrast to the other groups, criminal organizations are motivated by economic gain—making money from illegal activities.
[76] Ibid., 10.
[77] Lowther, "How Can the United States Deter Nonstate Actors," 172.
[78] Shultz Jr., "The Era of Armed Groups," 29.
[79] Lowther, "How Can the United States Deter Nonstate Actors," 172.
[80] Ibid.
[81] Rupert Smith, *The Utility of Force: The Art of War in the Modern World*, Kindle edition (New York: Knopf, 2007), 5.
[82] Ibid., 177.
[83] Ibid.
[84] Ibid.
[85] Ibid., 164.
[86] Ibid., 165.
[87] Adler, "Complex Deterrence in the Asymmetric-Warfare Era," 100.
[88] Lowther, "How Can the United States Deter Nonstate Actors," 175.
[89] Ibid.
[90] Ibid., 174.
[91] Ibid., 175.
[92] Ibid., 177.
[93] Knopf, "Use With Caution: The Value and Limits of Deterrence Against Asymmetric Threats."
[94] Adler, "Complex Deterrence in the Asymmetric-Warfare Era," 100.
[95] Shultz Jr., "The Era of Armed Groups," 21.
[96] Lowther, "How Can the United States Deter Nonstate Actors," 173.
[97] Delpech, *Nuclear Deterrence in the 21st Century*, 17.
[98] Adler, "Complex Deterrence in the Asymmetric-Warfare Era," 85.
[99] Delpech, *Nuclear Deterrence in the 21st Century*, 1.
[100] Smith, *The Utility of Force*, 177.

[Author's Note: I wish to thank Dr. (LTC, USA) Jeffrey B. Bacon, a faculty member in NIU's Anthony G. Oettinger School of Science and Technology Intelligence, for his helpful comments. The views expressed in this paper are those of the author and do not reflect the official policy or position of the Department of Defense, the Department of Homeland Security, the Federal Emergency Management Agency, or the U.S. government.]

Samuel Chi, a master's degree candidate at the National Intelligence University, is an attorney-advisor with the Department of Homeland Security, specializing in information technology and cybersecurity law.

Improving Sources and Methods by Training Ethnic Slavs

by Mason Shuya

INTRODUCTION

One of the most pressing issues for U.S. national security in the 21st century is the renewal of great power competition.[1] The Donald J. Trump administration has decided to emphasize this renewed rivalry in the latest *National Security Strategy* (2017). There have been arguments made that one particular nation, the Russian Federation, is reasserting itself and engaging in a new Cold War with the United States and its allies.[2] If this is indeed the case, then the United States and its allies will have to recognize that they are in for an enduring struggle that, perhaps as in the Cold War, can last decades. One weakness that should be addressed by U.S. intelligence services is this glaring deficiency: Americans are very weak with foreign languages and face a foreign language crisis.[3] One advantage the United States has is its tradition of receiving migrants and the establishment of migrant communities. The U.S. also has a history of accepting Russian migrants at different times, especially after the end of the Cold War.[4] This leads to one possible question for the Intelligence Community when having to face renewed threats from an old foe: Can the United States overcome its weaknesses in foreign languages by recruiting ethnic Slavs/Russians to join the Intelligence Community for the purpose of countering the Russian Federation in this new Cold War? This article seeks to answer the question by analyzing the history of Russian migration to North America and intelligence policy in both the United States and Canada that would address whether this recommendation is even feasible.

One weakness that should be addressed by U.S. intelligence services is this glaring deficiency: Americans are very weak with foreign languages and face a foreign language crisis.

The idea of recruiting and training ethnic Slavs would fall under the category of "sources and methods" within intelligence policy and strategy. While the usage of the phrase seems common enough, what does it mean and why is it so guarded? James Wirtz defines the phrase as "a term used to describe the practice of intelligence collection and analysis" and continues to describe the phrase as the origins of the information and the ways that it was obtained.[5] This is important because this is the answer with which personnel from CIA will respond when asked, "Is the Agency returning to look at Russia or increasing its size within that division?" The specific answer usually given is "I'm sorry, I can't answer that—sources and methods." However, references to an aggressive and re-assertive Russia within the *National Intelligence Strategy* and the confirmation hearing of Gina Haspel, Director of the CIA, would indicate that this is becoming an intelligence priority.[6] The Russian threat has also been the focus of numerous House and Senate Intelligence Committee hearings, with interviews of witnesses such as former Ambassador to Russia Michael McFaul and former CIA Chief of Russian Operations Steve Hall. Yet, in line with the theme at the beginning of this paragraph, Mr. Hall testified before Congress, "I will not be able to address in great detail what I know of how the Russian intelligence services specifically do their work. I cannot risk exposing the sources and methods our own intelligence services use, nor those of our allies."[7] Consequently, with a focus on both Russia and U.S. "sources and methods" regarding Russia, how would it even be possible to recruit ethnic Slavs for this new looming Cold War? The answer was touched upon in the introduction but lies with history—migration.

RUSSIAN MIGRATION TO NORTH AMERICA

In the 1870s, the first wave of emigres from the Russian Empire headed to North America.[8] They settled in the American Great Plains, from Kansas, Nebraska, and Colorado in the United States to Manitoba and Saskatchewan in Canada. Whether settling in the American or Canadian Great Plains, the overwhelming majority were leaving the oppressive Russian regime, violence, and persecution (religious and political). This migration was one of the original issues that drove Canadian-Russian foreign

policy in the 19th and early 20th centuries, as Canada was establishing a large network of agents to help Russian emigres resettle in Canada.[9] While the oppression of the czarist regime was widespread, economic opportunity was also a large factor in enticing these immigrants to North America.[10]

...there is an ample population of Russian/ Slavic language speakers who have been raised with Western culture and ideals.

Another large wave of Russian immigrants came following World War I and the Soviet Revolution, settling in the major cities on the U.S. East Coast and establishing communities of well-educated Russians.[11] The lasting impact of these communities today is roughly 870,000 Russian-language speakers in the United States (per U.S. Census Bureau) and roughly 196,000 Russian-language speakers in Canada (per Statistics Canada).[12] It has also meant roughly 360,000 other Slavic language speakers in the United States (per U.S. Census Bureau) and 110,000 Ukrainian language speakers in Canada (per Statistics Canada). What the statistics indicate is that there is an ample population of Russian/Slavic language speakers who have been raised with Western culture and ideals. The oldest of these communities was established nearly 150 years ago, leaving generations of ethnic Russians and Slavs to become either American or Canadian and sympathetic to liberal democracy in rejection of autocratic governance. What can also be learned from these statistics is that there is a population of Americans and Canadians who can either speak Russian or languages similar enough to learn Russian. With this language aptitude population present in the United States, is there a framework for this targeted recruitment of ethnic minorities within intelligence practice?

EXAMPLES FROM THE PAST

To put it simply, the U.S. has done it before. Leading up to the Allied invasion of Sicily in World War II, Italian-Americans (ethnic and naturalized) were instrumental in providing vital intelligence so that the U.S. and British militaries could invade Italy from the south.[13] These ethnic Italians (and naturalized Italians) filled the ranks of the U.S. Army and the Office of Strategic Services (OSS). This coordinated effort for intelligence even included information and social networking from organized crime figures like "Lucky" Luciano.[14] The strategy of using ethnic peoples for national security has also occurred much more recently, both during the Cold War and even into the 21st century. One Cold War example would be CIA case officer George Kisevalter, who was born in in pre-Revolution Russia as a White Russian and then moved with his family to the United States.[15] Kisevalter was the CIA case officer who was in charge of handling Soviet GRU officer Major Pyotr Semyonovich Popov, the first Soviet asset for the CIA during the Cold War. Trento acknowledges that Kisevalter was "the first of an elite cadre of case officers who would travel the world for the CIA," but does not elaborate any further as to whether they specifically had Russian backgrounds like Kisevalter or not. Jeremy Risen, however, does discuss this phenomenon of recruiting specific language speakers once again during the George W. Bush administration and the lead-up to the Iraq War in 2003.[16] Risen writes that Dr. Sawsan Alhaddad was one of 30 Iraqi exiles who were recruited by the CIA to return to Baghdad and talk with family members still actively within Saddam Hussein's national security apparatus, particularly as scientists within the weapons of mass destruction (WMD) program. It should also be clarified that these exiles, like Dr. Alhaddad, had moved to places like Cleveland, Dallas, Chicago, and Houston to begin peaceful lives as doctors or engineers, not as revolutionaries banished in defeat.

...61.6 percent of U.S. Intelligence Community employees are male and 76.6 percent of employees are white.

While the preceding paragraph details only one mention of "ethnic" peoples doing something for the United States, and two examples of asking naturalized citizens, it also leads to some type of framework for this thinking. This framework actually comes from the Office of the Director of National Intelligence (ODNI), which releases guides and plans for its approach to human capital. Through a Freedom of Information Act request, Damien Van Puyvelde was granted a copy of the ODNI's *Strategic Human Capital Plan 2012-2017* and found that 61.6 percent of U.S. Intelligence Community employees are male and 76.6 percent of employees are white.[17] Dr. Van Puyvelde and Dr. Stephen J. Coulthart argued that there should be greater diversity within the Intelligence Community and that, even with all of its efforts to fix the problem, there were still too many barriers to this diversity. Their argument also reveals that ODNI and the Intelligence Community as a whole are analyzing the types of threats that the country is facing, which actually include foreign language deficiency. This ODNI strategy also specifically states, "Beyond the traditional Equal Employment Opportunity categories such as race, ethnicity, gender, and age, the ODNI will consider

diversity in its broadest context, including diversity in cultural understanding, foreign languages and dialects, highly specialized skills, and technological expertise." This plan continues with identifying recruitment opportunities for both first-generation and second-generation Americans as just as important as the "race, ethnicity, gender, and age" previously described. In essence, it states that ODNI has begun a framework for recruitment of potential employees that fit mission needs which, at this moment in time, seem to revolve around the Russian Federation. The next question is: Does Canada have a similar framework?

THE CANADIAN EXPERIENCE

Why should we include Canada in an essay analyzing possible U.S. sources and methods? The answer is two-faceted: geographic proximity and the "Five Eyes" alliance. The geographic proximity was already touched upon previously, as migration patterns of Russians and Slavs led to new homes in either the United States or Canada. In 2017 Australian Andrew O'Neil argued that, while the United States is the dominant power of the alliance, the other members of this selective group (Australia, Canada, New Zealand, and the United Kingdom) actually have a much more fluid relationship with the United States within the alliance and are more capable of defense policy other than merely consuming U.S. signals intelligence.[18] O'Neil also details the formation of the alliance in 1947, following victory in the Second World War but also as a result of the growing threat of the Soviet Union. Aside from the "Five Eyes," the security relationship between the two countries is interlinked through the North American Aerospace Defense Command (NORAD). This alliance was specifically set up so that the two North American powers would be able to deter Soviet attacks against the continent during the Cold War.[19] This framework of mutual defense was established during the Cold War, yet still remains applicable today.

Aside from the "Five Eyes," the security relationship between the two countries is interlinked through the North American Aerospace Defense Command (NORAD).

Like the United States, Canada sought to reorganize itself after the attacks on September 11, 2001. The adoption of the Anti-Terrorism Act (2001) granted further powers to defense personnel within the country.[20] A few years later, a nationwide poll found that 64 percent of respondents were more in favor of national security over personal liberty, as opposed to 32 percent the other way, paving the way for the Conservatives to retake control of the government. This view was reflected in the *Canadian Defence Strategy* under Premier Stephen Harper, which called for an increase in Canadian defense spending including investment in intelligence personnel and equipment.[21] Harper's successor, Justin Trudeau, decided to continue with increasing defense spending outlined by the addition of 300 new intelligence personnel from both the military and civilian sectors in order to meet obligations to military allies.[22] Beyond the national defense strategy for their country, security personnel at the Canadian Security and Intelligence Service (CSIS) have released academic papers on the threat emanating from Russia in acknowledgment of return to a traditional state-on-state conflict and forecasting another decades-long conflict between the United States and Russia.[23] In short, the literature regarding Canadian policy for defense and intelligence also seems to point toward increasing capabilities and concerns over the threat of Russia.

The literature regarding Canadian policy for defense and intelligence also seems to point toward increasing capabilities and concerns over the threat of Russia.

Demographics might also indicate the feasibility of recruiting these ethnic groups to respective intelligence communities for the purpose of watching Russia. In April 2018, George M. Reynolds and Amanda Shendruk authored a piece for the Council on Foreign Relations that detailed the demographics of the U.S. military. It found that the largest overwhelming demographic of personnel were white males, and that the majority of Great Plains states were supplying only upwards of 2,000 recruits statewide annually.[24] The idea of this article is similar to one regarding the Canadian military. In a 2008 article for the *Canadian Military Journal,* Hans Jung wrote that the majority of recruits to Canada's defense forces were "white males… coming from rural areas or from urban areas with a population of less than 100,000."[25] The problem with the demographics from both articles is that the term "white male" is used within the demographic but no further specificity. In the United States, the category "white" refers to ethnic backgrounds that span from Europe to the Caucasus and the Middle East. Should the idea of recruiting ethnic Slavs and Russians be deemed desirable for the intelligence communities of the United States and Canada, further research into ethnic demographics of current military force size would give a better indication of how many U.S. and Canadian citizens of these backgrounds are already interested in national

security. Similarly, further research into attitudes of ethnic Slavs/Russians from both countries should also be conducted. In 2015 the Pew Research Center released results from some surveys which found that both Canada and the U.S. were the strongest advocates of arming Ukraine to fight Russia as well as inviting Ukraine to join the North Atlantic Treaty Organization.[26]

Further research is needed into ethnic demographics of current force sizes to get an indication of how many of these ethnic people are interested in national security.

APPLICATION FOR OTHER THREATS

The central focus of this essay has been on the application of using ethnic minorities to fight Russia, but there are also opportunities for applying this concept of targeted recruitment of ethnic minorities to other problem areas as well. Besides Russia, the nation of most concern is China. Coincidentally, China, like Russia, also has a long history of migration to North America, providing communities of Chinese speakers, with the majority speaking either Mandarin or Cantonese.[27] The U.S. Census Bureau states that there are nearly 2,900,000 Chinese speakers in the United States, with Mandarin and Cantonese speakers at a little over 450,000 speakers each. Statistics Canada also reflects roughly 600,000 speakers each of Mandarin and Cantonese, putting Canada's Chinese-speaking population at 1,200,000. There are also enough numbers to continue this idea with Korean speakers and Persian speakers, in addressing the rogue states of North Korea and Iran. The U.S. Census Bureau puts the number of Korean speakers at 1,100,000 Americans while Statistics Canada puts the number at 160,000 speakers. In the U.S. there are also 391,000 Persian speakers while in Canada there are 225,000. These numbers indicate there are large enough populations for the Intelligence Community to look to for individuals who speak the language, but there are some drawbacks. As mentioned earlier, the demographical data regarding those who had served in the military did not dive very deeply into ethnic background. This means that it did not differentiate "Chinese" or "Korean" from "Asian" just as it did not differentiate "Russian" and "Slavic" from "White." Additionally, the U.S. Census Bureau adheres to the Office of Management and Budget's 1997 assertion that "white" includes "a person having origins in any of the original peoples of Europe, the Middle East, or North Africa" in terms of race for ethnic purposes. This would suggest further research is needed into ethnic demographics of current force sizes to get an indication of how many of these ethnic people are interested in national security, as mentioned earlier.

CONCLUSION

While the United States is clearly a dominant world power, one of its greatest weaknesses is a deficiency in foreign languages as the majority of its citizens speak only English. History has actually afforded the country the ability to mend this weakness to its advantage through patterns of migration. As geopolitical tensions between the United States and Russia are turning toward a new Cold War, the history of migration, specifically of Russian immigrants to the United States, has left a series of communities of disenfranchised people able to speak the Russian language (or a Slavic language close enough to facilitate learning Russian). This has also been true for Canada, the northern neighbor of the United States. Like migration, history has shown that the defense policies for these two countries, and their allies, has benefitted from using their ethnic minority groups. This was the case in the Second World War and the Cold War. With the resurgence of a geopolitical power struggle between the United States and the Russian Federation, it may become imperative that U.S. intelligence services make use of these ethnic minorities, plus the alliance relationship with Canada, to train the next generation of intelligence analysts and practioners for this new Cold War.

[Author's Note: Individual personnel are not named within this work, for their protection. The questions were asked in an academic setting within a private environment.]

NOTES

[1] *National Security Strategy of the United States of America, 2017*, Office of the President of the United States of America, accessed April 3, 2019, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.
[2] Mason Shuya, "Russian Cyber Aggression and the New Cold War," *Journal of Strategic Security* 11, no. 1 (2018): 1-18, https://scholarcommons.usf.edu/jss/vol11/iss1/2; Clint Walker, "Looking into the Language of Russians," Lecture, TEDxUMontana, Missoula, MT, February 20, 2015.
[3] Terrence G. Wiley, "The Foreign Language 'Crisis' in the United States: Are Heritage and Community Languages the Remedy?" *Critical Inquiry in Language Studies* 4, no. 2-3 (September 19, 2007): 179-205.
[4] Sebastiao Salgado and Ivan Chermayeff, "From Moscow to Brighton Beach," *World Policy Journal* 14, no. 1 (1998): 44, accessed April 3, 2019, http://0-search.ebscohost.com.lib.utep.edu/login.aspx?direct=true&db=a9h&AN=9706152113&site=ehost-live&scope=site.

[5] James J. Wirtz, "The Sources and Methods of Intelligence Studies," in *The Oxford Handbook of National Security Intelligence,* ed. Loch K. Johnson. (New York: Oxford University Press, 2010), 59-70.
[6] *National Intelligence Strategy of the United States of America, 2019*, Office of the Director of National Intelligence, accessed April 3, 2019, https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf; *Nomination of Gina Haspel to be the Director of the Central Intelligence Agency*, 115th Cong. 25 (2018) (statement of Gina Haspel, nominee to be Director of the Central Intelligence Agency), https://www.intelligence.senate.gov/hearings/open-hearing-nomination-gina-haspel-be-director-central-intelligence-agency#.
[7] *Putin's Playbook: The Kremlin's Use of Oligarchs, Money and Intelligence in 2016 and Beyond*, 115th Cong. 25 (2018) (statement of Steven Hall, Former CIA Chief of Russia Operations), https://docs.house.gov/meetings/IG/IG00/20190328/109160/HHRG-116-IG00-Wstate-HallS-20190328.pdf.
[8] Norman Saul, "American Collections on Immigrants and Émigrés from the Russian Empire," *Slavic & East European Information Resources* 4, no. 4 (September 1, 2003): 49-61.
[9] David Davies, "The Pre-1917 Roots of Canadian-Soviet Relations," *Canadian Historical Review* 70, no. 2 (1989): 180-205.
[10] Vadim Koukouchkine, *From Peasants to Labourers: Ukrainian and Belarusan Immigration from the Russian Empire to Canada* (Montreal: McGill-Queen's University Press, 2007), 4.
[11] "Polish/Russian - Soviet Exiles - Immigration...- Classroom Presentation | Teacher Resources," *Library of Congress*, accessed April 3, 2019, https://www.loc.gov/teachers/classroommaterials/presentationsandactivities/presentations/immigration/polish3.html.
[12] "Detailed Languages Spoken at Home and Ability to Speak English for the Population 5 Years and Over: 2009-2013," United States Census Bureau, accessed April 3, 2019, https://www.census.gov/data/tables/2013/demo/2009-2013-lang-tables.html.
"Linguistic diversity and Multilingualism in Canadian Homes," Statistics Canada, accessed April 3, 2019, https://www12.statcan.gc.ca/census-recensement/2016/as-sa/98-200-x/2016010/98-200-x2016010-eng.cfm.
[13] Stefano Luconi, "Italian Americans and the Invasion of Sicily in World War II," *Italian Americana* 25, no. 1 (2007): 5-22, http://0-www.jstor.org.lib.utep.edu/stable/41330565.
[14] Luconi, "Italian Americans," 2007.
[15] Joseph J. Trento, *The Secret History of the CIA* (New York: MJF Books, 2001).
[16] Jeremy Risen, *State of War: The Secret History of the CIA and the Bush Administration* (New York: Free Press, 2006).
[17] Damien Van Puyvelde and Stephen Coulthart, "The Intelligence Community Must Remove Barriers to Minority Recruitment," *Defense One*, January 25, 2016, https://www.defenseone.com/ideas/2016/01/intelligence-community-must-remove-barriers-minority-recruitment/125377/.
[18] Andrew O'Neil, "Australia and the 'Five Eyes' Intelligence Network: The Perils of an Asymmetric Alliance," *Australian Journal of International Affairs* 71, no. 5 (September 3, 2017): 529-543.
[19] Matthew Trudgen, "The Key to the Canada-United States Relationship: Homeland and Continental Defence in American Strategic Culture," *Canadian Foreign Policy Journal* 22, no. 2 (May 3, 2016): 184-198.
[20] Stéphane Lefebvre, "Canada's Legal Framework for Intelligence," *International Journal of Intelligence and CounterIntelligence* 23, no. 2 (February 26, 2010): 247-295.
[21] "Canada First Defence Strategy," Government of Canada, accessed April 3, 2019, https://www.canada.ca/content/dam/dnd-mdn/migration/assets/FORCES_Internet/docs/en/about/CFDS-SDCD-eng.pdf.
[22] "Strong Secure Engaged: Canada's Defence Strategy," Government of Canada, accessed April 3, 2019, http://dgpaapp.forces.gc.ca/en/canada-defence-policy/docs/canada-defence-policy-report.pdf
[23] "Russia and the West: The Consequences of Renewed Rivalry," Canadian Security Intelligence Service, accessed April 5, 2019, https://www.canada.ca/content/dam/csis-scrs/documents/publications/RUSSIA_AND_THE_WEST-ENG.PDF.
[24] George M. Reynolds and Amanda Shendruk, "Demographics of the U.S. Military," Council on Foreign Relations, April 24, 2018, https://www.cfr.org/article/demographics-us-military.
[25] Hans Jung, "Can the Canadian Forces Reflect Canadian Society?" *Canadian Military Journal* 8, no 3 (2008): 27-36, http://www.journal.forces.gc.ca/vo8/no3/jung-eng.asp.
[26] Jacob Poushter, "Key Findings from Our Poll on the Russia-Ukraine Conflict," Pew Research Center, June 10, 2015, https://www.pewresearch.org/fact-tank/2015/06/10/key-findings-from-our-poll-on-the-russia-ukraine-conflict/.
[27] Erika Lee, "The 'Yellow Peril' and Asian Exclusion in the Americas," *Pacific Historical Review* 76, no. 4 (2007): 537-562.

Mason Shuya is a graduate student at the University of Texas at El Paso and its National Security Studies Institute. He first earned a BA degree in Security Studies with the program and opted to continue with the MS in Intelligence and National Security Studies. While a student at UTEP, he has published and presented, both domestically and internationally, work focusing on the state of geopolitical relations among the United States, its allies, and the Russian Federation. His overseas experience includes intensive Russian language study in Estonia and Ukraine, as well as a research internship with the Terrorism Research Center, a think tank in Warsaw, Poland.

Russian Cyber Campaigns in Support of Military Operations

by MAJ (USA) John E. Arthur VI

OVERVIEW

This article is not designed to state specifically state that Russian-aligned cyber forces are acting in concert with the Russian government; it is an analysis of what is, not what may be. The truth of the situation regarding alleged Russian cyber network operations (CNO) is that there have been concerted cyber campaigns directed at the former Soviet Bloc nations of Estonia, Georgia, and Ukraine that have facilitated Russian strategic goals.

Frustratingly, the preponderance of information regarding computer network attacks (CNAs) tends to be relatively myopic in its scope. The reporting highlights the type of attack and its digital impact, but very rarely emphasizes the political/military impact of a cyber attack on an existing conflict or area of tension. This unintentional scoping tends to limit full understanding of CNOs and how they are becoming a new crucial tool or arm of statesmanship. This article's goal is to familiarize the reader with Russian Advanced Persistent Threats (APTs) and to provide a pattern analysis of the cyber campaigns surrounding the three aforementioned conflicts and how they supported military operations.

CYBER ATTACKS AND WAR

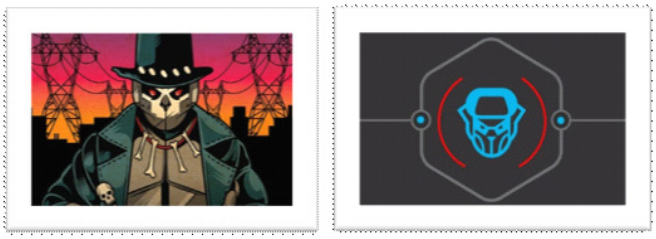
From a legal perspective, the formal definition of warfare, and what is meant by an act of war, primarily focuses on the usage of "force"; it is a poorly defined term.[1] Understandably, Western nations have been historically hesitant to group asymmetric forms of power—such as economic or political coercion—as an act of force or aggression.[2] Accordingly, when the United Nations Charter was designed, it was too proscriptive as to the definition of force; conversely, the North Atlantic Treaty Organization's charter was too broad.[3] The hazy demarcation of what is and is not war provided clarity only to international-level politics with respect to classical forms of conflict. This construct has benefited Western nations as it provided the ability to leverage their size, position, and economic power against smaller states or ostracized nations. CNAs further blur the demarcation line of war and, interestingly, also provide state actors an avenue to attack and potentially cripple rival nations in an obfuscated manner. Furthermore, the law of war has not focused heavily on the causal justifications for war as it was historically self-evident, in which one nation bombs or invades another, causing a loss of property and life.[4] Accordingly, offensive cyber operations reside in this international legal gray area due to a historic lack of specificity regarding the application of power, force, and war.

It must be noted that the majority of nations have started to align their cyber capabilities under their respective military organizations.[5] The inherent militarization of cyber operations will continue due to the idea that no sovereign nation will be able to wage war successfully against another nation without a coinciding cyber attack targeting the communications infrastructure. As demonstrated during the invasion of Operation IRAQI FREEDOM, it is effective to disable or destroy that critical infrastructure in order to render the command and control elements inert. Now, it can now be done not with a missile but with a cyber attack.[6]

RUSSIAN CYBER THREAT OVERVIEW

The digital community tries to identify offensive hackers or otherwise malicious cyber organizations. When a certain organization has been identified, whether through its routine techniques or other specific identifying actions, it will often be classified as a specified Advanced Persistent Threat (APT). There is some discrepancy between the number of Russian-flavored APTs. FireEye currently reports that there are two: APT28 and APT29.[7] APT28 has historically targeted Eastern European and NATO organizations and tends to focus on the defensive realm for both of those targets. APT29 tends to target and focus more on the policy side of Western governments.

CrowdStrike—another leading APT tracker—breaks down the Russian cyber threat into four different groups, each of which incorporates the sobriquet "BEAR" in its title.[8]



VOODOO BEAR and COZY BEAR Images[9]

There is some overlap regarding multiple APT tracking systems. For example, APT29 is also known as COZY BEAR. VOODOO BEAR has traditionally focused on espionage and sabotage; it is also the organization that has been identified as being responsible for the Ukrainian power grid attack in 2015, as indicated in CrowdStrike's artwork.[10] VENOMOUS BEAR and FANCY BEAR, which tend to specialize in phishing attacks and malware creation, are the remaining two APTs tracked by CrowdStrike.

Three Analyzed Cyber Campaigns

While there have been some ancillery Russian cyber attacks in the past—on October 26, 2002, two Chechen websites were targeted by alleged Russian actors following the Beslan massacre—this article focuses on analyzing the similarites surrounding alleged Russian CNAs in Estonia, Georgia, and Ukraine.[11] Each of these lengthy cyber campaigns was selected because: (1) Each country claimed Russia directly attacked it; (2) each campaign employed similar techniques, tactics, and procedures; and (3) each campaign demonstrated a continual escalation in ability and type of attack.

CAMPAIGN ANALYSIS METHODOLOGY

The data for this analysis were collected from open source websites for the three Russian cyber campaigns.[12] Due to the fact that some cyber attacks were enduring and some military attacks are still ongoing, only the initiation of a particular attack was charted. In order to be able to distinguish visually between an initiated cyber attack and an initiated military attack, cyber attacks were coded as a "2" and military attacks were coded as a "1" on the Y axis on all of the following graphs. Additionally, all cyber attacks are colored green and all of the kinetic military attacks are colored red. The dates or duration of the conflict comprise the X axis of all the charts.

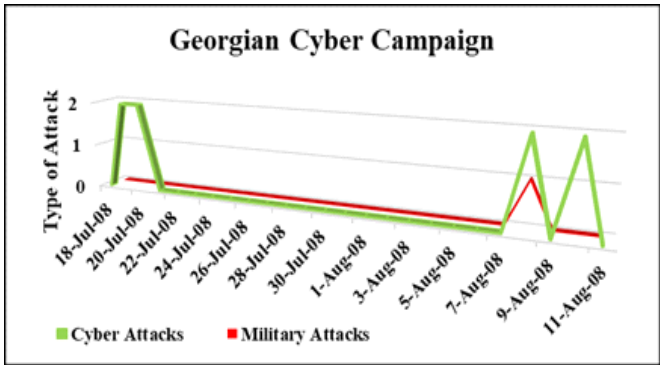
RUSSIAN-ESTONIAN CYBER CAMPAIGN

While the Estonian Cyber Campaign did not culminate in a physical Russian military attack, the Estonian Foreign Minister directly stated, "Russia is attacking Estonia…the attacks are virtual, psychological, and real," and publicly contemplated invoking Article 5 of the NATO Charter calling for the mutual defense of a NATO partner.[13] While this cyber campaign did not materialize into a physical invasion, due to its duration and scale of attack the Russian CNA directed against Estonia needs to be analyzed from a campaign perspective. The "Estonian Cyber Campaign" chart depicts the duration of the series of cyber attacks levied against Estonia starting on April 25, 2007, and culminating with the last wave of attacks which began on May 18, 2007. For charted elements that form a flat top (May 8 through May 9, 2007), there were numerous attacks initiated on those two days.

The propensity of the attacks against Estonia were Distributed Denial of Service (DDoS) attacks which are designed to overwhelm the target servers and bring the associated services that the servers provide to a halt. The sequencing of the targets was as follows: (1) Governmental sites; (2) newspaper organizations; (3) financial institutions; and (4) ISP providers. The suggested actors for these attacks were unidentified, but of Russian origin (for example, the Russian Business Network).[14]

The sequencing of targets is clearly indicative of an effort first to diminish state command and control and then to target further other information sources in an effort to either

obfuscate the nature of the cyber attack and/or diminish Estonians' confidence in their government. Such confidence would further be eroded as the individual's financial institutions were affected simultaneously with their ability to connect to the Internet in search of information regarding the CNO.



RUSSIAN-GEORGIAN CYBER CAMPAIGN

The "Georgian Cyber Campaign" chart depicts both the invasion of Georgia by Russia on August 8, 2008, and the series of CNAs levied against Georgia starting on July 19, 2008, and culminating with the last wave of attacks which began on August 10, 2008. For charted elements that form a flat top (July 19 through July 20, 2008), there were numerous attacks initiated on those two days.

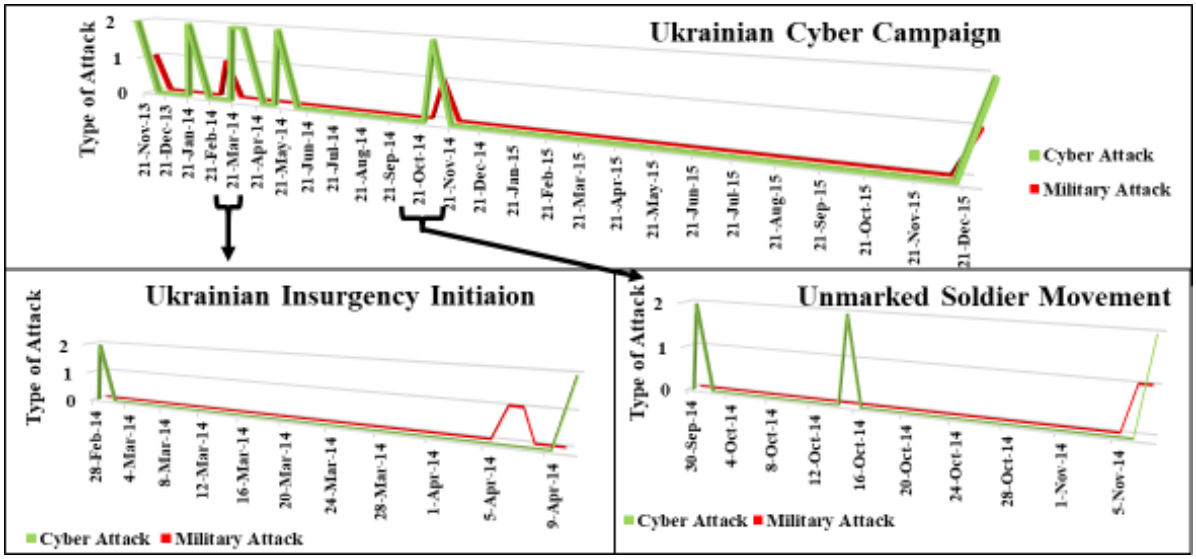
The propensity of the attacks against Georgia were botnet DDoS attacks—meaning that there were numerous computers that were utilized as a network to simultaneously attack the target—and SQL Injects, primarily delivered through email phishing. The sequencing of the targets was as follows: (1) Governmental sites; (2) news organizations; (3) IT infrastructure and associated servers; (4) Georgian financial institutions; and (5) Georgian education and business websites. The suggested actors for these attacks are APT28 and other unidentified Russian hackers.[15]

The sequencing of targets is very similar to the Estonian campaign; it is clearly indicative of an effort first to break down state command and control and then to further target information sources that would have provided the Georgians redundant communication channels. These cyber operations greatly facilitated the subsequent Russian invasion on August 8, 2008; the following cyber attack on August 10, 2008, helped diminish the possibility of insurgent action by limiting internal Georgian communications.

RUSSIAN-UKRAINIAN CYBER CAMPAIGN

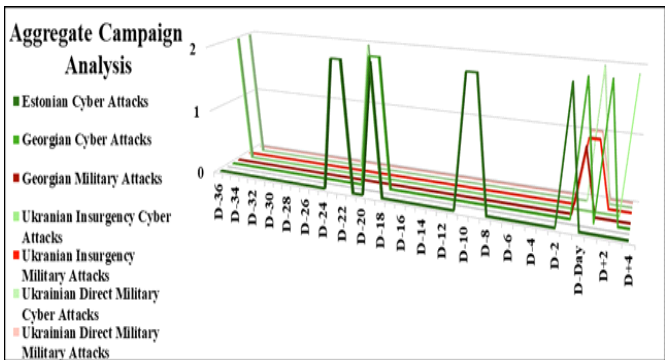
The "Ukrainian Cyber Campaign" chart depicts both the insurgency and military operations executed by Russia and the series of cyber attacks levied against Ukraine starting on November 21, 2013, through the attack on the Ukrainian power grid on December 31,2015, which could arguably have been both a cyber and military attack. Due to the fact that the Ukrainian conflict is still ongoing, the focus of the analysis was geared toward the two major military actions of that conflict: (1) The initiation of the Russian-aligned insurgency; (2) the first reporting of non-uniformed Russian soldiers moving into the region.

The EuroMaiden protests in November 2013 may have caught Russia unaware there was not an initial cyber operation; however, GRU documents obtained by *The Washington Post* showed that Russia began to organize a hasty social media disinformation campaign through the use of bots and other erroneous manufactured reports.[16] As Russia was not able initially to block the reporting of the protests, the second-best option was to begin to blur the factual reporting and manipulate public opinion toward a



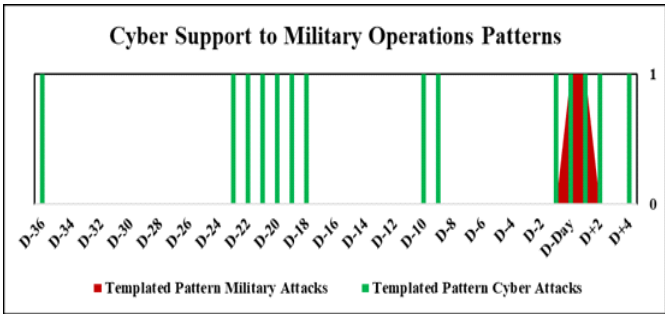
favorable Russian viewpoint. Aside from social engineering/information warfare-style attacks, malicious software (malware), such as Snake and X-Agent, was installed respectively in Ukrainian government and military artillery systems. Further botnet DDoS attacks targeted Ukrainian websites and also the Ukrainian electoral systems in 2014. As mentioned, a robust CNO targeting the Ukrainian power grid was successfully executed in 2015. The sequencing of the targets was as follows: (1) Ukrainian populace; (2) governmental systems; (3) military systems; (4) Ukrainian websites; (5) Ukrainian electoral systems; and (6) Ukrainian utility systems. Two identified actors for some of these attacks were FANCY BEAR (X-Agent) and VOODOO BEAR, which was behind the Ukrainian power grid attack.[17]

The sequencing of targets, while similar to the other cyber campaigns, is also significantly different due to the time required both to develop and deliver the malware onto the targeted systems. This is indicative of Russian cyber plans that had been occurring for at least a year prior to the actual attack. While the EuroMaiden protests may have caught Russia off-guard initially, it was well positioned to take advantage of internal Ukrainian turmoil.



RUSSIAN CNO PATTERNS IN EASTERN EUROPE

The "Aggregate Campaign Analysis" chart depicts all of the analyzed cyber campaigns put onto a D-Day scale, where D-Day is the initiation of military operations (or in the case of Estonia the initiation of the last wave of CNAs). Once this chart is put into a binary format (0 if no attack occurred and 1 if an attack occurred), as depicted in "Cyber Support to Military Operations," a distinct pattern is developed where one can identify three deliberate phases of cyber support to a potential military operation.



The first phase (usually occurring around D-36) tends to be a shaping operation, in that it creates the conditions for the success of the decisive operation or the kinetic attack.[18] This phase tends to target, via malware, governmental/military organizations or be geared toward Computer Network Exploitation (CNE) operations. The focus of this type of attack seems to be designed to seize the initiative through which the terms of the engagement will be dictated throughout the campaign.

The second phase (occurring between D-23 and D-18) is a sustaining operation usually marked by prolific CNA operations and that continues throughout the campaign. This phase tends to focus on IT/media/news targets and will also coincide with social media disinformation campaigns designed to dominate the information spectrum and also create confusion.

It is interesting to note that Estonia was attacked on D-10 through D-8 but not invaded, whereas the countries that were invaded were not subject to new cyber attacks during this period. This could potentially be an indication that the nature of the effort is purely a cyber campaign or it could be just an anecdotal anomaly.

Visual Depiction of the Templated Final Phase

The final phase, disruption, primarily focuses on dominating the adversary via inform-and-influence activities and through CNAs. These attacks tend to consist of DDoS/SQL Inject- type attacks aimed at the aforementioned targets but now also including financial and business institutions. By attacking and disrupting these types of targets, Russia will be able effectively to distract the targeted citizens from rapidly developing into an insurgency or organizing a more robust means of defense.

CONCLUSIONS

While the patterns presented in the "Cyber Support to Military Operations Patterns" are limited and based on a data set of only three different campaigns, their development is worth focusing on in order to build a holistic understanding of the true nature and effect of Russian cyber campaigns—whether or not they are directly ordered by the Russian state. The similar sequencing and targeting exhibited throughout these campaigns can be used as indicators to help template and forecast future Russian operations. This vein of research, the coupling of cyber and military operations, needs to be analyzed continually as nations' information and cyber capabilities become more advanced.

[Author's Note: All statements of fact, analysis, or opinion are those of the author and do not reflect the official policy or position of the Department of Defense or any of its components, the National Intelligence University, or the U.S. government.]

NOTES

[1] William H. Boothby, Conflict Law: The Influence of New Weapons Technology, Human Rights, and Emerging Actors (The Hague, Netherlands: T.M.C. Asser Press, 2014), 20-26.
[2] Heather Harrison Dinniss, Cyber Warfare and the Laws of War (Cambridge, UK: Cambridge University Press, 2012), 40-49.
[3] Ibid., 40-49.
[4] Jens D. Ohlin, "Cyber Causation," in Cyberwar: Law and Ethics for Virtual Conflicts, eds. Jens D. Ohlin, Kevin Govern, and Claire Finkelstein (Oxford, UK: Oxford University Press, 2015), 37.
[5] Larry May, "The Nature of War and the Idea of 'Cyber War'," in Cyberwar: Law and Ethics for Virtual Conflicts, eds. Jens D. Ohlin, Kevin Govern, and Claire Finkelstein (Oxford, UK: Oxford University Press, 2015), 15.
[6] Walter L. Perry, Richard E. Darilek, Laurinda L. Rohn, and Jerry M. Sollinger, eds., Operation IRAQI FREEDOM: Decisive War, Elusive Peace (Santa Monica, CA: RAND Corporation, 2015), 151, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1200/RR1214/RAND_RR1214.pdf.
[7] "Advanced Persistent Threat Groups," FireEye, last accessed May 5, 2019, https://www.FireEye.com/ current-threats/apt-groups.html.
[8] Adam Meyers, "Meet the Advanced Persistent Threats: List of Cyber Threat Adversaries," CrowdStrike, last modified February 24, 2019, https://www.CrowdStrike.com/blog/meet-the-adversaries/.
[9] Ibid.
[10] Adam Meyers, "CrowdStrike's January Adversary of the Month: VOODOO BEAR" CrowdStrike, January 29, 2018, https://www.CrowdStrike.com/blog/meet-CrowdStrikes-adversary-of-the-month-for-january-voodoo-bear/.
[11] "Russians wage cyber war on Chechen Web sites," Computer Crime Research Center, accessed May 10, 2019, http://www.crime-research.org/news/2002/11/Mess1502.htm.
[12] For further information and a listing of the source data used for analysis, please contact the author.
[13] P.W. Singer, and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford, UK: Oxford University Press, 2014), 110, 122.
[14] Andrezej Kozlowski, "Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan," special edition, *European Scientific Journal*, vol. 3 (Fall 2014): 238, http://www.eujournal.org/index.php/esj/article/ viewFile/2941/2770.
[15] "APT28: A Window into Russia's Cyber Espionage Operations?" Threat Research, FireEye, last modified October, 27, 2014, https://www.FireEye.com/blog/threat-research/2014/10/apt28-a-window-into-russias-cyber-espionage-operations.html.
[16] Ellen Nakashima, "Inside a Russian disinformation campaign in Ukraine in 2014," National Security section, *The Washington Post*, December 25, 2017, https://www.washingtonpost.com/world/national-security/inside-a-russian-disinformation-campaign-in-ukraine-in-2014/2017/12/25/f55b0408-e71d-11e7-ab50-621fe0588340_story.html?noredirect=on&utm_term=.46cef0fddfd7.
[17] "CrowdStrike's January Adversary of the Month: VOODOO BEAR" CrowdStrike, January 29, 2018, https://www.CrowdStrike.com/blog/meet-CrowdStrikes-adversary-of-the-month-for-january-voodoo-bear/.
[18] ADP 3-0: Unified Land Operations (Washington, DC: Headquarters, Department of the Army, 2017), 13, https://www.army.mil/e2/rv5_downloads/info/references/ADP_3-0_ULO_Oct_2011_APD.pdf.

MAJ (USA) John E. Arthur VI holds a BA in International Relations from the Virginia Military Institute. He graduated from the National Intelligence University in 2019, earning a Master of Science and Technology Intelligence degree with dual concentrations in Cyber Intelligence & Data Analytics and Emerging Technologies & Geostrategic Resources. This article is based on a paper he wrote while a student at NIU's Anthony G. Oettinger School of Science and Technology Intelligence. Currently John serves as the S3 of the National Ground Intelligence Center (NGIC) in Charlottesville, Virginia.

Intelligence Reform:
The Need for Empowerment of the Director of National Intelligence

by Kimbra L. Fishel

OVERVIEW

Empowerment of the Director of National Intelligence is needed to facilitate coordination, direction, and integration of the U.S. Intelligence Community. Peer competitors, emerging nuclear and potential nuclear powers, and non-state entities threaten U.S. security and dictate the need for such action. Greater collaboration, coordination, and integration of the 17 intelligence agencies is required to effectively meet an overlapping international and domestic security environment. This article offers policy guidelines for empowering the Director of National Intelligence to perform the job intended by the Intelligence Reform and Terrorism Prevention Act of 2004.

INTRODUCTION: THE BOTTOM LINE

Current and future threats to the security of the United States indicate the need for intelligence integration at the highest level to facilitate coordination, direction, and collaboration of the Intelligence Community (IC). In December 2017, the Trump administration released the *National Security Strategy of the United States* (NSS). Peer competitors such as Russia and China, threats from emerging nuclear and potential nuclear powers such as North Korea and Iran, and asymmetric threats from non-state entities such as ISIS and Al Qaeda are presented as main challenges to U.S. national security.[1] While the U.S. intelligence system is better equipped to meet peer-level threats, those from lower-level nuclear powers and asymmetric entities are problematic due to the closed nature of the system and the nebulous structure of the networks. Greater collaboration, coordination, and integration of the 17 separate intelligence agencies is required to meet these asymmetric challenges more effectively. Building upon the theories of Graham Allison and Arthur Lykke, this article offers policy guidelines for empowering the Director of National Intelligence (DNI) to perform the job that the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) intended.[2]

THE PROBLEM IN HISTORICAL AND CURRENT CONTEXT

Al Qaeda's 9/11 attacks on the American homeland ushered in the largest reorganization of U.S. government since the 1947 National Security Act. The Homeland Security Act of 2002 sought to prevent, respond to, and mitigate terror attacks within the United States.[3] *The Homeland Security Act* was followed by the Intelligence Reform and Terrorism Prevention Act of 2004. The IRTPA resulted from the report of the National Commission on Terrorist Attacks Upon the United States, which included a reassessment of the IC and how better integration and collaboration of it could be achieved to prevent future terrorist attacks in a new threat environment.[4] The IRTPA sought to alleviate the coordination problem among intelligence agencies by creating the position of Director of National Intelligence. The legislation attempted to designate the DNI as the ultimate person in charge of the intelligence bureaucracy, subordinate only to the President.

There are those who take issue with the findings of the 9/11 Commission Report that resulted in the IRTPA and the reorganization of the IC. For example, Stephen Marrin argues that the attack on 9/11 was a result of policy failure rather than a failure of strategic intelligence. He insists that that the U.S. was aware of the threat from Al Qaeda, but his quote from Benjamin and Simon is telling, that "the nation's intelligence and law enforcement authorities and its political leaders were put on notice that a new brand of terrorism that aimed at mass casualties had arisen."[5] Perhaps Paul Pillar overstates the case when he argues that the 9/11 Commission deliberately misrepresented the strategic intelligence available prior to 9/11, defending his own work in the area. However, he does raise legitimate questions regarding the nature of the changes wrought by a commission that mischaracterized the nature of the intelligence leading up to 9/11.[6] Finally, in an extremely well-written article, retired LTG (USA) General William Odom maintains that the new law was ill-conceived and that what emerged from the 9/11 Commission was an outrageous view that held the IC responsible for Presidential decision-making.[7]

While the characterization of the reforms is debatable, what is clear is that although a massive reorganization of the IC did occur, along with a realization that reform was required to meet current and future threats to the United States, the full intent of the IRTPA was not realized. Failure occurred at the implementation phase of putting the law into routine practice, resulting in the DNI lacking the control over the IC needed. Habeck and Stimson contend that this problem is made manifest in the following ways: the DNI does not oversee the entire community and only the CIA reports directly to the DNI; the CIA leadership resented intrusion of the DNI into CIA affairs; the DNI is not a command position as is the Secretary of Defense; and the DNI must be assured of Presidential support for success.[8] In addition to the DNI-DCIA relationship tension, a third player, the Under Secretary of Defense for Intelligence, also is in the mix. All three players jockey for positions of influence with the President and control over the IC. As a result, IRTPA's goal of a better system of coordination to meet threats remains problematic. The main question is how to strengthen the DNI most effectively to ensure a level of oversight for coordination and collaboration without stifling the need for disparate though cooperating entities at federal, state, and local levels required by a vast array of threats.

Intelligence scholars often discuss the need for intelligence reform based upon the major changes within the international system and that the strategic environment of the 21st century is fundamentally different than that of the Cold War era.

Reform of the IC does not exist in a vacuum. Rather, it exists within a political landscape at both international and domestic levels. According to Steven Salazar, the purpose of the U.S. Intelligence Community is to support military operations and inform policymakers to enhance the national security of the United States.[9] While intelligence customers have increased in number in the post-Cold War era, Salazar's contention is correct. The IC exists as a tool to be used in support of U.S. national security interests. This is as true today as it was when the community had its origins during World War II (hereafter WWII) and afterward evolved to meet the Soviet threat. The international setting is one of conflict and transformation.

Intelligence scholars often discuss the need for intelligence reform based upon the major changes within the international system and that the strategic environment of the 21st century is fundamentally different than that of the Cold War era. Roger George argues that the intelligence system evolved to meet a Soviet threat and not the myriad of threats present today.[10] George states, "A world dominated by a single dominant threat—the Soviet Union—gave focus and purpose to U.S. foreign policy; it was the 'main enemy' around which much of U.S. intelligence analysis was built. The twenty-first century presents a far more diverse, dynamic, and uncertain set of policy challenges and intelligence requirements."[11] However, what such scholars miss is that it is necessary to look within the outer framework of the bipolar model to see what transpired during the Cold War. Such an examination shows that while the U.S. was focused on the Soviet threats the threat environment was not static, and the IC operated to meet a variety of threats that emerged as the Cold War was raging. See, for example, the memoirs of former Directors of Central Intelligence (DCIs) Allen Dulles,[12] Richard, Helms,[13] William Colby,[14] Stansfield Turner,[15] and George Tenent,[16] who lay out the historical development of the CIA and the IC from its beginnings to the IRTPA and the context in which it operated. These practitioners show a world faced with a dynamic and changing threat environment that increasingly became more complex over time. An acknowledgment of what has not changed as well as what is different has implications for IC reform.

While the Cold War era was a bipolar international system, it was a dynamic one that moved from a tight bipolar to a loose bipolar system. In the post-WWII world, the poles tightly controlled their spheres of influence. However, this tight control changed with the Sino-Soviet split and the emergence of non-aligned powers. To be sure, the Soviets and the Americans remained the premier powers in a bipolar system, but new threats were emerging, in which the superpowers no longer completely controlled all states within the system. John Spanier coined the term "bi-polycentric" to describe this loosening of bipolar ties.[17] In response, the national-level IC turned its attention beyond the Soviet Union to address a changing international environment, though within a Cold War context.

What is interesting to note is that it was during the Cold War that the Intelligence Community turned its sights on aspects of the world that many argue today's IC must target. John Hedley states it this way: "Global threats to US national security would require global information. Intelligence, heretofore thought of essentially in terms of military operations during war, would need to cover not just enemy military forces but also political and economic developments world-wide."[18] In short, today's IC evolved to meet a global threat environment with many areas of overlap with that of the Cold War environment, including a major power threat from Russia which is similar though not identical to that of the former USSR, and emerging threats from rogue nations which had their origins during the Cold War. The difference now is the increased threat capability of all entities, including cyber capabilities, and the ability of

certain asymmetric entities such as Al Qaeda and ISIS to conduct successful attacks on the state, including infiltration of the domestic state. The result is an easing of the barrier between what constitutes a domestic and what constitutes an external or foreign threat. It is within this political landscape that today's IC evolved. It is in this political landscape that the U.S. government sought to advance and protect its national security interests using the IC as a major tool in the process.

The current Intelligence Community represents an evolution from its World War II beginnings through the present post-Cold War international system.

As such, the current Intelligence Community represents an evolution from its WWII beginnings through the present post-Cold War international system. It consists of 17 separate agencies loosely coordinated by the DNI.[19] Although Zegart discusses a design of the IC, there really is not an original design.[20] Rather, it began as Navy and Army Intelligence. The OSS was created by Franklin Roosevelt during WWII, based upon the recommendation of MG (USA) William Donovan. According to Jeffrey Richelson, the establishment of the OSS represented a revolution in U.S. intelligence because of the various functions it performed, including espionage, covert action, counterintelligence, and analysis, and because of "the breadth of its intelligence interests and its use of scholars to produce finished intelligence."[21] At the end of WWII, Harry Truman disbanded the OSS, sending parts of it to State and the military services. He retained a rump organization to create the Central Intelligence Group (CIG) in February 1946.[22] It was the CIG that provided the nucleus of the CIA. It is from this inception that the IC evolved throughout the Cold War to meet a Soviet threat and then to counter a growing number of emerging and changing threats throughout the world. The office of the DCI was created to coordinate all intelligence activities but did not have the power to do so. As the number of agencies increased, there were efforts to superimpose coordinating elements. For example, one of those was the Intelligence Community Staff in the 1970s. Nonetheless, optimal coordination among the vast number of bureaucratic agencies remained elusive.[23]

Presidential administrations from Truman to George W. Bush recognized the need for better coordination and control of the intelligence organization, but efforts to create greater control were resisted. Richard Best characterizes that resistance in the following way:

> Yet, it was effectively resisted for a number of reasons: among them, a determination by Presidents not to give the Legislative Branch an opportunity to reorganize an essential part of the Executive Branch's policymaking machinery; resistance by the Pentagon to any innovation that might reduce intelligence support to the military; the powerful inertia of the congressional appropriations and authorization processes; and the determination by the Central Intelligence Agency (CIA) to retain direct access to Presidents.[24]

Resistance to change was both structural and cultural in nature, involving the natural inclination of branches of government to protect their own turf, the bureaucratic wrangling within the federal government, and the culture of agencies such as the CIA that were not inclined to share information readily. It is argued that September 11 demonstrated the failure of U.S. intelligence to prevent a major attack upon the United States. According to Melvin Goodman, it exposed the inability of analysts to "perform strategic analysis, challenge flawed assumptions and share sensitive secrets."[25] Goodman correctly states the IC did not imagine a terror operation utilizing commercial aircraft as weapons within the United States, although Osama bin Laden declared war on the United States in the 1990s and the CIA was tracking Al Qaeda operatives. However, Goodman errs in asserting that strategic intelligence was not provided by the community or that the political leadership was not aware of the Al Qaeda threat. The IC errors that were present, particularly at the operational and tactical levels, were embedded within a national mindset that tended to view terror as a criminal act rather than a tactic in warfare. 9/11 demonstrated that Al Qaeda was utilizing the tactic of terror in its war against the West in spectacular events. It was after this attack that the U.S. really began to view terror as a tactic in warfare rather than merely a criminal action. Consequently, the U.S. began to adjust its policies based on this new realization.[26]

The shock of 9/11 provided the necessary catalyst to overcome resistance to reform. What was needed was better collaboration and sharing of information, although holdover issues from pre-9/11 days remained. Specifically, the nature of the terror threat required cross-sharing of information, yet there remained an inherent tendency not to do so. For example, the CIA specifically guards its information[27] and does so with extensive use of the Originator Controlled—ORCON—protective marking,[28] and turf wars abound.

IRTPA's creation of the DNI was an attempt to address and rectify these issues. The Joint Chiefs of Staff Chairman's role in the strategy and budgetary process under the Department of Defense Reorganization Act of 1986, also known as Goldwater-Nichols, served as the model for the DNI role

under IRTPA.[29] Although the law established this new role for the DNI, the organizational structures within the U.S. government and the personalities involved in competing agencies must implement the law into practice. During the George W. Bush administration, the relationship between the DNI and the DCIA was in the process of being established by the office holders, Mike McConnell and Michael Hayden, respectively. It is interesting to note that Hayden opposed the 9/11 Commission's report urging the realignment of the Intelligence Community because he believed it would be a "drain on time and energy."[30] Hayden maintains that DCI George Tenent was a strong figure in 2004 and that a "feckless DNI would actually make matters worse."[31]

As Hayden correctly indicates, the relationship between the DNI and the DCIA is one of the most important relationships within the Community.[32] It is this relationship that failed to solidify as a routine practical application of IRTPA. Under the Obama administration, the DNI was largely emasculated as the DCIA was elevated to NSC principal status by the President.[33] Under the Trump administration, the DCIA remains the most powerful member of the IC, and the relationship between the DNI and other agency heads remains unclear. However, the Undersecretary of Defense for Intelligence (USDI) is almost, if not more of, a threat to the desired role of the DNI than the DCIA. The USDI retains control of all DoD agencies, including DIA, NSA, NGA, NRO, and the service intelligence organizations. The USDI also influences the intelligence elements of the Joint Staff and the combatant commands.[34] The changing nature of the capabilities of the DNI and challenges to the DNI's preeminent role stand in conflict with the intent of the DNI's role under IRTPA. As a result, there remains a vast number of agencies and a lack of solid means of coordination despite the 2004 law.[35] If the issue of the DNI's role is resolved, then there is the prospect for a better coordination system to meet threats.

APPLYING ALLISON TO INTELLIGENCE

The United States operates in a Westphalian international system in which the primary actors are nation-states. Despite the rise in non-state actors in this system, including international governmental organizations (IGOs), non-governmental organizations (NGOs), multinational corporations (MNCs), and asymmetric entities including terror organizations, the state remains the defining unit of the system. Classical realist theory can be traced back to at least Thucydides and the famous *History of the Peloponnesian War*, but the father of modern realism is Hans Morgenthau. His seminal book *Politics Among Nations*[36] remains a premier work in modern IR realist theory, and it is upon this theory that other works such as Graham Allison's classic *Essence of Decision*[37] builds.

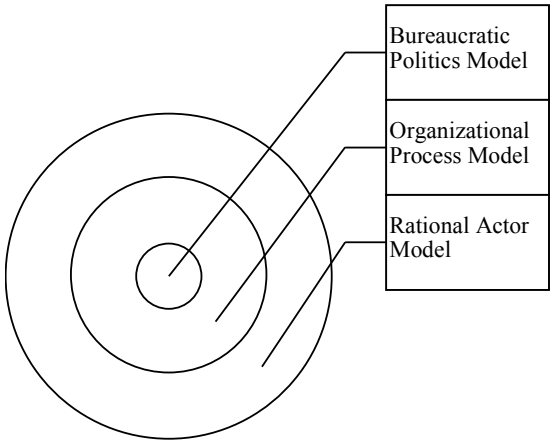
Applying Allison's theoretical framework to the problem of reform of the Intelligence Community is advantageous as it is encompassing enough to take in the strategic political landscape in which the community operates as well as the ingrained cultures in diverse agencies and the individual motivations and perceptions of important players.

Allison utilizes a case study of the Cuban Missile Crisis to define three different lenses or models: the Rational Actor Model, the Organizational Process Model, and the Bureaucratic Politics Model, through which decision-making occurs.[38] Model I is the Rational Actor Model, which is reminiscent of Morgenthau. According to Allison, analysts see states as unitary rational actors, and actions undertaken by states can be understood in terms of the strategic problems faced by the state. Model II Is the Organizational Process Model, which sees choices made by governments as products of standard operating procedures or regular behavior patterns. Model III is the Bureaucratic Politics Model, which looks at outcomes as a result of bargaining among players, the individuals involved, and their perceptions and motivations.

Applying Allison's theoretical framework to the problem of reform of the Intelligence Community is advantageous as it is encompassing enough to take in the strategic political landscape in which the community operates as well as the ingrained cultures in diverse agencies and the individual motivations and perceptions of important players. Often, theories of organizational change or bureaucratic bargaining and negotiation neglect the overall strategic setting in which such interactions or procedures take place.

Allison's models can be conceptualized in Figure 1. The IC is illustrated as an onion in which layers are pulled back to reveal its functioning. The outer portion represents the Rational Actor Model, in which the state interacts with the international environment, and individuals in the policy community act according to this model. One ring inward represents the Organizational Process Model, composed of standard operating procedures of bureaucratic organizations. The second inward portion of the sphere represents the Bureaucratic Politics Model, in which bargaining, compromise, and turf wars are played out by individuals with their own characteristics, personalities, and beliefs.

Figure 1: Illustration of Graham Allison's Conceptual Models



The outer layer, the rational actor, views the state as responding to the strategic challenges presented by a calculation of costs and benefits of actions. The IC provides valuable analysis of information that is one input toward the calculation of costs and benefits. It is also a valuable supplier of information as to the nature of the strategic environment. If policy leaders fail to grasp the nature of the environment in which they are operating at the strategic level, errors can occur regardless of good intelligence and analysis, and cost/benefit determinations will suffer. This is the real problem at the strategic level with the 9/11 attacks. Despite solid intelligence warnings at the strategic level of the danger posed by Al Qaeda and Osama bin Laden, a failure to understand the nature of the threat as one not just of terrorism but of an asymmetric, ideologically-based Islamist attack on the existing international structure dominated by the U.S. and Western powers likely prevented the types of actions required at the tactical and operational levels needed to avert the attacks. In short, preventing 9/11 required an active engagement in war. Imagine such measures as the USA PATRIOT Act, or the crackdown on airport security, or the invasion of Afghanistan happening before 9/11. It took a major attack upon the United States to move the country to a war footing and attempt the changes that the IRTPA envisioned.[39]

If the outer layer is peeled back, the Organizational Process Model shows that there are sets of standard operating procedures that organizations follow within the state. The IC is no exception. The IRTPA created the Office of the DNI to give the IC the needed cohesion and direction in response to an international environment that contained a new type of threat. In so doing, it attempted to rework the standard operating procedures to make the system more responsive to its different parts. The concept of the DNI as head of the IC, modeled after the Chairman of the Joint Chiefs of Staff, could provide the needed authority for vertical coordination. Unfortunately, organizational processes are highly resistant to change and the DNI was not empowered enough to do the job the legislation envisioned. The role of the DNI was further complicated by the USDI, an office created by former Secretary of Defense Donald Rumsfeld to control the DoD agencies with the greatest proportion of the intelligence budget, and President Obama's elevation of the DCIA to principal status on the NSC. Further exacerbating the problem was President Obama's siding with his DCIA over his DNI in a minor dispute over the appointment power of the DNI for the senior intelligence representative at U.S. embassies.[40]

If another layer is peeled back, a final element comes into play, the individual actors involved, all with different perceptions, ideals, and places of power in the hierarchical structure. Bureaucratic politics, turf wars, and organizational cultures ingrained into the individual thought process all play out as political maneuvering, bargaining, and fighting among individual actors. This can be seen in the conflicts between the DNI and the CIA and the role each plays vis-à-vis the ultimate person in charge, the Commander in Chief. The implementation of the law failed to establish the clearly defined role of who is in charge of the Intelligence Community below the President.

The challenge for the DNI is that he needs to gain and maintain the trust of the DCIA and USDI in his role representing the IC, and the President must view the DNI as his principal advisor for the IC.

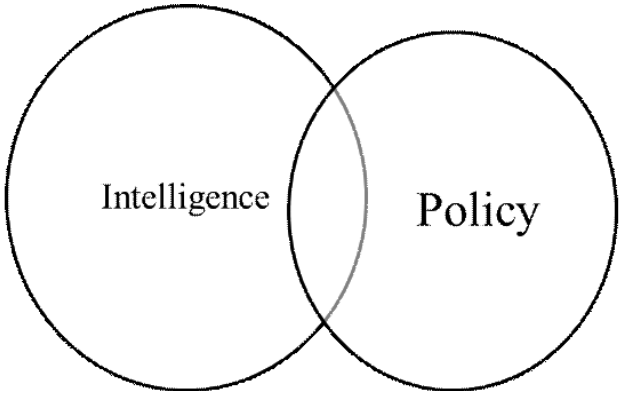
What does empowerment of the DNI look like? Allison's Model II suggests that the DNI needs to be understood within the IC as first in line of communication with the President. A standard operating procedure could be established that solidifies the DNI as the principal advisor to the President of the IC along similar lines to the CJCS. The CJCS does not command the other members of the JCS as they remain advisors to the President and the Secretary of Defense, but the CJCS is the principal military advisor. The other members of the JCS retain the right of direct communication with their superiors but usually do not exercise it because the CJCS is responsible for carrying their concerns forward. The challenge for the DNI is that he needs to gain and maintain the trust of the DCIA and USDI in his role representing the IC, and the President must view the DNI as his principal advisor for the IC. This was accomplished with CJCS through at least 40 years of evolution with a series of legislative acts

beginning with the 1947 National Security Act up through Goldwater-Nichols of 1986. In addition, there is a common underlying military culture present, and all service secretaries are subordinate to the civilian Secretary of Defense. There is no "Secretary of Intelligence" equivalent to the Secretary of Defense due to the nature of the intelligence system.

With the creation of the DNI, the IRTPA already allows for this type of evolution of the DNI, but key to this establishment given an absence of an underlying commonality of culture is the relationship between the DNI and the President and the President's willingness to empower the DNI in such a manner. Allison's Model III suggests that the bureaucratic politics involved including turf wars, political bargaining, and individuals jockeying for power will work against the establishment of such a procedure. This makes it imperative for the President to define clearly the relationship and, given that Presidents change every four or eight years, for that system to become so engrained that this type of DNI role becomes established across administrations.

The worlds of policy and intelligence are not equivalent, although there is overlap. Figure 2 illustrates where the worlds of policy and intelligence intersect. Note also that these are dynamic spheres, as members of the intelligence and policy communities move back and forth from one realm to the next.

Figure 2: Policy and Intelligence Overlap



The policy and intelligence spheres both contain areas that are independent of the intelligence and policy realms. From the policy sphere, for example, the President is the preeminent player and intelligence is one ingredient that goes into the formulation of policy and decision-making. It is, however, not the only factor. In the intelligence realm, for example, analysts reside in this sphere whose main purpose is to provide information and analysis of information, but not to make policy. There is, however, an area of overlap in which members of different agencies from each sphere come together. The President's National Security Council falls into this area of overlap as do the Principals Committee and the Deputies Committee. Examples of roles that fall into this area of overlap are the President, the Assistant to the President for National Security Affairs, the Secretary of Defense, the Secretary of State, the Director of National Intelligence, the Chairman of the Joint Chiefs of Staff, the DCIA, and the USDI. It is in this area that the President can elevate the DNI above the DCIA and USDI, making him the preeminent player and most influential of the intelligence heads in the policy arena. Being empowered with budgetary authority and influence gives him needed control for better vertical collaboration among agencies. This in turn allows for allocation of resources and providing incentives and disincentives on a horizontal basis to encourage needed integration and sharing of information. The key vehicle to achieving agency collaboration is the relationship among the DNI, the DCIA, and the USDI. If this problem is resolved, the other agencies should fall in line, setting the stage for better integration at both federal and state levels. One example of a solution would be for the DNI alone to sit on the NSC and the Principals Committee. The DCIA and USDI would sit on the Deputies Committee.

CONCLUSION: GUIDELINES FOR EMPOWERMENT OF THE DNI

The multidimensional nature of the global strategic threat environment requires an Intelligence Community that can target its assets appropriately. This is best accomplished through effective vertical integration of the IC to ensure horizontal collaboration. Building upon Allison's Models II and III, policy recommendations for empowering the DNI are as follows:

> (1) Allison's Model II indicates a new standard operating procedure for the IC should be established at the NSC level. The President has the ability and authority to do this, and no further legislation is required. This option rests upon the willingness of the President to regard the DNI in the same vein as the CJCS. The DNI becomes the main point of communication between the President and the heads of the intelligence agencies. This places him in a unique position to influence policy without stifling the interactions and healthy competitiveness of other agencies. In this way, the DNI becomes de facto what was envisioned by the IRTPA. A new operating procedure could be the catalyst for integrative change across the board.[41] The formal moving of the DCIA from the NSC Principals Committee to the Deputies Committee, and the inclusion of the USDI in the Deputies

Committee while the DNI sits on the NSC and Principals Committees, is a recommended course of action. This change also allows the DCIA or the USDI (depending on the NSC agenda) to sit in for the DNI if he is not available.

(2) The budgetary role of the DNI becomes like that of the CJCS. In this way, the DNI has influence over allocation of resources and, through such influence, can establish priorities over those resources and affect distribution down to the state and local level. This provides incentives for integration and collaboration at the horizontal levels. Whereas the DNI is responsible for the National Intelligence Program, the Military Intelligence Program falls under the responsibility of the USDI for the Secretary of Defense. The DNI must have the capability of reviewing both budgetary documents and reporting his objections to the President for modification. This type of budgetary oversight would strengthen the DNI in ways that are comparable to the CJCS. It requires the President to direct the Secretary of Defense to ensure the DNI has access to the Military Intelligence Program for oversight purposes.

(3) Allison's Model III indicates that the President must choose powerful individuals whom he views as trustworthy to hold the position of DNI. He must also make sure the DNI is also trusted by both the DCIA and the USDI to take their concerns to the President as the CJCS does with the service chiefs. The President must make clear the role of the DNI vis-à-vis himself in the policymaking process to other members of the Cabinet and the Intelligence Community. Those nominated by the President to hold the head position of other important intelligence agencies must understand the DNI position and the need for such a position given the threat environment. Choosing the right people is key to overcoming the bureaucratic politics tendency to engage in turf wars and instead finding the compromise needed among the agency heads for successful establishment of the new operating procedure. These suggestions fulfill institutional change guidance by altering behavior of individuals, which allows for the new standard operating procedure to become routinized and poised for integrative change.[42] It may set the stage for cultural change within agencies, but it does not require such change for action. The DNI must demonstrate by doing that he will honestly and fairly carry the concerns of the DCIA and the USDI to the President, and the USDI and DCIA must work out between themselves and the DNI the lines of communication. The DNI must also facilitate direct communication among these agencies' heads and the President when it is needed.

(4) Once the vertical collaboration and horizontal integration are established at the federal levels, the lines of communication and integration can be funneled to the state and local levels through fusion centers or equivalent entities. The challenge here is ensuring that, in addition to horizontal flow of information, information is also funneled vertically from state to federal levels where ultimate decision-making authority resides regarding overall U.S. national security. When this is accomplished, full integrative change across the board may be realized. The best use of the fusion centers in both horizontal and vertical integration is an avenue for future research.

These four policy recommendations are a start at reforming the Intelligence Community to improve vertical collaboration so that sharing of information and horizontal integration are possible through federal, state, and local levels. The IC operates in a high stakes world of power politics, where international and domestic threats blend and reform is necessary to meet a very dangerous world. However, reform does not take place in a vacuum but rather exists within a federal system of government composed of different entities and agencies, of which the Intelligence Community is only a part. The recommendations proposed herein work within that system to achieve meaningful reform that is doable.

NOTES

[1] *National Security Strategy of the United States*, The White House (December 2017), https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017- 0905.pdf.
[2] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. 108-458 (December 17, 2004), https://www.gpo.gov/fdsys/pkg/PLAW-108publ458/pdf/PLAW-108publ458.pdf
[3] Homeland Security Act of 2002, Pub.L. 107-296, 116 Stat. 2135 (November 25, 2002), https://www.dhs.gov/homeland-security-act-2002
[4] National Commission on Terrorist Attacks Upon the United States (2004), https://9-11commission.gov/report/.
[5] Marrin, Stephen, "The 9/11 Terrorist Attacks: A Failure of Policy Not Strategic Intelligence Analysis," *Intelligence and National Security*. 26, nos. 2-3 (April-June 2011): 182-202.
[6] Pillar, Paul R., "Good Literature and Bad History: The 9/11 Commission's Tale of Strategic Intelligence," *Intelligence and National Security* 21, no. 6 (December 2006): 1022-1044.
[7] Odom, William E., "Intelligence Analysis," *Intelligence and National Security* 23, no. 3 (2008): 316-332.
[8] Habeck, Mary, and Charles D. Stimson, "Reforming Intelligence: A Proposal for Reorganizing the Intelligence

Community and Improving Analysis," *Backgrounder*, Washington, DC:
The Heritage Foundation, No. 3129 (August 29, 2016): 1-10.
[9] Salazar, Steven L., "Chapter 8: Transforming the Intelligence Community," *Transformation*
Concepts for National Security in the 21st Century (2002): 247-284.
[10] George, Roger Z., "The Art of Strategy and Intelligence," *Analyzing Intelligence National*
Security Practitioners' Perspectives, 2nd ed., Roger Z. George and James B. Bruce, eds. (Washington, DC: Georgetown University Press, 2014).
[11] Ibid.
[12] Dulles, Allen, *The Craft of Intelligence* (New York: Harper Collins, 1963).
[13] Helms, Richard, *A Look Over My Shoulder* (New York: Random House, 2003).
[14] Colby, William, *Honorable Men* (New York: Simon & Schuster, 1978).
[15] Turner, Stansfield, *Burn Before Reading* (New York: Hatchette Books, 2005).
[16] Tenent, George, *At the Center of the Storm* (New York: Harper Collins, 2007).
[17] Spanier, John W., *Games Nations Play* (Washington, DC: CQ Press, 1995).
[18] Hayden, Michael V., "The State of the Craft: Is Intelligence Reform Working?" *World Affairs*
Journal (September/October 2010): 23, http://www.worldaffairsjournal.org/article/state-craft-intelligence-reform-working.
[19] Richelson, Jeffrey T., *The US Intelligence Community*. 7th ed. (Boulder, CO: Westview Press,
2016): 11.
[20] Zegart, Amy B., *Flawed by Design: The Evolution of the CIA, JCS, and NSC* (Stanford, CA: Stanford University Press, 1999).
[21] Richelson, *The US Intelligence Community,* 18.
[22] Hedley, John H., "The Evolution of Intelligence Analysis in the US Intelligence Community," *Analyzing Intelligence National Security Practitioners' Perspectives*. 2nd ed. Roger Z. George and James B. Bruce, eds. (Washington, DC: Georgetown University Press, 2014): 25.
[23] Fishel, John T., *American National Security Policy Authorities, Institutions, and Cases* (Lanham, MD: Rowman & Littlefield, 2017): 19-20.
[24] Richard A. Best, Jr., "Leadership," 254.
[25] Goodman, Melvin A., "9/11 The Failure of Strategic Intelligence," *Intelligence & National*
Security 18, no. 4 (Winter 2003): 59-71.
[26] National Commission on Terrorist Attacks Upon the United States (2004), https://9-11commission.gov/report/.
[27] Salazar, "Transforming the Intelligence Community," 263.
[28] Fishel, John T., author's personal communication with former national-level analyst, January 2018.
[29] Goldwater-Nichols Department of Defense Reorganization Act of 1986, PUBLIC LAW 99-433-
October 1, 1986, http://history.defense.gov/Portals/70/Documents/dod_reforms/Goldwater-NicholsDoDRecordAct1986.pdf.
[30] Hayden, "The State of the Craft," 23.
[31] Ibid.
[32] Ibid.
[33] Fishel, *American National Security Policy*, 23-25.
[34] Richelson, *The US Intelligence Community*, 523-526.
[35] Gutjhar, Melanie M.H., *The Intelligence Archipelago: The Community's Struggle to Reform in a*
Globalized Era (Washington, DC: Center for Strategic Intelligence Research, 2005).
[36] Morgenthau, Hans J., revised by Kenneth W. Thompson, *Politics Among Nations – The Struggle*
for Power and Peace, 6th ed. (New York: McGraw-Hill, 1985).
[37] Allison, Graham T., *Essence of Decision* (New York: Little Brown, 1971).
[38] Allison, Graham T., "Conceptual Models and the Cuban Missile Crisis," *The American Political Science Review* 63, no. 3 (1969): 689-718.
[39] Fishel, Kimbra, "Challenging the Hegemon: Al Qaeda's Elevation of Asymmetric Insurgent Warfare onto the Global Arena," *Networks, Terrorism and Global Insurgency*, Robert J. Bunker, ed., Taylor and Francis, 2005. Also published in *Low Intensity Conflict and Law Enforcement*, Special Edition, Robert J. Bunker, ed., 11, no. 2-3 (Winter 2004).
[40] Fishel, John, *American National Security Policy*, 25.
[41] Fernandez, Sergio, and Hal G. Rainey, "Managing Successful Organizational Change in the Public Sector," *Public Administration Review* 66, no. 2 (March 2006): 168-176.
[42] Ibid.

Kimbra L. Fishel is a political scientist specializing in U.S. national security, conflict, warfare, terrorism, and strategic intelligence. She has taught courses in International Politics, American Government, and the American Presidency at the University of Maryland at College Park, George Washington University, and the University of Oklahoma in Norman. She most recently developed an online course in Homeland Security for the University of Oklahoma that she will teach in the spring of 2021. She currently teaches for American Military University and is a doctoral candidate in AMU's new Doctor of Strategic Intelligence program. Kim has published numerous articles and book chapters.

[Editor's Note: In the interest of full disclosure, I presently serve on Ms. Fishel 's dissertation committee as an external reader and her late husband, LTC (USAR, Ret) John T. Fishel, who is cited in a couple of her footnotes, served on my master's thesis committee nearly four decades ago. Dr. Fishel and I also taught together at the William J. Perry Center for Hemispheric Defense Studies, National Defense University, over two decades ago.]

Operation MERKUR and the Battle for Maleme:
Allied Failures in Intelligence

by Daniel L. Harris

OVERVIEW

The Axis assault on the Allied-held island of Crete, Operation MERKUR ("Mercury"), occurred between May 20 and June 1, 1941. MERKUR was developed by Lieutenant General Kurt Student, Commander of the XI Air Corps, as the first, and thus essentially experimental, large-scale employment of airborne forces in the war effort. The Axis victory depended in large part on the prompt seizure of three critical airfields (and nearby ports)—Heraklion, Rethymno, and Maleme—located on the north of the island. The failure of British forces to repel the enemy at Maleme, and the subsequent retreat of defensive forces on the evening of May 20, allowed for the resupply and reinforcement of German paratroopers, creating an aerial beachhead from which Axis forces would capture Crete. An appropriate interpretation of Ultra intelligence prior to the battle, as well as effective communication of that information by the Commander of Allied forces on Crete, Lieutenant General Bernard Freyberg, to his subordinates, may have prevented the loss of Maleme airfield and, in turn, the battle.

DECISIVE BATTLE FOR MALEME

In the third volume of *Germany and the Second World War*, a seminal anthology of German military history, historian Detlef Vogel capstones his section on the battle for Crete with a curious aside: "The spectacular conquest of Crete. . .did not change the fact that this operation did not involve a decisive battle."[1] Vogel's assertion not only contradicts viewpoints expressed by officers and civilians present on Crete and academics years later, but ignores the restrictions imposed upon Lt Gen Student, all of which forced a decision at Maleme.

Crete, a mountainous island off the southern coast of Greece 160 miles long with a width between 8 and 35 miles, resembles, according to one British post-battle report, "a badly gnawed ham in which two great bites have produced two waists. . .[and invite] seizure by an invader."[2] Crete's "waists," however, were guarded by the Royal Navy, its rough terrain a natural barrier to air landings. The three aerodromes on Crete's northern coast, adjacent to the island's only deep water ports, constituted the sole "nodal points" available for enemy seizure.[3] Failure to secure an airfield would have crippled Student's invasion plans. Student's paratrooper forces would be isolated and vulnerable without resupply and heavy weaponry, which could arrive only over German-controlled airspace or through British-contested waters. Moreover, Student had employed nearly all of his paratrooper forces on the first day to disappointing effect: no objectives held, few reserves left to draw upon.[4] Preparations for the soon to be opened Eastern Front, combined with Hitler's diminishing peripheral interest in the Mediterranean theater, impressed upon Student the need to resolve the battle quickly and with limited resources. The setbacks of the first day made evident that this could not be accomplished through paratrooper deployments alone.

The tenuous German outpost was only fortified and expanded upon following the Allied retreat from Maleme, when artillery pieces, antitank guns, and troops were inserted "and the fate of Crete [sic] sealed."[5] Ignoring time and resource limitations, Maleme need not necessarily be considered a decisive engagement. Longer-term assault tactics, such as an island embargo enforced by German and Italian naval forces or repeated paratrooper deployments, would have represented alternatives to Student's vision for capturing Crete. A thorough campaign analysis, however, must avoid such temptations and rely upon those limitations in order to structure conclusions and counterfactuals feasible for the time. Such an approach will invariably treat Maleme as Crete's singular decisive engagement—its loss an unacceptable failure for both sides. "The enemy's stubborn defense [of Maleme] could have led to our defeat," observed General Julius Ringel, Commander of the 5th Mountain Division, "if he had grasped the situation from the very outset and had made use of all his available forces and resources."[6] Such observations serve as the basis for what follows: an analysis of the Allied defense of Maleme and the identification of how "available forces and resources" may have been reconfigured to victorious effect.

INTELLIGENCE ACCURACY

British signals intelligence—codenamed Ultra—identified the operational blueprint for MERKUR well in advance of the May 20 D-day. Early intercepts in mid-April offered the first image of German intentions—namely, the major parachute assault of a Mediterranean island.[7] By April 25, the same day Hitler issued Directive 28 ordering his air force to undergo preparations for the occupation of Crete,[8] the British had identified the island. Two subsequent Ultra reports—OL 2170 and OL 2/302—issued on May 7 and May 13, respectively, outlined in detail the German battle plans. The reports indicated that the attack would center around XI Air Corps' successful capture of the Heraklion, Rethymno, and Maleme airfields. This action would be accomplished through a preliminary attack on British anti-aircraft defenses by 150 long-range bombers and 100 heavy fighters, followed by a parachute landing of 12,000 men of the 7th Air Division. Once the fields were seized, approximately 600 Junker 52 transport aircraft would usher in reinforcements and supplies. Simultaneously, a seaborne contingent of 10,000 men guarded by Italian light naval forces would land on Crete. The later report stated that neither the airfields nor the island's largest port, Suda Bay, were to be mined.[9] With the exception of minor discrepancies in troop estimates, Ultra intelligence predicted German battle plans for MERKUR, affording British defensive forces an invaluable edge. Lt Gen Freyberg was first briefed on Ultra intelligence concerning MERKUR on April 30, days after his appointment as Commander of Allied forces on Crete.[10]

FAILURES IN INTELLIGENCE INTERPRETATION AND COMMUNICATION

Despite Ultra evidence indicating a primarily airborne assault on Crete, Freyberg lacked confidence in the Royal Navy's capacity to interdict a seaborne invasion and diverted significant resources to protecting coastal areas. Freyberg was, by his own admission, "mostly preoccupied by seaborne landings, not by the threat of air landings."[11] In the weeks following the Greek government's capitulation to Germany in April 1941, British forces evacuating the mainland for Crete and those stationed on the island were subjected to frequent daytime Luftwaffe raids. British troop movements were forced to occur on nights with little moonlight, when Luftwaffe visibility was lowest.[12] Unlike the evacuation of British Expeditionary Forces from Dunkirk, troops evacuating Greece could not rely on Royal Air Force (RAF) fighter support, whose nearest bases were located 400 hundred miles away in North Africa.[13] The island defenders fared little better, possessing at most 36 Hurricanes[14] (just six in the week prior to the assault and none during),[15] operating from within the "centre of a semi-circle of German airfields."[16] The largest ports on Crete were subjected to constant bombardment and the supply of resources to the island was unpredictable.[17] During one three-week period, just 11 percent of the goods shipped from Egypt arrived safely to port in Crete.[18] These demonstrations of Luftwaffe air superiority indicated to Freyberg that the Royal Navy would be operating without fighter protection and at high risk to its fleet, providing minimal support to his forces on Crete.

MERKUR would serve as the proving ground for the first major paratrooper assault in history and only the fourth employment in the war.

While Freyberg's risk assessment for the fleet was correct—the Royal Navy sustained heavy losses of one aircraft carrier, three cruisers, six destroyers (with 13 other vessels damaged), and over 1,800 men[19]—Freyberg undervalued the fleet's utility. General Student, biased by his branch, had appointed the seaborne contingent a supporting role for the prioritized aerial assault. The navy was charged with the resupply of the airborne troops, shipping heavy weaponry and men that could not be airlifted. The low emphasis placed on the seaborne leg of the operation was evidenced by the improvised nature of the fleet awarded to Naval Commander Southeast Admiral Schuster: 63 motor sailers and seven freighters, salvaged during the Greek invasion, under the protection of an Italian light naval escort.[20] On the night of May 21, the Royal Navy "wholly accomplished its task of preventing any invasion by sea" by interdicting the first of two planned German transports.[21] British and German casualty estimates vary, but the number of those drowned hovers between 500 and 2,500 troops, many recovered by the German Air Sea Rescue Service.[22] Despite the triumphs of German airpower over Crete, the Royal Navy proved adept at mitigating the threat of seaborne invasion while operating within heavily restricted waters.

Freyberg's focus on the coast was also biased by the novelty and mystery of airborne assaults. MERKUR would serve as the proving ground for the first major paratrooper assault in history and only the fourth employment in the war. Precedents had been set by the Germans on a lesser scale in the seizure of two lightly held airfields in Norway (April 1940) and the Belgian fortress of Eben Emael (May 1940).[23] Still, no island had ever before been captured by air. German paratrooper forces were also steeped in lore and elicited fear,[24] known to be elite-trained and among the youngest and most fervent

ideologues (many, indeed, were veterans of the Nazi Youth).[25] The British would not develop their own paratrooper forces, the 1st Parachute Battalion, until several months after MERKUR.[26] The dearth of historical comparisons likely weighed heavily on Freyberg's planning, restricting his reference points and incentivizing preparation for a conventional island siege.

Further complicating Freyberg's orientation of the island's defensive posture was his obligation to protect the sources of Ultra intelligence. On April 30, Freyberg was appointed as the island's seventh commander in seven months of British occupation and "read in" to the British government's "most secret sources," the foundation for his defensive preparations (codenamed SCORCHER).[27] The decision by Freyberg to withhold information from his subordinates concerning enemy objectives—namely the priority of the three aerodromes—and to fail to fortify these objectives more heavily have been explained, by some, as attempts by the island's commander to protect the source of the intelligence.[28] While withholding information from junior officers in order to prevent leaks would have been an understandable precaution, Freyberg's correspondence suggests fears of a seaborne invasion, rather than security concerns, were of greater personal distress.[29] It also seems implausible that Freyberg, a New Zealander and decorated soldier by background, would have withheld critical information—such as the postponement of the attack from May 17 to May 20[30]—from his men, many of them compatriots, in order to protect information which massive German force mobilizations in Greece had all but explicitly outed. Limiting the fortifications of the airfields would have also seemed appropriate had German reconnaissance been of concern. British officials were well aware, however, of German intelligence failures. Neither Cretan agents nor reconnaissance flights provided the German intelligence apparatus with a "clear picture of British defense preparations."[31] Such knowledge gaps ought to have appeared glaring when it was discovered that early German intelligence reports characterized the island as "lifeless,"[32] housing a British garrison of 5,000 men and no Greeks (in reality, the island housed around 27,000 British and imperial forces and 14,000 Greeks).[33] The digging of trenches around vulnerable sections of the airfields would have proved invaluable to the defenders, and their erection would have almost certainly gone unnoticed by the attackers.[34] The failure of the island's commander to transmit pertinent information to those with a need to know appears less the result of careful considerations over security and more likely the manifestations of a belief that a primarily airborne assault, as indicated by Ultra intelligence, was unlikely to occur.

HOW MALEME MIGHT HAVE HELD

Interpreting the significance of Maleme for a defensive posture based on Ultra intelligence, Freyberg and his subordinates may have made several critical battlefield alterations in the pursuit of holding the airfield. Awareness of the German plan to seize and utilize the aerodromes, combined with the effectively non-existent RAF presence on the island, Freyberg could have ordered the Heraklion, Rethymno, and Maleme airstrips mined, rendering them unusable for troop transport. Mined or intact, the airstrips would have represented an objective worth garrisoning with the island's reserves, whose distance from the battlefield, lack of communications, and poor transportation options crippled their reaction time. Troops stationed at these critical objectives ought to have been advised to counterattack landed enemy troops rapidly before they could regroup and hold positions. Moreover, given the enormous casualty rates inflicted on German paratroopers by small arms fire in their descent, Greek soldiers and Cretan civilians could have been better armed to maximize the defensively advantageous position. Assuming a revised defensive posture failed to repel the initial contingent of German paratroopers at Maleme on the afternoon of May 20, actions taken by Lieutenant Colonel Andrew and Brigadier Hargest to hold and reinforce the aerodrome position would have frustrated German resupply efforts.

Freyberg orders the Heraklion, Rethymno, and Maleme airstrips mined, prohibiting German transport aircraft from landing on the island.

In the weeks leading up to MERKUR, Freyberg had refused to mine Crete's airstrips, erroneously believing they were required to support RAF activities in defense of the island. Although the RAF had maintained a steady presence on the island since "fortress Crete"[35] was established in November 1940, it had always been negligible. Fighter losses in Greece, overstretched resources in foreign theaters, Luftwaffe air superiority, and the failure to conceive—as Hitler had—of Crete as a long-range bombing platform for strikes on the Romanian oil fields at Ploesti resulted in limited fighter and bomber deployments on the island.[36] Supporting the dwindling number of Hurricanes were, as Freyberg lamented, only 17 "obsolete aircraft."[37] While the prospects of RAF support from the far-flung British outpost in Alexandria were not to be entirely foregone, the flight time over the island, even with the aid of added fuel tanks, was limited to only minutes. Despite these handicaps, the RAF sent out several sorties on May 23; their effect, however, was minor.[38] Too few fighters were deployed too late in the battle to prove useful.

Freyberg also believed the enemy capable of circumventing the aerodromes altogether through dispersed crash landings of transport aircraft.[39] This is among the most curious, least defensible, and persistently held of Freyberg's beliefs in the planning for MERKUR. From a topographical vantage point, Crete presents a mountainous landscape hostile to air landings. Included in a report published by the British government on the Greek and Cretan campaigns, the island was deemed "most unsuited for landings," necessitating the maintenance of the aerodromes in "preventing an invasion by landings from the air."[40] Moreover, Ultra intelligence had been specific concerning the enemy's priority in capturing, securing, and employing the airstrips for transport aircraft.[41] The initial heavy bombardments by the Luftwaffe on the morning of the attack, concentrating around, but not atop, the runways, further evidenced the enemy's desire to maintain them.[42] While Freyberg may be credited for predicting the crash landing of the enemy's glider-borne "shock troops" in the preliminary hours of the battle, gliders carried just 2,000[43] of the 32,000 total airborne troops[44] in 72 aircraft (compared with the 500 transport aircraft which would later land at Maleme).[45] Glider-borne troops also suffered enormous casualties due to adverse terrain, incoming fire, and dust clouds which obscured their fields of view. It was clear to Student, as it ought to have been to Freyberg, that the brunt of the German invasion force would arrive on transport planes at secured airstrips.

Freyberg reduces or eliminates his reserves, bolstering troop numbers at the airfields and facilitating more advantageous force ratios for the Allies.

The decision by Freyberg to hold troops in reserve failed to account for Crete's exceedingly poor infrastructure. Freyberg's reserves would either serve as reinforcements for his forces holding the three airstrips or repulse a foreseen seaborne invasion. While troop numbers at the airfields varied, each defense sector maintained one third of its forces in and around the runway, with the rest holding the perimeter as reserves.[46] At the Maleme sector (which included Suda Port), this equated to a "force reserve" of two battalions[47]—the 21st and 23rd—drawn from the roughly 11,500 defending troops.[48] These troops would be ordered to move rapidly from their remotely located installations to the battlefield, when signaled. However, only one road ran along the northern coast of the island which connected the three sectors, and just three others traversed north to south (two of which had been cut by parachutists and one stopped seven miles short of the coast).[49] The concentration of all key island objectives along one coastal roadway, and the assumption that a force of mobile reserves could traverse it to come to the aid of a "hard-pressed sector,"[50] ignored the issues of roadway congestion and enemy route blockages. Moreover, the coastal roadway proved an easily identifiable target for Luftwaffe bombardments.

Such defensive challenges, according to British military historian Major General Ian Playfair, may have been at least partially offset by each sector's capacity to "transmit information and orders rapidly."[51] This too, however, would prove a challenge for Freyberg's forces. The field telephone networks on the island were known to be susceptible to Luftwaffe attacks, yet neither Freyberg nor his predecessors had made the acquisition of wireless communications tools a priority.[52] Consequently, the initial enemy bombardment of the island on May 20 immediately isolated the Maleme sector from command headquarters.[53] The effects of fractured communications on reserve forces were twofold. On a tactical level, the commanding officer at Maleme, Lieutenant Colonel Andrew, without direct line of sight on the battle, was forced to rely on alternative means of communication with his defensive and reserve forces, such as runners and flares. Andrew's runners "seldom got through the fire" and his flare signals were never received by the reserve battalions.[54] On an operational level, failures in communication caused Andrew's superiors both to undervalue the urgency of his situation and to labor under disprovable assumptions (such as the notion of widespread enemy crash landings).[55] It remains a great irony of the battle for Crete that its defenders were better informed of the battle plans and movements of the enemy when the latter was hundreds of miles offshore than when it was on their doorstep.

It remains a great irony of the battle for Crete that its defenders were better informed of the battle plans and movements of the enemy when the latter was hundreds of miles offshore than when it was on their doorstep.

Freyberg orders his troops to adopt rapid counteroffensive tactics in order to deny German paratroopers the opportunity to develop fortified lodgments.

Freyberg prepared his troops to adhere to a defensive force posture which failed to capitalize on key advantages presented by a paratrooper assault. In the days prior to the battle, Freyberg had ordered his troops to avoid the temptation of rushing out and engaging the enemy. Rather, they were encouraged to erect barbed-wire defenses and await enemy attacks. Freyberg's subordinates had voiced concerns over this approach, arguing swift counterattacks were the most effective means of preventing paratrooper lodgments.[56] Freyberg's approach, as it turned out, failed to make the most effective use of the disorganization and confusion of the paratrooper assault. German paratroopers landed over dispersed areas (often overshooting their

landing zones), amid enemy fire, without clear direction from their commanding officers.[57] Many of them were killed in the initial glider-borne assault (including the battalion commander of the Maleme group, Brigadier General Meindl, and both of his company commanders).[58] Many others lost or damaged their radios, the only means of communicating and regrouping. The chaos of the situation was characterized in a post-battle report published by the U.S. Army Air Force, which noted the parachutists' "[initial] inclination was to hide and take no active part in the proceedings for several hours" and remained their most vulnerable in the first 10-15 minutes after landing, before "they were given time to collect in organized bodies [and recover] their morale."[59] The Allied "barricading" posture was one of the factors which enabled parachutists to consolidate along the unfortified Tavronitis River bed to the west of the airfield. From their established position, the Germans would advance to take Hill 107 and subdue its two 4-inch guns, the airstrip's principal defensive outpost.[60] Barricading failed to disrupt and dislodge the enemy while it was at its weakest, giving it time to reorganize, regroup, and gain the battlefield initiative.

Freyberg arms Greek soldiers and Cretan civilians better in order to maximize German paratrooper losses during their most vulnerable moments.

Parachutists were most vulnerable in their descent and sustained their heaviest losses while in the air. Their limited mobility and control over direction within their harnesses made evasion from enemy fire difficult. Critically, parachutists had been armed only with knives, automatic pistols, and light machineguns, relying on separately dropped canisters for their heavier weaponry.[61] The limits imposed by firepower and directionality on the Germans translated advantageously for the defending forces, which were able to employ similar light weaponry from mobile and defensible positions to devastating effect. The battle had transformed, according to one intelligence officer who served on Freyberg's staff, from one "in which…the most up to date and deadly weaponry was being brought to bear" to one "being fought predominantly with small arms."[62] Bolstering the Allied advantage was the poor quality of German intelligence, which had misinformed the Luftwaffe of Allied positions and troop numbers. Many artillery installations remained intact following the initial Luftwaffe bombardment, and in several cases parachutists were dropped directly atop well-camouflaged defensive outposts.[63] The close proximity of parachute troops to the island's defenders also barred the Luftwaffe from providing close air support.[64] These factors combined to allow the Allies to inflict enormous casualties on the descending Germans. The lethality of the drop was most severe for those landing on defended positions, with an average of 4/5, or 80 percent, of those forces killed.[65] On the night of May 21 alone, of the 550 men dropped on the fortified vineyards surrounding Maleme, two companies were nearly entirely eliminated.[66] The German officer corps was equally afflicted, suffering the loss of "practically all the officers in one battalion" and "nearly all [the] company commanders" of the 3rd Parachute Rifle Regiment.[67]

Cretan underarming was a product of historical tensions between the island population and the Greek government.

Freyberg's forces failed to maximize their window of opportunity during the initial parachute drop by underarming Greek soldiers and Cretan civilians. In addition to the approximately 27,000 British forces garrisoned on the island, another 14,000 Greek troops organized into 11 battalions were on hand,[68] 3,500 of whom were stationed around Maleme.[69] Although many Cretan men of fighting age had been sent north and captured while fighting alongside Greek forces on the Albanian front, a native force remained on the island.[70] Each group suffered from severe arms shortages for different reasons. Greek soldiers, evacuated from the mainland alongside their fleeing British counterparts, were forced to compete for salvaged arms with Freyberg's forces, with the latter receiving priority. Moreover, poorly positioned weapons caches on Crete made attractive targets for Luftwaffe bombings in the weeks leading up to the invasion, depleting already limited stocks.[71] Cretan underarming was a product of historical tensions between the island population and the Greek government. Revolts against the repressive regime of Greek dictator Ioannis Metaxas, as well as the king, who they felt had betrayed them through granting the regime legitimacy,[72] had resulted in large-scale weapons confiscations by the government.[73] Between them, these forces were "half-trained, poorly armed, and older" than their British counterparts, yet "they possessed one salient virtue; the great majority had volunteered."[74] Cretan forces also had knowledge of the land and an ingrained culture of hunting, which made them adept marksmen.[75] Expecting limited resistance, if not a willing welcome, from these Greek and Cretan troops, German paratroopers were shocked by the ferocity of their competitors. Greek troops suffered heavy losses, and continued to fight for days after Maleme had been lost and the island's fate appeared certain. So frustrated was General Student by their efforts that, following his occupation of the island, he ordered extrajudicial retributions exacted upon the Cretan defenders.[76]

Lieutenant Colonel Andrew does not retreat from Maleme on May 20, averting German occupation of the airfield that night.

Regardless of the outcome of the actual, or revised, defensive fortifications, on the night of May 20 Lieutenant Colonel Andrew possessed the means to hold Maleme; he simply did not know it. Three factors contributed to Andrew pulling back his troops: his being underinformed of battlefield developments causing him to believe the situation was more dire than it was, the shortfall of his tactical "ace in the hole" tank deployment, and the failure of reinforcements to materialize come nightfall. Andrew's inability to visualize the field of battle or communicate with his two forward companies (C and D) throughout the day, as noted earlier, led him to fear the worst. Starting with the initial glider assault at 0800 and lasting for three hours, dust clouds left in the wake of aircraft crashes and the exhaust from Andrew's own anti-aircraft guns obscured his sightline.[77] Unable to visualize his men personally, or to communicate with them through radios or runners, Andrew was prevented from ordering artillery strikes. He instead resorted to ordering the two Matilda tanks at his disposal to assist his men.[78] Facing isolated German forces without the support of heavy armor, the tanks would prove a formidable weapon. Moreover, the gathering dust clouds and interspersed nature of the troops would prevent Luftwaffe intervention. Several hours after the dust clouds settled, it became evident to Andrew that the tank foray had failed; one had been equipped with the wrong ammunition and the other had become stuck on a boulder.[79] It was at this time, 1745 hours, that Andrew, believing his forces were at risk of being overrun, informed his commanding officer, Brigadier Hargest, of his need to exact a limited withdrawal.[80] Andrew was told to await reinforcement by two companies from the 23rd Reserve Battalion. When by 2200 hours the troops had not materialized, Andrew had his troops fall back from the airfield and abandon Hill 107.[81]

Despite Andrew's fears, based on ignorance of what was occurring around him, his forces had successfully held Maleme throughout the day of May 20. In addition to the heavy casualties and confusion which characterized the initial parachute assault, psychological factors played a prominent role in checking a German advance. Andrew's tank deployment, while ineffectual in many respects, sowed fear among German troops advancing on Hill 107, prompting their forces to scatter. Witnessing the movement of Allied armor and the prevention of two of their transport aircraft from landing through powerful bursts of machinegun and anti-aircraft fire, German troops felt underequipped and isolated.[82] Contributing to the feeling of abandonment were the visible naval explosions that night between the RAF and Schuster's vessels, which the Germans knew to be their last-resort lifeline. The paratroopers had been thrust into an "almost hopeless situation" where they found themselves "surrounded by greatly superior enemy forces, [struggling] for survival."[83] By the end of the first day, the 22nd Battalion was waging a fight with just half its original numbers; yet, it had allowed none of its defensive lines to be broken and had inflicted crippling real, and psychological, losses on its enemy.[84]

Brigadier Hargest sends reinforcements to Lieutenant Colonel Andrew on May 20 to bolster his forces and prevent his retreat and, the next day, launches an effective counterattack to deny German use of the airfield.

Hargest's unwillingness to furnish Andrew with reinforcements on the night of May 20 appears rooted in misunderstandings between the two officers. Beginning during the early afternoon of May 20 and continuing through mid-evening, Andrew made repeated requests to Hargest for reinforcements from the 21st and 23rd Reserve Battalions. Hargest refused early requests outright and acceded only when Andrew threatened a limited withdrawal. Even then, Hargest sent only a fraction of the forces requested, which arrived as Andrew was already consolidating his retreat.[85] Justifying his early refusal, Hargest had claimed the reserves were tied down attacking German paratroopers. Whether Hargest had been misinformed himself or was lying to Andrew has been a topic of debate, but it is undisputed that this was a falsehood.[86] The 850 men of the 21st and 23rd had seen only light combat in the morning, were rested and eager to fight, and when integrated into the weary ranks of the 22nd would have outnumbered the enemy four to three.[87] It appears likely that Hargest viewed the dire picture Andrew painted of his situation as an exaggeration. Hargest was aware that Maleme was the most strongly fortified sector on the island and that German paratroopers had been successfully repelled at each of the remaining aerodromes.[88] Hargest, like Freyberg, also continued to plan for a coastal assault, fearing any drawdown of the reserves would weaken his posture for such an invasion. It should not be dismissed that the clash of personalities between Hargest, a career politician in the New Zealand parliament with little military experience, and Andrew, a brave yet inarticulate lifelong soldier, likely led both to believe the other lacked the experience necessary to appreciate the situation.[89]

The counter-assault to retake Maleme was plagued by indecision and poor judgment regarding mission objectives. Hargest had been informed of the extent of Andrew's withdrawal at 0200 hours on the morning of May 21 and considered the merits of launching a counter-assault.[90] Hargest believed the threat of Luftwaffe raids to his reserves come daylight outweighed the setbacks of allowing Student a landing platform the next day. Hargest postponed the attack for the following night when his troops could deploy

earlier and maximize their fighting while under the cover of darkness.[91] Although Luftwaffe intervention, as discussed earlier, was a very formidable threat and principal concern for the defenders, the past day's events had demonstrated that the Luftwaffe would not attack defending forces when too closely interspersed with its own. Hargest's forces simply needed to reenter the battlefield, not retake it, where they could antagonize the enemy, continue to render the airstrip unusable, and buy time.[92] Ironically, the counterattack which Hargest ordered for May 22 commenced at 0330 hours, much too late in the morning to rely for long on the night cover Hargest so prioritized. The counterattack was "from the first doomed to failure."[93] Handicapped by its late start and the few forces committed to it, the Allied initiative not only failed in its primary objective to reestablish defensive positions around the airfield but also in its secondary role to place reserve troops within close enough proximity of enemy forces to guarantee success against air attacks. Student himself recognized the blessings of Hargest's indecision, writing after the fact, "In all probability my battalion, the IV Battalion of the Storm Regiment, would not have been able to withstand an energetic counter-attack in battalion strength."[94] Confident in his position on Maleme following two successful May 21 air landings, Student set in motion a transport convoy which would not again be interrupted by Allied resistance.[95]

CONSEQUENCES OF THE NEW APPROACH

A reorientation of Crete's defense posture around the airfields based on enhanced intelligence interpretation, as has been advocated in this article, necessarily invites a weakening of coastal armaments and a greater susceptibility to a seaborne invasion, Freyberg's initial fixation. It could be argued that Admiral Schuster, capitalizing on the exodus of Royal Navy forces from the Aegean on May 22 (resulting in German air and naval superiority), may have deployed the second of his two transport armadas to disembark on the now lightly defended coastline.

A second German naval thrust under these revised defensive conditions appears unlikely given the poor state of German intelligence, the continued reliance on the Italian Navy, and the service-level biases within the operational planning staff. The failure of German reconnaissance to identify, and the Luftwaffe to target, well-camouflaged defensive fortifications wrought unsustainable losses to Student's paratroopers on the first day of the fight.[96] Aware of the deficiencies in intelligence-gathering, and coming off the loss of half of his fleet the day prior, Schuster would likely have feared a naval repeat of Student's airborne losses. Considering a second deployment of his unarmed, vulnerable civilian fleet, Schuster not only required confidence in an uncontested voyage—unfurnished by the Italian navy—but of an uncontested landing, which German intelligence could not provide with confidence. Assuming Schuster possessed confidence in his capacity to launch a successful seaborne invasion, it is unlikely that those in the operational chain of command above Schuster would have approved of it. MERKUR was a remarkable testament to the cooperation of German military services—employing elements of the airborne, the Luftwaffe, and the navy—yet was clearly an air force-led operation, the first of its kind ever. Luftwaffe chief Goering delegated 4th Air Force commander General Loehr to head the unified command structure, which consisted of General Student (XI Air Corps), Admiral Schuster (Naval Forces), and General Richthofen (Luftwaffe VIII Air Corps).[97] Goering and Student possessed vested, institutional interests in proving to Hitler the efficacy of their revolutionary type of assault. German parachute regiments had been Student's brainchild, and he had advocated fiercely for them to form a new strategic arm within the German military.[98] The original planners of MERKUR debated the optimal methods for the capture of aerodromes (dispersed landings over large areas vs. concentrated landings) but never seriously questioned the premise of a paratrooper-based assault.[99] It was in large part Goering's and Student's confidence in this untested strategy which led Hitler to opt for an assault on Crete rather than one on Malta, which had been proposed by armed forces chief General Jodl on the same day.[100] Sending in Schuster's forces would have been a tacit admission by Goering and Student of their failure in judgment.

PROXIMITY TO REALITY

Despite a wealth of evidence to indicate measures Freyberg ought to have taken to fortify Maleme based on the Ultra intelligence he possessed at the time, the likelihood he would have seriously reoriented Crete's defensive posture remains low, the result of poor civilian guidance. The effective judgment of military commanders derives in part from the clarity of direction they received from their civilian superiors. Prime Minister Churchill vacillated over strategic objectives in regard to Crete, confusing the commander charged with achieving them. On the one hand, Churchill had vigorously championed arming the island from the outset of British occupation.[101] As the battle neared, Churchill urgently messaged Freyberg, conveying that the island must "be stubbornly defended,"[102] and provided British and Greek evacuees to assist in the defensive fortifications. Yet, in the seven months of British occupation, Crete had been poorly staffed and armed. Conflicting opinions over Crete's strategic significance by military leadership, including Field Marshal Wavell, had resulted in limited resources being diverted to the island.[103] Allied setbacks in Greece had also refocused Churchill's priorities. Crete, once considered a fortress, was to be transformed into a "receptacle of

refugees."[104] Churchill triaged his strategic priorities in an April 18 transmission to his chiefs of staff, asserting that "victory in Libya counts first; evacuation of troops from Greece second; Tobruk shipping, unless indispensable to victory, must be fitted in as convenient; Iraq can be ignored and Crete worked up later."[105] Within this confusing interplay between Churchill's rhetoric and actions was added Freyberg, who arrived on Crete to no established command headquarters, few personnel, and a "true state of disorganization."[106]

From Churchill's correspondence with Freyberg, it is evident that the former's strategic oscillations had a disorienting effect on the latter's defensive planning. Urgent telegrams to Churchill concerning Freyberg's fears of an airborne attack were contradicted later by responses to similar concerns held by others: "cannot understand nervousness; am not in the least anxious about airborne attack."[107] Such bipolar behavior may well be viewed as a manifestation of Freyberg's disorientation and uncertainty in the face of a looming, existential threat, exacerbated by a lack of civilian direction. Sound Ultra intelligence enhanced Freyberg's understanding of German intentions, but not of Allied priorities. Was Freyberg's objective to hold the island to the last man, deplete German paratrooper forces by a certain margin, or protect the island for as long as it took to evacuate its occupants safely? If the first, Freyberg's actions resulted in an unequivocal Allied "loss." Yet, viewed through the lens of German paratrooper casualties and troops evacuated, Crete presented at least a partial victory for the Allies, who inflicted a 2-1 casualty count on their enemy (excluding Royal Navy losses) and evacuated roughly 18,000 British troops.[108] The answers to these and many other unaddressed strategic questions would have better provided Freyberg with the "ends" necessary to best orient his "means" within the enemy battle parameters, as guided by Ultra.

CONTEXTUALIZING CRETE WITHIN THE WIDER WAR

The battle for Maleme, like any military operation, derives wartime significance insofar as it fits within the wider prosecution of the German war effort, both at the local level (the capture of Crete), the theater level (the Mediterranean air and naval campaign against Great Britain), and at a grand strategic level (global theaters generally, the opening of the Eastern Front specifically). Previous passages have discussed how the German capture of Maleme proved a decisive engagement within the context of securing Crete and explored counterfactuals which may have changed the course of the battle. The next section will examine the wide berth between the perceived and actual utility of Crete to the German war effort within the Mediterranean campaign, and will examine how its prosecution impacted Operation BARBAROSSA. Considering the hypothetical Allied retention of Maleme in the first few days of MERKUR from this multi-tiered vantage point, it seems highly probable that Hitler would have abandoned his siege of the island.

FAULTS IN GERMAN STRATEGIC REASONING

Following the German occupation of Greece and preceding the planning of MERKUR, Hitler developed perceptions concerning Crete's utility to the greater war effort which were either disprovable at the outset or would prove to be soon after the assault began. Firstly, a British-held Crete was perceived to pose a security risk to Axis sealanes across the Aegean, specifically threatening Italian oil routes from the Danube to the Dardanelles.[109] Surveillance of the island, however, had falsely revealed Crete as "lifeless" and would have identified Crete as a naval refueling platform rather than a base for interdiction operations.[110] Maritime transport lines would also invariably still pass by Malta, a British possession with the infrastructure to support commerce disruption.[111] Such pre-battle insights aside, by May 22 the Luftwaffe and the Italian Navy had forcefully repelled the last vestiges of Royal Navy presence from the Aegean, ameliorating the naval threat.[112] Secondly, Hitler enumerated in Directive 28 his desire for Crete to serve "as a base for air warfare against Great Britain in the eastern Mediterranean." Such goals were incompatible, however, with the resource needs of BARBAROSSA, for which he cautioned in the same directive against taking any action which might "entail any delay" in its undertaking.[113] Indeed, just 21 days after German forces captured Crete, the Eastern Front was opened, and Luftwaffe aircraft and paratroopers were transferred to the next theater, unable to capitalize on their victory.[114] Hitler also believed German paratrooper forces stationed on Crete could be deployed to the Middle East and North Africa to aid in Rommel's offensives.[115] The prohibitive losses to Student's XI Air Corps on the first day not only critically limited the number of troops which could be redeployed to another theater but also shook Hitler's confidence in the efficacy of major paratrooper assaults in general, evidenced by his later employment of Student's paratroopers in infantry roles along the Eastern Front.[116]

Hitler's greatest misperception in regard to Crete was the threat it posed, under Allied possession, to the Ploesti oil fields in Romania. Accounts of Hitler's thought processes during this period noted his fear over losing this vital strategic asset as a principal motive for launching MERKUR.[117] British airfields on Crete, however, were not built for aircraft capable of launching the long-range

attacks necessary to reach the 1,100-km distance to Romania. Although the British possessed the Wellington bomber, built to fly such distances, they could neither guarantee a safe flight path over Allied territory nor continuous fighter support, both critical to mission success. Questions of operational feasibility were subsumed by the simple lack of aircraft necessary to prosecute a campaign of this kind.[118] Waging a strategic bombing campaign on the continent and protecting against Luftwaffe raids at home, the RAF was too overstretched to provide Crete with the forces necessary to make a dent in German oil production. Assuming the worst-case scenario for the Germans—a refitting of Crete's infrastructure to support the Wellingtons, now garrisoned on Crete in great numbers and enjoying flight security—Hitler would still have been able to prohibit Allied bombings from the Italian-held Dodecanese Islands. Located just 215 km from Crete, the Dodecanese would prove an ideal platform from which to launch surveillance and bombing runs on the British outpost.[119]

CONCLUSION

Had Maleme held in those first few days of the fight, some or many of the above contradictions in reasoning may have impacted Hitler's resolve to capture Crete. For Hitler, Crete represented the capstone to a successful Balkans campaign, the death knell to an impotent power, Great Britain. Student, eager to prove the worth of the paratrooper assault, and Goering, embarrassed by the Luftwaffe's defeat in the Battle of Britain and eager to reestablish his service's prestige, had assured Hitler of a quick and easy victory.[120] Most importantly, the impending assault on the Soviet Union was Hitler's obsession. Capitalizing on a perceived "window of opportunity" of relative Soviet military weakness in order to exterminate the Bolsheviks and establish a German *Lebensraum*, or "living space," dwarfed considerations for other theaters. Where the prosecution of the latter seriously affected the planning for the former, namely the "very real danger that too high a percentage of first-class troops might be diverted to a secondary theater of war," Hitler's preference was clear.[121] The evolution in Hitler's strategic thinking between Directive 28 (April 25, 1941), in which he envisioned establishing Crete to prosecute an expanded Mediterranean campaign,[122] and Directive 31 (June 9, 1941), which tempered German goals to the "organisation and establishment of this base, its supply and protection," demonstrated that even the successful capture of Crete represented a pyrrhic victory in Hitler's eyes.[123] Considering MERKUR had been "sanctioned…on the understanding that the airborne troops would be relieved at once,"[124] a protracted fight at Maleme would have been, based on Hitler's strategic ambitions at the time, entirely unpalatable.

NOTES

[1] Gerhard Schreiber, Bernd Stegemann, and Detlef Vogel, *Germany and the Second World War, Volume III: The Mediterranean, South-east Europe, and North Africa (1939-1941),* trans. Dean S. McMurry, Ewald Osers, and Louise Willmot (Oxford, UK: Oxford University Press, 1995), 555.
[2] Britain Ministry of Information, *The Campaign in Greece and Crete* (London: Her Majesty's Stationery Office, 1942), 45.
[3] Ibid.
[4] Major General I.S.O. Playfair, Captain (Royal Navy) F.C. Flynn, Brigadier C.J.C. Molony, and Air Vice-Marshal S.E. Toomer, *The History of the Second World War: The Mediterranean and Middle East, Volume II: The Germans Come to the Help of Their Ally (1941)* (London: Her Majesty's Stationery Office, 1956), 134.
[5] George E. Blau, *Invasion Balkans! The German Campaign in the Balkans, Spring 1941* (Shippensburg, PA: Burd Street Press, 1997), 131.
[6] General Julius Ringel, as quoted in U.S. Department of the Army, *The German Campaigns in the Balkans (Spring 1941)* (Washington, DC: November 1953), 147.
[7] Antony Beevor, *Crete 1941: The Battle and the Resistance* (New York, Penguin Group, 1991), 90.
[8] Adolf Hitler, *Führer Directive 28* (April 25, 1941).
[9] OL 2170 and OL 2/302 in Beevor, *Crete 1941: The Battle and the Resistance* (New York: Penguin Group, 1991), 362-363.
[10] Beevor, *Crete 1941: The Battle and the Resistance* (New York: Penguin Group, 1991), "Most Secret Sources."
[11] Lt Gen Bernard Freyberg as quoted in Beevor, *Crete 1941: The Battle and the Resistance* (New York: Penguin Group, 1991), 93.
[12] Britain Ministry of Information, *The Campaign in Greece and Crete* (London: Her Majesty's Stationery Office, 1942), 38.
[13] Ibid., 39.
[14] Blau, *Invasion Balkans! The German Campaign in the Balkans, Spring 1941* (Shippensburg, PA: Burd Street Press, 1997), "Defense Forces."
[15] Ibid., 62.
[16] Playfair, Flynn, Molony, and Toomer, *The History of the Second World War*, 128.
[17] Britain Ministry of Information, *The Campaign in Greece and Crete* (London: Her Majesty's Stationery Office, 1942), 49.
[18] Blau, *Invasion Balkans! The German Campaign in the Balkans, Spring 1941* (Shippensburg, PA: Burd Street Press, 1997), 96.
[19] Playfair, Flynn, Molony, and Toomer, *The History of the Second World War*, 147.
[20] Blau, *Invasion Balkans! The German Campaign in the Balkans, Spring 1941* (Shippensburg, PA: Burd Street Press, 1997), "Attack Forces."
[21] Britain Ministry of Information, *The Campaign in Greece and Crete* (London: Her Majesty's Stationery Office, 1942), 55.
[22] Playfair, Flynn, Molony, and Toomer, *The History of the Second World War*, 137.
[23] Ralph Bennett, *Ultra and Mediterranean Strategy 1941-1945* (London: Hamish Hamilton, Ltd., 1989), 58.
[24] One belief, circulated among Allied troops, was of German paratroopers dressed as nuns, deployed behind enemy lines.

Such accounts were recorded from soldiers beyond Crete; yet, the widely held fear appears to have no basis in reality.
[25] Ian Stewart, *The Struggle for Crete: 20 May-1 June 1941, A Story of Lost Opportunity* (London: Oxford University Press, 1966), 83.
[26] "The Parachute Regiment," *United Kingdom National Army Museum*, December 2019.
[27] Schreiber, Stegemann, and Vogel, *Germany and the Second World War*, 540.
[28] At this time, Freyberg falsely believed Ultra to be the work of a well-placed human asset, rather than the accumulation of signals intercepts. Such a belief may explain Freyberg's secrecy as in the service of protecting the "informant." It would also explain why Freyberg might have distrusted the validity of the information.
[29] Beevor, *Crete 1941: The Battle and the Resistance* (New York: Penguin Group, 1991), 93.
[30] Ibid., 81.
[31] Schreiber, Stegemann, and Vogel, *Germany and the Second World War*, 539.
[32] Stewart, *The Struggle for Crete*, 89.
[33] U.S. Department of the Army, *The German Campaigns in the Balkans (Spring 1941)* (Washington, DC: November, 1953), 121.
[34] Geoffrey Cox, *A Tale of Two Battles: A Personal Memoir of Crete and the Western Desert 1941* (London: William Kimber & Co., Limited, 1987), 111.
[35] Adolf Hitler, *Führer Directive 31* (June 9, 1941).
[36] Beevor, *Crete 1941: The Battle and the Resistance* (New York: Penguin Group, 1991), 86.
[37] Lt Gen Freyberg as quoted in Stewart, *The Struggle for Crete*, 62.
[38] Playfair, Flynn, Molony, and Toomer, *The History of the Second World War*, 140.
[39] Beevor, *Crete 1941: The Battle and the Resistance* (New York: Penguin Group, 1991), "Most Secret Sources."
[40] Britain Ministry of Information, *The Campaign in Greece and Crete* (London: Her Majesty's Stationery Office, 1942), 45.
[41] Early Ultra reports did acknowledge, despite German intentions, that the landing of transport aircraft in open terrain was "possible."
[42] Beevor, *Crete 1941: The Battle and the Resistance* (New York: Penguin Group, 1991), 110.
[43] U.S. Department of the Army, *The German Campaigns in the Balkans (Spring 1941)* (Washington, DC: November 1953), 130.
[44] U.S. Army Air Forces, *The Attack on Crete and Notes on the German XI Air Corps* (September 1942), 3.
[45] Playfair, Flynn, Molony, and Toomer, *The History of the Second World War*, 129.
[46] Stewart, *The Struggle for Crete*, 109.
[47] Playfair, Flynn, Molony, and Toomer, *The History of the Second World War* 127.
[48] Schreiber, Stegemann, and Vogel, *Germany and the Second World War*, 541.
[49] Britain Ministry of Information, *The Campaign in Greece and Crete* (London: Her Majesty's Stationery Office, 1942), 49.
[50] Playfair, Flynn, Molony, and Toomer, *The History of the Second World War*, 123.
[51] Ibid.
[52] Beevor, *Crete 1941: The Battle and the Resistance* (New York: Penguin Group, 1991), "Most Secret Sources."
[53] Playfair, Flynn, Molony, and Toomer, *The History of the Second World War*, 132.
[54] Ibid.
[55] Stewart, *The Struggle for Crete*, 308.
[56] Beevor, *Crete 1941: The Battle and the Resistance*, (New York, Penguin Group, 1991), 'Most Secret Sources.'
[57] Britain Ministry of Information, *The Campaign in Greece and Crete* (London: Her Majesty's Stationary Office, 1942), 51.
[58] U.S. Department of the Army, *The German Campaigns in the Balkans (Spring 1941)* (Washington: November, 1953), 130.
[59] U.S. Army Air Forces, *The Attack on Crete and Notes on the German XI Air Corps* (September, 1942), 6-7.
[60] Beevor, *Crete 1941: The Battle and the Resistance*, (New York, Penguin Group, 1991), 113.
[61] U.S. Army Air Forces, *The Attack on Crete and Notes on the German XI Air Corps* (September 1942), 27.
[62] Cox, *A Tale of Two Battles*, 72.
[63] U.S. Department of the Army, *The German Campaigns in the Balkans (Spring 1941)* (Washington, DC: November, 1953), 145.
[64] Ibid.
[65] U.S. Army Air Forces, *The Attack on Crete and Notes on the German XI Air Corps* (September 1942), 43.
[66] U.S. Department of the Army, *The German Campaigns in the Balkans (Spring 1941)* (Washington, DC: November 1953), 135.
[67] Playfair, Flynn, Molony, and Toomer, *The History of the Second World War*, 148.
[68] Britain Ministry of Information, *The Campaign in Greece and Crete* (London: Her Majesty's Stationery Office, 1942), 45.
[69] Stewart, *The Struggle for Crete*, 112.
[70] U.S. Department of the Army, *The German Campaigns in the Balkans (Spring 1941)* (Washington, DC: November, 1953), 123.
[71] Stewart, *The Struggle for Crete*, 112.
[72] The king and his exiled government had themselves taken refuge on the island following the German occupation of Greece.
[73] Beevor, *Crete 1941: The Battle and the Resistance* (New York: Penguin Group, 1991), "The Battle of Crete."
[74] Stewart, *The Struggle for Crete*, 59.
[75] Cox, *A Tale of Two Battles*, 72.
[76] Schreiber, Stegemann, and Vogel, *Germany and the Second World War*, 552.
[77] Stewart, *The Struggle for Crete*, 167.
[78] Ibid., 172-173.
[79] Ibid.
[80] Ibid.
[81] Cox, *A Tale of Two Battles*, "Fateful Night at Maleme."
[82] U.S. Department of the Army, *The German Campaigns in the Balkans (Spring 1941)* (Washington, DC: November, 1953), 130.
[83] Ibid., 132.
[84] Playfair, Flynn, Molony, and Toomer, *The History of the Second World War*, 133.
[85] Ibid.

[86] Beevor, *Crete 1941: The Battle and the Resistance* (New York: Penguin Group, 1991), 125.
[87] Stewart, *The Struggle for Crete*, 258.
[88] Ibid., 178.
[89] Ibid., 180.
[90] Ibid., 257.
[91] Ibid.
[92] Ibid.
[93] Ibid., 308.
[94] General Student as quoted in Stewart, *The Struggle for Crete*, 259.
[95] Britain Ministry of Information, *The Campaign in Greece and Crete* (London: Her Majesty's Stationery Office, 1942), 53.
[96] U.S. Department of the Army, *The German Campaigns in the Balkans (Spring 1941)* (Washington, DC: November 1953), 135.
[97] Ibid., 145.
[98] Beevor, *Crete 1941: The Battle and the Resistance* (New York: Penguin Group, 1991), "The Spear Point of the German Lance."
[99] Playfair, Flynn, Molony, and Toomer, *The History of the Second World War*, 129.
[100] Blau, *Invasion Balkans! The German Campaign in the Balkans, Spring 1941* (Shippensburg, PA: Burd Street Press, 1997), "Strategic Factors and Planning."
[101] Schreiber, Stegemann, and Vogel, *Germany and the Second World War*, 532.
[102] Prime Minister Churchill, as quoted in Beevor, *Crete 1941: The Battle and the Resistance* (New York: Penguin Group, 1991), 86.
[103] Schreiber, Stegemann, and Vogel, *Germany and the Second World War*, 532.
[104] Ralph Bennett, *Ultra and Mediterranean Strategy 1941-1945* (London: Hamish Hamilton, Ltd., 1989), 62.
[105] Prime Minister Churchill as quoted in Playfair, Flynn, Molony, and Toomer, *The History of the Second World War*, 124.
[106] Lt Gen Freyberg as quoted in Stewart, *The Struggle for Crete*, 52.
[107] Ibid., 91.
[108] Playfair, Flynn, Molony, and Toomer, *The History of the Second World War*, 147.
[109] Playfair, Flynn, Molony, and Toomer, *The History of the Second World War*, 129.
[110] Blau, *Invasion Balkans! The German Campaign in the Balkans, Spring 1941* (Shippensburg, PA: Burd Street Press, 1997), "Strategic Factors and Planning."
[111] Colonel Kurt Helmut Schiebold, *Operation Merkur 1941 – A Failure in Strategic Leadership* (Carlisle, PA: U.S. Army War College, 2002), 11.
[112] U.S. Department of the Army, *The German Campaigns in the Balkans (Spring 1941)* (Washington, DC: November 1953), 133.
[113] Adolf Hitler, *Führer Directive 28* (April 25, 1941).
[114] U.S. Department of the Army, *The German Campaigns in the Balkans (Spring 1941)* (Washington, DC: November 1953), 147.
[115] Britain Ministry of Information, *The Campaign in Greece and Crete* (London: Her Majesty's Stationery Office, 1942), 62.
[116] U.S. Department of the Army, *The German Campaigns in the Balkans (Spring 1941)* (Washington, DC: November 1953), 147.
[117] Beevor, *Crete 1941: The Battle and the Resistance* (New York: Penguin Group, 1991), "Most Secret Sources."
[118] Schiebold, *Operation Merkur 1941*, 11.
[119] Schreiber, Stegemann, and Vogel, *Germany and the Second World War*, 553.
[120] Ibid., 530.
[121] U.S. Department of the Army, *The German Campaigns in the Balkans (Spring 1941)* (Washington, DC: November 1953), 121.
[122] Adolf Hitler, *Führer Directive 28* (April 25, 1941).
[123] Adolf Hitler, *Führer Directive 31* (June 9, 1941).
[124] Playfair, Flynn, Molony, and Toomer, *The History of the Second World War*, 149.

Daniel L. Harris is a master's degree candidate in Security Studies at the Georgetown University School of Foreign Service and a columnist for the Security Studies Review. *He is currently a research assistant at the National Defense University's William J. Perry Center for Hemispheric Defense Studies, where his work centers on Latin American security issues and their effect on U.S. interests in the region. He aims to continue his work in the region as a military analyst following graduation. Prior to Georgetown, he worked for a private firm investigating sanctioned actors involved in drug trafficking, money laundering, and offshore embezzlement networks throughout the Western Hemisphere. Through numerous published articles and white papers, and as a speaker at an industry conference, he has exposed the businesses, financial holdings, and support networks of illicit actors. Daniel received his undergraduate degree in Political Science from Occidental College.*

Venezuela: A Case Study of Iran's Grand Strategy to Penetrate Latin America and the U.S. Response

by Dr. Magdalena Defort

OVERVIEW

This article focuses on Iran's grand strategy to infiltrate the Bolivarian Republic of Venezuela during Hugo Chávez's and Nicolás Maduro's leadership. It includes the different phases of soft and hard power, as the foreign policy mechanisms, that the Islamic Republic of Iran has used in dealing with Venezuela. This study is pressing because of recent events including the assassination of Major General Qassem Soleimani, the head of the Islamic Revolutionary Guard Corps-Quds Force (IRGC-QF) by a U.S. drone in Baghdad, Iraq. At that time, Hezbollah announced it would pursue revenge for Soleimani's death. In addition to this event, another killing took place—the last bastion of Venezuela democracy, the National Assembly, was taken over by one of Maduro's supporters who was proclaimed as its head. The expansionist strategies used by foreign power Iran are analyzed in relation to U.S. policy response through an array of different legislative initiatives and economic sanctions applied on both regimes. Finally, this article will look at different recommendations to the U.S. and Latin American governments about how they should challenge the security threat in the region.

IRAN'S GRAND STRATEGY AS ITS FOREIGN POLICY MECHANISM

Iran's use of different tactics to penetrate Venezuela makes it difficult to define by a single term. A unique political science, military, or diplomatic definition does not exist because Iran uses an array of operations to achieve its goals; its infiltration is the epitome of all of these terms. Due to the difficulty in finding a more precise term to define its strategic presence in the region, a broad definition to describe the Iranian phenomenon of foreign policy toward Latin America is "Grand Strategy." This term is defined as the collection of plans and policies at the political, military, diplomatic, and economic levels, joined together by the state to advance its national interest. Grand Strategy is a more easily comprehended term that comprises all policies (means) to achieve its objective (ends).[1] Instruments or mechanisms (ways) would be applied to methods that Iran uses to craft its "Grand Strategy." According to a well-known construct developed by Colonel Arthur F. Lykke, Jr. (1989), strategy equals *ends* (objectives toward which one strives) plus *ways* (courses of action) plus *means* (instruments by which some end can be achieved).[2] Although this concept was formulated by an expert in military affairs, it would be applicable also to the non-military mechanisms that Iran employs in Venezuela.

> ***Nye divided "soft power" into three categories: cultural, ideological, and institutional, which correspond to Iran's infiltration of Venezuela.***

Katzman (2016) discusses Iran's foreign policy as a product of many factors and, at the same time, its use of a number of different tools in carrying out its foreign policy. Some tactics are conventional and others unconventional. Iran uses more traditional tools such as diplomacy or establishes economic or cultural agreements to stamp its footprint on the region. It maintains its embassies or other representation in all Latin American countries through its diplomatic relations.[3]

Soft power, one of the mechanisms of Grand Strategy used by the Islamic Republic of Iran, is defined by Nye (2011) as the ability to "get others to want the outcomes that you want," more particularly "the ability to achieve goals through attraction rather than coercion." This is the ability to coerce through threats and inducements ("sticks" and "carrots"). On the contrary, hard power, another component of Iran's Grand Strategy, is "the ability to get others to act in ways that are contrary to their initial preferences and strategies."[4] Nye divided "soft power" into three categories: cultural, ideological, and institutional, which correspond to Iran's infiltration of Venezuela.[5]

"Hard power" encompasses a wide range of coercive policies, such as coercive diplomacy, economic sanctions, military action, and military alliances for deterrence and mutual defense. Hard power can be used to

establish or change a state of political hegemony or balance of power. Some of the hard power components have been used by Iran in Venezuela. In addition, Nye introduces "smart power" as the "balance of hard and soft power."[6] For Nye, soft power is even more important than hard power in international politics because it enables a change of behavior in others, without competition or conflict, by using persuasion and attraction.

FOUR PHASES OF IRAN'S PENETRATION OF VENEZUELA

In 2000 Chávez traveled for the first time to the Middle East to meet the heads of state of the Organization of Petroleum Exporting Countries (OPEC) and invite them to Caracas to commemorate OPEC's 40th anniversary scheduled for September 2000. During that visit, Iranian President Muhammad Khatami met Chávez. This summit was of importance not only for Venezuela but also for the Arab states because it underscored that their revolutionary ideology joined both worlds against U.S. imperialism. A fascination for Colonel Gamal Abdel Nasser's Egyptian Revolution in 1952 against the British colony and the Suez Canal's nationalization in 1956 inspired the Bolivarian leader.

The revolutionary past of the Latin American and Arab worlds, particularly the Islamic Republic of Iran, became a driving force to cement relations between these different civilizations which portrayed themselves as the victims of imperialism and liberal democracy imposed by the United States. The anti-U.S. strategy of both worlds' revolutions began with the first step of strategic penetration. According to Joseph Humire, strategic penetration reflects different phases, from cultural to diplomatic to economic to military.[7] A penetration of Venezuela links to Iran's export of revolution. For the Iranian regime, the revolution was not only a historical event, but an array of concepts, values, and political and social meanings that created a new vision of the world.[8]

A. Soft Power Mechanism: Cultural and Religious Footprint

The cultural exchange between Iran and Latin America began in the 1980s with a wave of Lebanese immigration. According to the Argentinian prosecutor in the case of the bombing of the Argentine-Israeli Mutual Association (Associatión Mutual Israelita Argentina, or AMIA) in Buenos Aires, Argentina, Alberto Nisman, Sheik Mohsen Rabbani was an architect of Iran's foothold in Latin America. He was an intellectual author of the Hezbollah terrorist attack on the Jewish Cultural Center in Buenos Aires in 1994. Rabbani was a focus of connections between the two parties. In 1989 Iran began its first Islamic construction project in Caracas, Venezuela, known as the Ibrahim Ibin Abdul Aziz Al-Ibrahim Mosque, which concluded in 1993. In 2005 Tehran opened the Center for Iran-Latin America Cultural Exchange (Centro de Intercambio Cultural Iran Latino America, or CICIL) in Caracas. It is run by an Islamic foundation based in the Iranian religious center of Qom and headed by Mohsen Rabbani, an Iranian cleric.[9] It is only the second Islamic center in Latin America after the one in Buenos Aires.

The plethora of Islamic religious-cultural centers and educational institutions dispersed throughout Venezuela proves the foothold of Iran's first stage of expansion. The Margarita Island-Caribe Islamic Community Margarita (Isla Margarita-Caribe la Comunidad Islámica Venezolana), the Association of World League of Venezuela (Associación de la Liga Mundial de Venezuela), the Islamic-Venezuelan Center (Centro Islámico Venezolano), and the Islamic Center of Punto Fijo (Centro Islámico de Punto Fijo) are Islamic entities located in the Bolivarian country.[10] The cultural and religious centers serve to spread the revolutionary principles and to recruit the future warriors of revolutions.[11]

Although the educational institutions and media organs play their primary and innocent role of promoting Islam among Venezuelans, their covert function is Hezbollah recruitment, training, and operations for spies. Hezbollah "cultural" activities include infiltrating, proselyting, and radicalizing the Islamic community in Latin America according to Iranian revolutionary principles.[12]

Financial institutions and charitable organizations established in Venezuela served as a platform to fund Hezbollah. Ghazi Nasr al-Din is a Venezuela-based Hezbollah supporter who, as a Venezuelan diplomat and a president of Shia's Islamic Center in Caracas, provided funds to Hezbollah. He was a Charge d'Affaires at Venezuela's embassy in Damascus, Syria, and was subsequently appointed Director of Political Aspects at the Venezuelan Embassy in Lebanon. According to the U.S. Department of Treasury, he provided information on banks and accounts where the funds would be transferred to Hezbollah's cause.[13] According to Alberto Nisman, Sheik Mohsen Rabbani was an architect of Iran's foothold in Latin America. Rabbani not only laid the blueprint for how to carry out an Islamic terrorist attack in Latin America, but more importantly how to cover it up.

B. Soft Power Mechanism: Diplomacy

Islamic cultural and religious centers were a platform that allowed Iran to establish a more formal diplomatic footprint in Venezuela. Although officials traveled back

and forth and relations between the two nations had begun even before the Islamic Revolution in 1979, their diplomatic ties strengthened under the Bolivarian leader's mandate. In his original, 674-page report from 2006, Nisman described how Iran achieved its diplomatic footprint after moving forward from the cultural layer.

In 2000 Bolivarian leader Chavez visited several Arab countries and invited their heads of state to commemorate OPEC's anniversary scheduled for September of that year in Caracas, Venezuela. He warmly welcomed his "brothers" from the "powerful Arab, Islamic world."[14] The Iranian President, Muhammad Khatami, participated in OPEC's summit in Caracas. Despite the fact it was not the only official meeting between Venezuelan and Iranian heads of state, it can be classified as the beginning of closer relations between two anti-imperialist countries at the diplomatic level with economic objectives.

Diplomatic relations between the two countries, and their mutual support on the international scene, emerged in 2005 with the presidential election of Mahmoud Ahmadinejad in Iran and the earlier establishment of the Bolivarian Alliance in the Western Hemisphere in 2004. These two events were the most important engines of strengthening relations between the two civilizations. Chávez visited Iran 13 times, and his counterpart has made six trips to Venezuela since 2005.[15] During his visit to Caracas in 2007, the Iranian president received the Collar of the Order of Liberator, the highest honor for a dignitary, which proved the esteem in which Iran's president was held.[16] In turn, current President Nicolás Maduro has traveled to Tehran two times, and his Iranian counterpart, Hassan Rouhani, has visited Caracas once. This points to a measurable decrease in relations during Maduro's presidency, although in August 2019, Ambassador of the Islamic Republic of Iran Mostafá Alaeí traveled to Venezuela and received the highest award from President Maduro, the Francisco Miranda Order, for advocating on behalf of self-determination and sovereignty of the people.[17] This demonstrates the ideological and diplomatic affinities the anti-imperialist countries share. As diplomatic relations between the two presidents advanced, economic cooperation also intensified.

C. Soft Power Mechanism: Economy

Oil diplomacy, as a geopolitical strategy, was one of the most relevant economic tools between the two OPEC countries (Venezuela and Iran); in fact, it opened a door for the next joint venture between Venezuela's state defense contractor, CAVIM, and Iran's Parchin Chemical Industries to conduct the covert activities.[18] Chaìvez knew how to use oil wealth diplomacy to promote his country abroad in the Western Hemisphere and beyond. Both countries used petroleum power to push back against Washington's hegemony. Iran promoted its petro-alliances with its hemispheric neighbors to regain power in the Middle East. Furthermore, the oil agreement was a way for Iran to avoid the economic sanctions imposed by the United States in the wake of the hostage crisis of 1980. The economic agreements facilitated the use of the other mechanism of Iran's strategy toward Venezuela: military power.

D. Hard Power Mechanism: Military

Military agreements between Venezuela and Iran also reflected an economic backdrop. In case of a country with a lack of transparency and the necessity to take unlawful steps to achieve its objectives, the economic agreement was a perfect tool because it had a double purpose (i.e., a material used in manufacturing bicycles resembles that used to construct part of a missile).

Around 1982, the Iranian government held a seminar attended by almost 400 Islamic religious representatives to explain how Iran was going to export its revolution. Javad Mansouri, the first commander of the Iranian Revolutionary Guard, felt the revolution could be exported only with grenades and explosives, and he endorsed turning all Iranian embassies into intelligence centers to export Iranian interests.[19] For the Iranian ayatollahs, though, the military agreements would be important in advancing their strategic goals and gaining a new ground to conduct operations against the United States and Israel.

U.S. RESPONSE TO IRAN'S PRESENCE IN VENEZUELA

Despite the fact the Middle Eastern country has maintained diplomatic relations with Venezuela from the creation of OPEC in 1960, the first notification of Iranian presence in the Bolivarian Republic reached the U.S. when newly elected Iranian President Mahmoud Ahmadinejad came to Venezuela for a formal visit in 2006. This trip was alarming for the United States due to its purposes: economic collaboration, investment of Iranian Petrobras in Venezuela's oil refineries, and support of the Latin American country to keep Iran's oil price in euros, instead of dollars, to weaken U.S. influence over investment banks. Another claim was that a visit would lead to an exchange of uranium from the Amazonas for Iran's nuclear technology.[20]

In September 2006, before the UN General Assembly, Chávez called President Bush "the devil" who thinks, as he said, he is "the owner of the world."[21] These deeply

offensive words toward his U.S. counterpart escalated diplomatic tensions and heralded a new chapter of foreign relations with the United States that the Latin American populist president had crafted for his country and his allies. The division was so profound that the United States began to look even more closely at both countries. In a 2006 resolution, the International Atomic Energy Agency (IAEA) stated that Iran had failed in its obligations to comply with comprehensible safeguard agreements (CSA) and there were undeclared materials or activities inside the country.[22] All these events of 2006 paved way for a new security era designed by Venezuela's strategic allies to balance power with the United States.

In 2010 the U.S. Department of Defense delivered an unclassified report on Iran's military power about an increasing presence of IRGC-QF in Latin America, and particularly in Venezuela.

Since the Islamic Republic of Iran strengthened its relationships with Venezuela, the Latin American country began to fail in most of its agreements for cooperation with its hemispheric neighbor. First, it ceased to "fully cooperate with the United States anti-terrorist efforts" pursuant to Section 40 A of the Arms Exports Control Act (22 U.S.C. 2781). In 2009 the U.S. House of Representatives approved its version of the Foreign Relations Authorization Act for FY2010 and FY2011, H.R. 2410, that would have required a report within 90 days after enactment of sanctions against Iran's and Hezbollah's actions in the Western Hemisphere. As a result, the United States prohibited all arms sales to Venezuela starting in 2006. Second, Venezuela no longer collaborated in countering drug trafficking pursuant to provisions of the Foreign Relations Authorization Act, FY2003 (P.L. 107-228, §706; 22 U.S.C. 2291j).[23] A similar determination regarding its failure in the war on drugs was made in August 2019. Third, in 2008, for its alleged support to Iran and its proxy, Hezbollah, sanctions were imposed on CAVIN pursuant to the North Korea Nonproliferation Act of 2006 (Public Law 109-112).[24] This sanction was imposed by the 109th Congress.

In 2010 the U.S. Department of Defense delivered an unclassified report on Iran's military power about an increasing presence of IRGC-QF in Latin America, and particularly in Venezuela. It stated that "if U.S. involvement in conflict in these regions deepens, contact with IRGC-QF, directly or through the extremist groups it supports, will be more frequent and consequential."[25]

Most U.S. policies toward Venezuela's and Iran's actions were implemented separately until the legislative initiatives pursuant to the 111th and the 112th Congressional Assemblies. In 2012 the 112th Congress recognized a complexity of threats and the need to use a comprehensive strategy to counter Iran's growing hostile presence in the Western Hemisphere by working together with U.S. allies and partners in the region to deter threats to U.S. interests by Iran, the Iranian Islamic Revolutionary Guard Corps (IRGC), the IRGC Quds Force, and Hezbollah. It was to call for multiagency collaboration between Latin American and U.S. governments to counter the Iranian threat in the Western Hemisphere. The Act of 2012 (P.L. 112-220, H.R. 3783) sought "to provide for a comprehensive strategy to counter Iran's growing hostile presence and activity in the Western Hemisphere, and for other purposes." Its first paragraph defines Iran's objective in Latin America: establish economic and security agreements to create the network of economic and security relationship to end international sanctions and oppose the Western world to constrain its ambitions. The law required the Secretary of State to conduct an assessment within 180 days of the "threats posed to the United States by Iran's growing presence and activity in the Western Hemisphere" and offer a strategy to address those threats.[26]

Its footprint in Venezuela is underpinned by a complex web of praiseworthy interpersonal and inter-organizational links that infiltrate multiple religious and cultural networks, diplomatic institutions, companies, and financial entities that frequently serve as a cover for its illicit activities, e.g., money laundering, drug trafficking, and recruitment of new revolutionary fighters, among others.

In 2016 the 114th Congress determined that, after Chávez's death in 2013 and Ahmadinejad's departure from the presidency in the same year, new Iranian President Hassan Rouhani did not prioritize Latin America as Iran's top strategic region. The Obama administration softened its political tone and actions against Iran and instead focused more on Venezuela's political and economic crisis and human rights rather than any action against Iran's activity in the country. As Representative Duncan said, "There is a little bit of difference between administration's actions here."[27] The sanctioned Joint Iran-Venezuela Bank is the institution that can have access to U.S. financial markets via Venezuela.

In 2017 USSOUTHCOM commander Admiral Kurt Tidd stated that Iran, among the other external actors, e.g., Russia and China, views the Latin American economic, political, and security arena as an opportunity to achieve its respective long-term objectives and advance interests that may be incompatible with those of the United States. The vision of these countries on the international order strongly differs from that of the United States. Perhaps Iran does not pose a direct military threat, but it does warrant close scrutiny. Its activities in the region are malign.[28] Tidd's statement correlated with that of General John Kelly, former SOUTHCOM commander, in his posture statement from 2015 that, because Iran conducts its foreign policy in Latin America, the United States should be concerned.[29]

With the deepening crisis in Venezuela, street uprisings, and tense relations with Teheran regarding its involvement in the war in Syria, the Trump administration crafted a more radical policy toward both countries, known as "maximum pressure."[30] The core of Trump's foreign policy focused on using the rounds of sanctions on both countries to induce their repressive regimes to change. The policy addressed sanctions against Maduro, his government, and any national or foreign third party (secondary sanctions) that help Maduro stay in power.

With respect to Iran in 2019, the Trump administration took actions against the Central Bank of Iran (CBI) and the National Development Fund of Iran (NDFI) under its counterterrorism authority, E.O. 13224. Both institutions provided billions of dollars for the IRGC-QF and its proxy, Hezbollah, and the action was a part of a maximum-pressure policy on Tehran to counter attempts to achieve its revolutionary values through regional destabilization.[31] This economic and financial policy was to target Iran's proxy funding. Although the sanctions clearly defined Iran's activity in the Middle East region, they would have an even larger scope and include Iran's proxy activities in Latin America.

CONCLUSIONS AND RECOMMENDATIONS FOR ACTION

Iran has a strategic, long-term, consistent policy not only in a region of its traditional influence, but also in Latin America. Its footprint in Venezuela is underpinned by a complex web of praiseworthy interpersonal and inter-organizational links that infiltrate multiple religious and cultural networks, diplomatic institutions, companies, and financial entities that frequently serve as a cover for its illicit activities, e.g., money laundering, drug trafficking, and recruitment of new revolutionary fighters, among others. Iran benefited from new ground for its strategic operations, established a new friendship with populist leaders, freely explored the strategic minerals needed for its military and nuclear objectives, created Hezbollah's cells, and, partially, reduced its international isolation. Without a doubt, the soft and hard power resulted in perfect foreign policy mechanisms to penetrate the Bolivarian Republic of Venezuela and its allies. Despite the fact there are contradictory statements, reports, and hearings on the existence of an Iranian missile base in Venezuela, about which various scholars have speculated, this external actor has succeeded in its long-standing revolutionary expansionist strategy in the Bolivarian country.

Its footprint in Venezuela is underpinned by a complex web of praiseworthy interpersonal and inter-organizational links that infiltrate multiple religious and cultural networks, diplomatic institutions, companies, and financial entities that frequently serve as a cover for its illicit activities, e.g., money laundering, drug trafficking, and recruitment of new revolutionary fighters, among others.

Unfortunately, Venezuela has lost more than it has gained from the alliance with this Middle Eastern power. Chávez, a charismatic populist leader, attempted to bring to his people liberty and independence from the U.S. hegemonic position in the region. His Bolivarian Revolution was to be a sister of the Islamic Revolution; however, it was not to be. The respective religious and cultural backgrounds were different, and only the revolutionary ideology agenda was common. The Bolivarian Revolution was to spread the universal principles and values throughout the ALBA bloc. Because of huge petroleum resources and his petro-diplomacy, Chávez could afford to buy the new friends. He built up his *chavista* project through corruption, rigged elections, and friendship with other autocrats having similar ideological affinities and power aspirations. He needed Iran's help to build repressive security forces to tackle any opposition. His power was more concentrated inside his own country and within the Bolivarian bloc than it was outside Latin America.

Contrary to the Bolivarian movement, the Islamic Revolution was to spread, using soft and hard power to insinuate itself into Venezuela's corrupt government. Iran profoundly explored Venezuela's society and astutely inoculated it into a complex web of Bolivarian bloc criminal organizations. Even more, Iran created its own

networks to achieve its objectives, e.g., Venezuela's former Vice President Tereck el Aissami, who was branded a "Specially Designated Narcotics Trafficker" under the Kingpin Act in 2017.[32]

Venezuela's former Vice President Tereck el Aissami...was branded a "Specially Designated Narcotics Trafficker" under the Kingpin Act in 2017.

On January 5, 2020, Major General Qassem Soleimani, commander of the Elite Quds Force, was killed by a U.S. drone strike in Baghdad, Iraq. In response, Iran announced a vindication for Soleimani's death and suspension of Iran's commitments to a nuclear deal established with the world powers in 2015. This radical decision will enable the regime to activate centrifuges in its stockpile of nuclear fuel.[33] In the aftermath of the assassination, Hezbollah leader Hassan Nasrallah announced that his militants will seek revenge for killing the most important figure in the Middle East.[34] The next event to occur, dissolution of the National Assembly in Venezuela, cemented Maduro's absolute power.[35]

Iran and the United States at times have been on the verge of war, and Venezuela can become a center of gravity where the powers clash to protect their national interests and influence in the region. For Soleimani, the geostrategy would have been achieved only through indirect defensive attacks using a plethora of Shia proxy forces. Now it is likely that a large portion of the Shia community and Hezbollah's "sleeper cells" in Venezuela will be called to join and orchestrate terrorist attacks in different spots against U.S. and Israeli residents in the Americas. Venezuela's Iran-backed militia will protect Maduro even more because of U.S. policy attempting to oust him from power.

The current volatile security scenario in the Bolivarian country and the Middle East is even more unpredictable and dangerous now because of recent events that have fueled violence, anger, and calls for retribution. Soleimani's "axis of resistance" could start its revenge by targeting foes in the Middle East and exploring all asymmetric options.[36] It demonstrates how dangerous Huntington's clash of civilizations could be in the post-9/11 world if the 1979 Islamic Revolution explodes again and Bolivarian Venezuela retains its revolutionary *chavista* regime. This is why the United States should look for leverage in collaboration with and support of Latin American countries through diplomacy. It should soften its foreign policy toward the Middle East and negotiate the presence of its troops on foreign soil. Otherwise, asymmetric warfare may end with WMD deterrence.

NOTES

[1] Peter Feaver, "What is grand strategy and why do we need it?" *Foreign Policy,* April 8, 2009, https://foreignpolicy.com/2009/04/08/what-is-grand-strategy-and-why-do-we-need-it/

[2] Arthur F. Lykke, Jr., "Defining Military Strategy," *Military Review* 69*,* no 5 (May 1989), 3.

[3] Kenneth Katzman, "Current Politics and Economics of the Middle East," *Hauppauge,* Vol. 7, Iss. 1 (2016), 25-75.

[4] Joseph Nye, *The Future of Power* (New York: Public Affairs, 2011), 11.

[5] Eric X. Li, "The Rise and Fall of Soft Power: Joseph Nye's concept lost relevance, but China could bring it back," *Foreign Policy,* August 20, 2018, https://foreignpolicy.com/2018/08/20/the-rise-and-fall-of-soft-power/.

[6] Joseph Nye, "On the Rise and Fall of American Soft Power," *New Perspectives Quarterly* 22(3), 2005, 75-77.

[7] "Joseph M. Humire, co–author of *Iran's Strategic Penetration of Latin America*, before the U.S. House of Representatives, Committee on Foreign Affairs, Subcommittee on the Western Hemisphere (WHEM) and Subcommittee on the Middle East and North Africa (MENA)," House Office, March 18, 2015, 4, https://docs.house.gov/meetings/FA/FA07/20150318/103177/HHRG-114-FA07-Wstate-HumireJ-20150318.pdf.

[8] Ahmad Mousa, "Recruitment of Persian Language: The Role in Exporting Iranian Culture and Revolution," *Journal for Iranian Studies*, Year 2, Issue 5, December 2017, 28, https://rasanah-iiis.org/english/wp-content/uploads/sites/2/2018/03/Recruitment-of-Persian-Language.pdf.

[9] Rabbani was implicated in the 1994 bombing of the Jewish cultural center in Buenos Aires that killed 85 people.

[10] Al'takwa, Association Civil, http://www.altakwa.com.ve/centros-islamicos.

[11] Ilan Berman and Joseph M. Humire, *Iran's Penetration of Latin America* (Lanham: MD, Lexington Books, 2012), 5.

[12] Joseph Humire, 4.

[13] "Treasury Targets Hezbollah in Venezuela," U.S. Department of the Treasury, June 18, 2008, https://www.treasury.gov/press-center/press-releases/pages/hp1036.aspx.

[14] Vélez, 142.

[15] Marc Daou, "Chavez leaves behind mixed legacy in Arab world," *France 24,* July 3, 2013, https://www.france24.com/en/20130307-chavez-leaves-behind-mixed-legacy-arab-world.

[16] Michael Dodson and Manochehr Dorraj, "Populism and Foreign Policy in Venezuela and Iran," *Journal of Democracy* Winter/Spring 2008, 81, http://blogs.shu.edu/diplomacy/files/archives/08%20Dodson.pdf.

[17] Simón García, "Iran's Ambassador to Venezuela receives the Francisco Miranda Order in Its First Class," *Gobierno Bolivariano de Venezuela: Ministerio del Poder Popular para Relaciones Exteriores*, August 8, 2019, http://mppre.gob.ve/en/2019/08/08/iran-ambassador-venezuela-receives-francisco-miranda-order-first-class/.

[18] Emanuele Otthonghi, "Iran looks to Latin America to revive missile infrastructure", *The Hill,* August 29, 2016, https://thehill.com/blogs/pundits-blog/international/293632-iran-looks-to-latin-america-to-revive-missile-infrastructure.

[19] David Barnett, "Argentine prosecutor accuses Iran of establishing terror network in Latin America," *FDD's Long War Journal*, May 30, 2013.

[20] Simón Romero, "Venezuela Strengthens Its Relationships in the Middle East," *The New York Times,* August 21, 2006, https://www.nytimes.com/2006/08/21/world/americas/21venez.html.
[21] 2006: Chávez calls Bush "the devil," *YouTube,* September 20, 2006, https://www.youtube.com/watch?v=lOsABwCrn3E.
[22] "Annual Report 2005," *International Atomic Energy Agency*, 67, https://www.iaea.org/sites/default/files/anrep2005_full.pdf.
[23] "Venezuela: Overview of U.S. Sanctions", *Congressional Research Service: Informing Legislative Debate since 1914*, updated February 21, 2020, https://fas.org/sgp/crs/row/IF10715.pdf.
[24] U.S. Department of State, Diplomacy in Action, "Iran, North Korea, and Syria Nonproliferation Act: Imposed Sanctions," updated May 29, 2013, https://2009-2017.state.gov/t/isn/inksna/c28836.htm.
[25] "Unclassified Report on Iran's Military Power of Iran, April 2010," https://fas.org/man/eprint/dod_iran_2010.pdf.
[26] "To provide for a comprehensive strategy to counter Iran's growing hostile presence and activity in the Western Hemisphere, and for other purposes," 112th Congress of the United States of America, H.R.3783, House Office, March 1, 2012, https://www.govinfo.gov/content/pkg/BILLS-112hr3783enr/html/BILLS-112hr3783enr.htm.
[27] "Venezuela's Crisis: Implications for the Region," Hearing before the Subcommittee of the Western Hemisphere of the Committee on Foreign Affairs House of Representatives, 114th Congress, *Government Publishing,* June 2016, https://www.govinfo.gov/content/pkg/CHRG-114hhrg20529/html/CHRG-114hhrg20529.htm.
[28] Posture statement of Admiral Kurt W. Tidd, Commander, United States Southern Command, before the 115th Congress, Senate Armed Services Committee, April 6, 2017, https://www.southcom.mil/Portals/7/Documents/Posture%20Statements/SOUTHCOM_2017_posture_statement_FINAL.pdf?ver=2017-04-06-105819-923.
[29] Posture statement of General John F. Kelly, United States Marine Corps, Commander, United States Southern Command, before the 114th Congress, Senate Armed Services Committee, March 2015, https://www.armed-services.senate.gov/imo/media/doc/Kelly_03-12-15.pdf.
[30] "Iran Sanctions," CRS, November 2019, https://fas.org/sgp/crs/mideast/RS20871.pdf.
[31] "Treasury Sanctions Iran's Central Bank and National Development Fund," U.S. Department of the Treasury, September 2019, https://home.treasury.gov/news/press-releases/sm780.
[32] "Kingpin Act Designations; Publication of Counter Narcotics Sanctions," U.S. Department of the Treasury, December 19, 2019, https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20191219_33.aspx.
[33] Erin Cunningham, "Iran announces it is suspending all commitments to the 2015 nuclear deal", *The Washington Post,* January 5, 2020, https://www.washingtonpost.com/world/body-of-commander-slain-by-us-strike-arrives-in-iran-to-crowds-of-mourners/2020/01/05/4ca3281a-2f17-11ea-bffe-020c88b3f120_story.html.
[34] Liz Sly and Sarah Dadouch, "Hezbollah says retribution for Soleimani's death must target U.S. military, not civilians", *The Washington Post,* January 5, 2020, https://www.washingtonpost.com/world/middle_east/hezbollah-says-retribution-for-soleimanis-death-must-target-us-military-not-civilians/2020/01/05/50869828-2e62-11ea-bffe-020c88b3f120_story.html.
[35] Rachelle Krygier and Anthony Faiola, "Venezuela's last democratic institution falls as Maduro stages de facto takeover of National Assembly, *The Washington Post,* January 5, 2020, https://www.washingtonpost.com/world/the_americas/venezuelas-last-democratic-institution-falls-as-maduro-stages-de-facto-takeover-of-national-assembly/2020/01/05/8ba496fe-2d8f-11ea-bffe-020c88b3f120_story.html.
[36] A plethora of Iran's proxy forces from the Middle East (Lebanon, Syria, Iraq, Iran, and Yemen) fight to recover the Levant.

Dr. Magdalena Defort is originally from Poland and holds a PhD degree from the Universidad Nacional Autónoma de México (UNAM). She is certified in postdoctoral studies from the Instituto de Ciencias Sociales of the same university. Magdalena recently graduated from the master's degree program in National Security at the Daniel Morgan Graduate School of National Security. She also held a research fellowship in the Center for a Free and Secure Society. Prior to coming to Washington, she was a Visiting Scholar at the University of Miami in Coral Gables, Florida. She was co-chair of an interdisciplinary research group exploring "Ill-Liberal Latin American Democracies." Furthermore, she was a co-author and co-editor of a research project/book titled The Decline of US Hegemony and Latin America Integration in the 21st Century: New Patterns of Regional Cooperation and Conflict? (ALBA and UNASUR). *Her interests include terrorism, drug trafficking, insurgency, and civil-military relations in Latin America. She focuses her research studies on Iran's strategic penetration of that region. Furthermore, she studies the nexus between insurgency and organized crime. In 2011 she participated in a course on "Terrorism and Inter-Agency Coordination" at the William J. Perry Center for Hemispheric Defense Studies, National Defense University, in Washington. She earned a fellowship from the Secretary of International Relations of Mexico, which enabled her to complete her project. Magdalena is an author of three books and various articles.*

[Editor's Note: I too was at the Perry Center (then called CHDS) teaching intelligence and civil-military relations to civilian and military officials from Latin America and the Caribbean, but over a decade prior to Dr. Defort's time there. She co-authored a previous article in *AIJ* with then-DMGS adjunct professor Col (USMC, Ret) W. Preston McLaughlin, who will have a solo article in the next issue.]

Homeland Security:
Advancing Intelligence-Led Policing in Confronting Jihadi-Salafism

by Bruno Brkic

SUMMARY

Jihadi-Salafism is one of many threats to homeland security. As Jihadi-Salafists might misuse the current Syrian refugee crisis to inspire terrorist attacks in U.S. urban areas, the Intelligence Community (IC) should introduce a new method for preventing Jihadi-Salafist attacks. Therefore, this article argues that:

(1) The U.S. government should continue offering hospitality and protection to Syrian refugees amid their arrival from previously Jihadi-Salafi-controlled territory in the Levant.

(2) The IC should enhance its present counterterrorism efforts in confronting terrorist attacks domestically by introducing a new model of counterinsurgency.

(3) Local, regional, and federal U.S. law enforcement agencies would be the best choice to implement the new counterinsurgency model in practice.

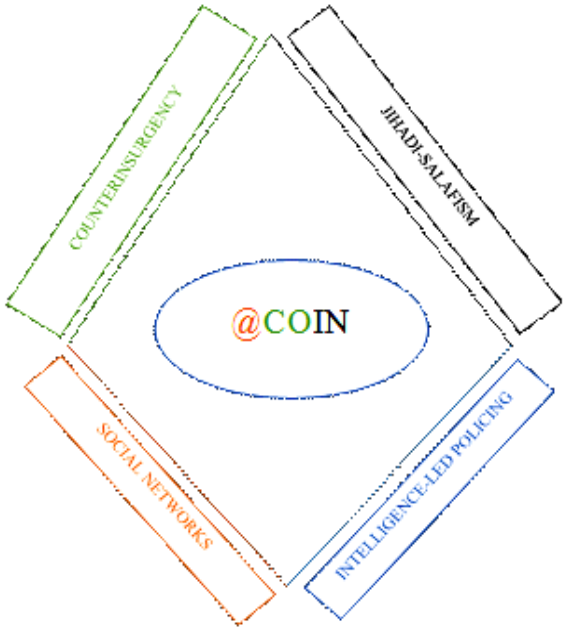


Figure 1: Graphic preview of the @COIN logic in Intelligence-Led Policing.

INTRODUCTION

Since 2011, the Syrian religious civil war has impacted the lives of millions living within that devastated country. What began as unrest against Bashar Al-Assad's authoritarian rule escalated into a rebellion of different military groups in various cities throughout Syria. The uprising saw the rise of the Islamic State of Iraq and al-Sham (ISIS), a new terrorist organization breaking off from al-Qaeda. As a result, many Syrians became refugees trying to resettle in neighboring countries, Europe, or even the United States. Those wishing to resettle in the U.S. found themselves facing both the U.S. Refugee Policies and Homeland Security Acts before crossing the Atlantic Ocean. While refugees to the U.S. from all around the world tend to integrate, fully lured by the ideas of life, liberty, and pursuit of happiness, this time their integration might be jeopardized by Jihadi-Salafist-inspired radicalization leading to urban insurgency. To prevent this from happening, the U.S. law enforcement community should introduce an online counterinsurgency model (@COIN) restricting Jihadi-Salafists' remote access to future Syrian-Americans. Consequently, @COIN would enhance the existing U.S. counterterrorism approach in protecting the homeland.

AL-ASSAD'S SYRIA AND THE RISE OF JIHADI-SALAFISM

Ten years after Bashar al-Assad took power in 2000, social and economic life changed considerably for average Syrians as societal values, expectations, and capacities were transformed. While the social market economy strategy aimed at improving the living standard and maintaining a high level of social protection, much of the evidence in the last decade suggests that market policies exacerbated social problems. With an average rate of 9.90 percent between 2000 and 2011, unemployment remained extremely high as wages remained well below the rising cost of living, and price volatility created economic uncertainty for hundreds of thousands, if not millions, of average Syrians.[1] Social market policies proved to be unsuccessful because the

structural shifts that were engendered by an economic system did not sufficiently direct resources toward the achievement of social ends.[2]

With the Arab Spring approaching in the Middle East, and the youth bulge creating a gap between mobilization and assimilation of the masses, Bashar al-Assad found himself under pressure to resign from office. On March 6, 2011, al-Assad's security forces arrested some fifteen children in the city of Dara'a, in southern Syria, for writing slogans against the regime. The crony socio-economic reform, continual freedom of speech suppression, and the incident in the city of Dara'a led to a series of anti-regime protests. By April 2011, youth activists had set up Local Coordination Committees across the country, which organized nationwide peaceful demonstrations every Friday and ensured that slogans were consistent and forward-looking. As the movement grew, similar grassroots groups emerged, including the Syrian Revolution General Commission and the Higher Council of the Syrian Revolution.[3]

However, the regime response came by force. Some 1,000 people died in the first three months of the uprising and 3,000 were detained. The corpses of activists and protesters were returned to their families bearing the marks of horrific torture, and even children were not spared.[4] This led to civil war, and in the early months of the conflict the "Free Syrian Army" (FSA) became a byword for any armed rebel militia. It called on soldiers to stand on the side of the people and their revolution and abandon their military units. Soon after, various militias declared themselves part of the FSA. Defections that followed were frequently advertised via YouTube with soldiers and officers in their Syrian army uniforms, holding their ID cards as verification, declaring their allegiance to the FSA.[5]

In January 2012, following FSA's appearance, al-Qaeda elements within the county established *Jabhat al-Nusra* (the Support Front), which was formed by *mujahedeen* (holy warriors) from the various fronts around the world. *Jabhat al-Nusra* saw itself principally as an Islamic movement extolling the virtues of "real" Islam and the necessity of jihad. *Al-Nusra* sought to present itself as a hyper-localized jihadist organization that would implement a patient and long-term strategy focused on integrating into local dynamics and shaping alliances.[6] Concurrently, many other Salafist and jihadist factions which appeared in Syria gave the conflict a religious character as they became a part of the emerging ISIS. As a result, this group's appearance led to international intervention in Syria as the U.S. government supported the FSA and fought directly against ISIS. At the same time, Iran and Russia came to al-Assad's rescue.

The religious civil war of Syria turned many people into refugees, attempting to leave the country and resettle somewhere else. Some hoped to start a new life in the U.S. but, because Syrian refugees came from a theater of war involving an array of Islamic political ideologies, they were subject to advanced security vetting procedures. Many Syrian-Americans seemed ready to accept U.S. founding principles, but some were feared to harbor Syrian and/or religious grievances. In any case, the U.S. Refugee Policies and Homeland Security Acts set the legal framework by granting refugees admission to the U.S. and restricting Jihadi-Salafists from reaching those who might struggle to embrace their new U.S. identities.

THE U.S. REFUGEE ADMISSION POLICIES

Refugees to the United States are allowed to resettle under the Immigration and Nationality Act (INA). The INA provides a uniform procedure for refugee admissions, authorizes federal assistance to resettle refugees and promote their self-sufficiency, and abolishes an *ad hoc* approach that had characterized U.S. refugee policy since World War II.[7] INA recognizes a refugee as "a person who is outside his or her country and who is unable or unwilling to return because of persecution or a well-founded fear of persecution on account of race, religion, nationality, membership in a particular social group, or political opinion." Usually, refugees are processed and admitted to the U.S. from abroad but, sometimes, INA grants asylum on a case-by-case basis to aliens who are physically present in the country. Regardless of these situations, refugees' admission depends on a joint decision by the President and Congress. The consultation results in a specific policy on refugee entrants, and the President sets the annual number of refugee admissions and the allocation of these numbers by region of the world.[8]

The total number of refugees coming to the U.S. has fluctuated in response to global events and national priorities. About three million refugees have resettled in the U.S. since Congress passed the Refugee Act of 1980.[9] The Act created the Federal Refugee Resettlement Program, which is the current national standard for screening and entrance of refugees into the country. From 1990 to 1995, an average of about 112,000 refugees arrived in the U.S. each year, many coming from the former Soviet Union. However, refugee entrants dropped off to fewer than 27,000 in 2002 following the 9/11 terrorist attacks by al-Qaeda a year earlier.[10] Of the 3,252,493 refugees admitted from 1975 to the end of 2015, twenty were confirmed terrorists.[11] Of those twenty, only three were successful in their attacks, killing a total of three people and imposing a total property damage cost of $45 million.[12] The three refugee terrorists were Cubans who

committed their attacks in the 1970s, before the passage of the Refugee Act of 1980. In comparison, the 9/11 attack resulted in 2,977 lost lives and over $100 billion in property damage.[13]

No refugees were involved in the 9/11 attacks.[14] However, that might change with the Syrian refugees coming from ISIS's controlled territory. While most terrorist groups have not used the refugee or asylum system to go to the U.S. and plot attacks, risks associated with Syrian refugees may be higher today. ISIS has been active in some Syrian refugee camps in the Middle East where the U.S. Intelligence Community's understanding of extremists in Syria was not as solid as in many other jihadist battlefields.[15] ISIS lost its physical caliphate, but it tries to regroup and refocus, looking for new paths to insurgency. Besides al-Qaeda, ISIS remains the most pressing radical Islamist terrorist threat to the U.S. homeland.[16] Given its losses in Iraq and Syria, the Jihadi-Salafist priority is building up affiliates elsewhere in the world. Therefore, the U.S. IC will have to work toward restricting their physical and ideological presence on U.S. soil.

THE IC AND VETTING PROCEDURES FOR REFUGEES

Besides the resettlement legal framework for refugees, the Departments of State (DOS) and Homeland Security (DHS) facilitate the procedural work by investigating refugees' credentials. DOS's Bureau of Population, Refugees, and Migration (PRM) coordinates and manages the U.S. refugee program to identify and admit qualified refugees for resettlement into the country. PRM holds responsibility for processing refugee cases, arranging for non-governmental organizations (NGOs), international organizations, or U.S. embassy contractors to manage Resettlement Support Centers (RSC) that assist in refugee processing.[17] RSCs conduct prescreening interviews of prospective refugees and prepare cases for submission to U.S. Citizenship and Immigration Services (USCIS), which handles refugee adjudications. There are three crucial areas for refugees: (1) groups which may be in danger of attack or of being returned to the country they fled; (2) groups of particular humanitarian concern to the United States based on their nationalities, clans, ethnicities, or other characteristics; and (3) groups which are seeking family reunification. These priorities provide access to U.S. resettlement consideration and are distinct from whether people qualify for refugee status.

The qualifications for refugee status are evaluated by the Secretary of DHS, who has discretionary authority to admit refugees to the United States. DHS's USCIS makes final determination about eligibility for admission. The USCIS Refugee, Asylum, and International Operations Directorate (RAIO), Refugee Affairs Division (RAD), and in some cases along with the International Operations (IO) Division, is responsible for interviewing refugee applicants, receiving and reviewing results of all background checks, and adjudicating applications for refugee status.[18] To be admitted to the U.S., a prospective refugee must be permissible under immigration law. INA sets health-related grounds, security-related grounds, public charges (i.e., poverty), and lack of proper documentation for inadmissibility.

Terrorism-related bases for rejection did not exist until the Immigration and Nationality Act of 1990 had them included. As part of a broader effort to streamline and modernize the security and foreign policy grounds for inadmissibility and removal, Congress added the terrorism consideration in the 1990 Act. Following the 9/11 terrorist attacks, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 amended the INA guideline to add "terrorism" for inadmissibility and to expand the definitional scope of terms used to describe terrorism-related activities and organizations. Consequently, an alien is generally inadmissible for engaging in terrorist activity if he or she gives any "material support," such as a safe house, transportation, communications, or funds, to a terrorist organization, any of its members, or an individual person engaged in terrorist activity. At the same time, terrorist organizations represent foreign entities involved in terrorist activities and threaten the security of U.S. nationals and/or their homeland.[19]

DHS's Homeland Security Investigations (HSI) entity is the most significant and longest-standing federal contributor to Joint Terrorism Task Forces (JTTFs) nationwide.[20] HSI's partnership with JTTFs ensures that the Department's legal, strategic, and tactical capabilities are fully utilized in furtherance of the counterterrorism mission. Every year, DHS prevents several thousand terrorist watch-listed individuals from traveling to or entering the United States. The Department employs a range of tools, including numerous vetting programs and capabilities, to detect such actors and ensure they cannot come through designated ports of entry or exploit the immigration system. DHS components patrol and rigorously enforce land, air, and sea borders. The Department is expanding cooperation with foreign governments to confirm individuals' identities better and detect threats before they can cause harm inside the United States. Most importantly, in addressing the danger coming from post-war Syria, DHS via USCIS engages in the comprehensive vetting of refugees and asylum seekers.

Between 2015 and 2017, some 20,826 Syrian refugees were admitted to the U.S. with 12,587 arriving in 2016 alone.[21] The decision to take in this number of refugees in a single year introduced pressure on the federal government to move more quickly in processing applications.[22] Nevertheless, all applicants went through the procedures for obtaining refugee status, and the USCIS instituted additional layers of review for Syrian refugee applications. Before being scheduled for an interview with a USCIS officer, Syrian cases are reviewed at USCIS offices abroad. Once they meet the criteria, cases are referred to the USCIS Fraud Detection and National Security Directorate (FDNS) for additional review and research.[23] FDNS conducts open-source and classified research on referred cases and synthesizes an assessment for use by the interviewing officer to inform lines of inquiry. FDNS's approach explains the context for the country conditions and how the regional activity impacts the overall qualifications for candidacy as a refugee. FDNS engages with law enforcement and IC members for assistance with identity verification and acquisition of additional information, if needed. Finally, a refugee is admitted to the United States if he or she is deemed not to pose a security threat.

...there is room for improvement in restricting Jihadi-Salafists who try to convert the refugee population into violent homeland extremists (VHEs) to commit attacks in their name.

The U.S. continues to be one of the leading countries in refugee resettlement as its entire IC makes refugees' entrance possible by distinguishing them from those willing to attack the homeland. While the U.S. legal framework for refugee admission is up to date and able to restrict terrorists from reaching this goal, there is room for improvement in restricting Jihadi-Salafists who try to convert the refugee population into violent homeland extremists (VHEs) to commit attacks in their name. Since 2014, there have been eight lethal terrorist attacks in the U.S., claiming 83 lives.[24] Seven of the eight attacks were Jihadi-Salafist-inspired. As more Syrian refugees from the previously Jihadi-Salafi-controlled territories enter the country, the chance of more frequent attacks could increase. Therefore, it is essential to upgrade the terrorist-centric, counterterrorism approach with the population-centric, counterinsurgency approach when dealing with future Jihadi-Salafi-inspired terrorist attacks in the U.S.

JIHADI-SALAFISM, INTELLIGENCE-LED POLICING, AND COUNTERINSURGENCY

Salafism, as a modern phenomenon, appears as the result of religion-based and consciousness-driven questions on the purpose of life.[25] While Salafists internally divide into purists, politicos, and jihadists, they split on which strategy best serves their goals. The purists focus on nonviolent methods of propagation, purification, and education; the politicos advance Salafi creed into the political arena to impact social justice and the right of God alone to legislate; and the jihadists call for a militant position leading to violence and revolution.[26] Jihadi-Salafism as "a religious-political ideology based on a fundamentalist conceptualization of Islam that informs the actions of contemporary terrorist organizations"[27] turns Salafi creed into jihad.[28] Jihadists such as Abu Mus'ab al-Suri understood the importance of Salafi ideology's contribution to politically motivated jihad.[29] Currently, because of its widely available propaganda in sound bites, video clips, and translated text on the Internet, the Jihadi-Salafists can feed the frustrations of youth in both the West and the East, allowing them to gain meaning for their existence by becoming mujahedeen and martyrs.[30]

The appearance of the Internet brought together Jihadi-Salafists all around the world, making the "online jihad" a legitimate form of their ideological struggle. The global computer network allows Islamic scholars—with or without formal Islamic education—to propagate the life of the Prophet and his companions (*al-salaf asl-salih*) as the correct model for the contemporary world and to reach a broad audience with limited religious knowledge.[31] Similarly to the Jihadi-Salafi scholar Lewis Atiyat Allah—known as the "desktop Jihadi"—who called for violence and terrorism in the post-9/11 world,[32] these "jihadi scholars" share their worldview online which might attract sympathizers wishing to create a global Muslim community (*Ummah*) by force.[33]

U.S. local, regional, and federal law enforcement agencies (LEAs) represent the best tool in preventing terrorism in general[34] and Jihadi-Salafism in particular[35] by utilizing intelligence-led policing (ILP). ILP is a business and managerial philosophy in which data analysis and crime intelligence are pivotal to an objective, decision-making framework. This framework facilitates crime and problem reduction, disruption, and prevention through both strategic management and effective enforcement strategies that target prolific and serious offenders.[36]

ILP is supporting a broader policing paradigm than does community-oriented policing (COP).[37] The COP has developed pro-ILP skills in many law enforcement

officers. These skills include the scientific approach to problem solving, environmental scanning, effective communications with the public, fear reduction, and community mobilization.[38] In early 1990, the New York Police Department (NYPD) developed a cutting-edge ILP model to deal with crimes. CompStat, a process for collecting, computing, mapping, and disseminating crime statistics, served as an analysis and managerial accountability crime prevention program, drastically reducing the offense rate in the city.[39] This approach also proved to be crucial in reducing crime in New York City.

The NYPD is well aware of the threat coming from al-Qaeda, ISIS, and other jihadi movements. Therefore, the Department has adopted a Jihadi-Salafi radicalization model acknowledging different stages of an individual's radicalization process leading to terrorism.[40] Consequently, NYPD's approach in dealing with future terrorist attacks offers a theoretical new approach for confronting Jihadi-Salafi-inspired urban insurgency. The approach might upgrade the countrywide terrorist-centric (counterterrorism) approach with the population-centric (counterinsurgency) approach when dealing with future Jihadi-Salafi-inspired terrorist attacks in U.S. urban areas. In particular, this approach might be crucial for homeland security in dealing with the four main reasons for future urban insurgencies: world population growth, urbanization, littoralization (the tendency for urban areas/cities to cluster on coastlines), and connectedness (the increasing connectivity among people wherever they live).[41]

Predictive policing uses available data to forecast crime hot spots as a basis for scientifically-based police decisions crucial in allocating police resources while conducting investigations online.

Insurgency may be defined as "an organized movement aimed at the overthrow of a constituted government through the use of subversion and armed conflict… Stated another way, an insurgency is an organized, protracted politico-military struggle designed to weaken the control and legitimacy of an established government, occupying power, or other political authority while increasing insurgent control."[42] Dealing with 21st century remotely-inspired insurgency in urban areas demands an advanced ILP involving Online Counterinsurgency (@COIN).

@COIN

Informational technology (IT) is useful in ILP to help in understanding online social network interaction. Modern software, such as a geographical informational system (GIS), can map crime hot spots, which allows predictive policing. Predictive policing uses available data to forecast crime hot spots as a basis for scientifically-based police decisions crucial in allocating police resources while conducting investigations online.[43] Artificial intelligence (AI) also might advance these investigations by introducing a new method of ILP involving @COIN. AI is the science of making machines do things that would require a lot of time if done by people,[44] and may be seen as the automation of activities such as decision-making, problem-solving, and learning associated with human thinking.[45] Also, AI is "the exciting new effort to make computers think…[and create] machines with minds, in the full and literal sense."[46] As a result, @COIN might become a state-of-the-art innovation in the post-9/11 environment,[47] and restrict Jihadi-Salafists' remote access to future Syrian-Americans.

To introduce an efficient @COIN, LEAs first have to understand the Jihadi-Salafist insurgency online since news distribution is not what it was fifty years ago.[48] It is not distributed merely by countries' press services or private broadcast operators. Information on different social events became easily and instantly available.[49] Consequently, the Internet allows Jihadi-Salafi-inspired terrorist attacks remotely as a low-cost, real-time text, voice, and video communication, enhancing social ties all around the world.

Social ties can be defined as an association of webs or actor-networks of diverse components.[50] As a source of actor-networks, social ties can explain how people create bonds among each other. However, "there is nothing more difficult to grasp than social ties."[51] To identify new forms of social ties that advance radicalization leading to terrorism, one should think "out of the box." These new forms of "democratic" communications, in which information and communication technologies erode cultural forms and roles, allow every digital being to connect by broadcasting messages independently.[52] Digital transformation offers both new opportunities and challenges for democracy. As the Internet became an essential part of our everyday routine, digital transformation impacted civic rights and engagement in the public sphere of every country.[53] Radical social movement leaders are well aware of this opportunity and use it to advance their agenda, which makes them susceptible to tracking online.

Syrian refugees use social platforms to collect and share information and develop patterns of their behavior online. In case their online activity includes Jihadi-Salafism-related content, @COIN might help in restricting Jihadi-Salafists' remote access to future Syrian-Americans by introducing a relevant counter-narrative that would oppose Jihadi-Salafism among Syrian refugees. It would also help the latter get over prior nationalistic and religious grievances while accepting a new identity as Syrian-Americans. Consequently, @COIN might enhance the existing counterterrorism approach by mapping out those Salafists spreading jihadi ideology.

The key to @COIN's success is to prevent Jihadi-Salafists from recruiting Syrian refugees willing to fight Americans domestically—in other words, to avoid fighting "accidental guerrillas."[54] However, this would not be an easy task. It will involve mutual trust between the U.S. IC members and large technical companies shaken by previous cases of personal data mismanagement and misuse. If adopted by the local, regional, and federal LEAs, @COIN would have to comply with the U.S. Constitution, big-tech data-privacy policies, and other relevant regulations advancing online investigations while respecting human rights.

CONCLUSION

Intelligence-led policing presents the best approach to confront Jihadi-Salafist-inspired radicalization leading to urban insurgency in the U.S. Local, regional, and federal LEAs arguably are the best suited to face this threat because they possess the legal framework, experience, and knowledge to deal with domestic Jihadi-Salafism. However, to succeed, LEAs will need help from the other members of the IC under the Director of National Intelligence. With collaboration among representatives of the IC, big technology, and civil society, @COIN has an unprecedented opportunity to help protect Americans and their property while respecting constitutionally-guaranteed rights to life, liberty, and the pursuit of happiness.

NOTES

[1] CEIC Data, *Syria Unemployment Rate*: 2000-2011, accessed on May 4, 2020, https://www.ceicdata.com/en/indicator/syria/unemployment-rate.
[2] Samer N. Abboud, *Locating the "Social" in the Social Market Economy* (Syracuse, NY: Syracuse University Press, 2014).
[3] Emile Hokayem, *Syria's Uprising and the Fracturing of the Levant* (London: Routledge, 2013), 69.
[4] Robin Yassin-Kassab and Leila Al-Shami, *Burning Country: Syrians in Revolution and War* (London: Pluto Press, 2018), 49.
[5] Christopher Phillips, *The Battle for Syria: International Rivalry in the New Middle East* (New Haven, CT: Yale University Press, 2016), 126.
[6] Charles R. Lister, *The Syrian Jihad: Al-Qaeda, the Islamic State and the Evolution of an Insurgency* (Oxford, UK: Oxford University Press, 2016), 67.
[7] U.S. Citizenship and Immigration Services, *Immigration and Nationality Act*, accessed on May 5, 2020, https://www.uscis.gov/legal-resources/immigration-and-nationality-act.
[8] U.S. Department of State, *Proposed Refugee Admissions for Fiscal Year 2019*, accessed on May 5, 2020, https://www.state.gov/wp-content/uploads/2018/12/Proposed-Refugee-Admissions-for-Fiscal-Year-2019.pdf.
[9] U.S. Department of State, *Refugee Admission*, accessed on May 6, 2020, https://www.state.gov/refugee-admissions/.
[10] Jens Manuel Krogstad, *Key facts about refugees to the U.S.*, Pew Research Center, accessed on May 6, 2020, https://www.pewresearch.org/fact-tank/2019/10/07/key-facts-about-refugees-to-the-u-s/.
[11] Alex Nowrasteh, *Terrorism and Immigration: A Risk Analysis*, Cato Institute, accessed on May 6, 2020, https://www.cato.org/publications/policy-analysis/terrorism-immigration-risk-analysis.
[12] Charlotte J. Moore, *Review of U.S. Refugee Resettlement Programs and Policies* (Washington, DC: Congressional Research Service, 1981), 3-16.
[13] Institute of the Analysis of Global Security, *How much did the September 11 terrorist attack cost America?* accessed on May 6, 2020, http://www.iags.org/costof911.html.
[14] Alex Nowrasteh, *Terrorists by Immigration Status and Nationality: A Risk Analysis, 1975-2017*, Cato Institute, accessed on May 7, 2020, https://www.cato.org/publications/policy-analysis/terrorists-immigration-status-nationality-risk-analysis-1975-2017.
[15] Seth G. Jones, *The Terrorism Threat to the United States and Implications for Refugees*, RAND Corporation, accessed on May 7, 2020, https://www.rand.org/pubs/testimonies/CT433.html.
[16] U.S. Department of Homeland Security, *Strategic Framework for Countering Terrorism and Targeted Violence*, accessed on May 7, 2020, https://www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-countering-terrorism-targeted-violence.pdf.
[17] U.S. Department of State, *U.S. Refugee Admissions Program*, accessed on May 7, 2020, https://2009-2017.state.gov/j/prm/ra/admissions/index.htm.
[18] U.S. Department of Homeland Security, *Privacy Impact Assessment for the Refugee Case Processing and Security Vetting*, accessed on May 8, 2020, https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis-refugee-july2017.pdf.
[19] U.S. Department of Homeland Security, *Strategic Framework for Countering Terrorism and Targeted Violence*, accessed on May 8, 2020, https://www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-countering-terrorism-targeted-violence.pdf.
[20] Ibid.
[21] U.S. Department of Homeland Security, *Annual Flow Report: Refugees and Asylees, 2017*, accessed on May 8, 2020, https://www.dhs.gov/sites/default/files/publications/Refugees_Asylees_2017.pdf.
[22] Teresa Welsh, "Why the U.S. Can't Immediately Resettle Syrian Refugees," *U.S. News & World Report*, September 15, 2015, accessed on May 8, 2020, https://www.usnews.com/

news/articles/2015/09/15/why-the-us-cant-immediately-resettle-syrian-refugees.
[23] U.S. Citizenship and Immigration Services, *Refugee Processing-Reynolds*, accessed on May 8, 2020, https://www.uscis.gov/sites/default/files/files/nativedocuments/Refugee_Processing_-_Reynolds.pdf.
[24] Peter Bergen and David Sterman, *Jihadist Terrorism 17 Years After 9/11: A Threat Assessment*, New America, accessed on May 8, 2020, https://www.newamerica.org/international-security/reports/jihadist-terrorism-17-years-after-911/.
[25] Oliver Roy, *The Failure of Political Islam* (Cambridge, MA: Harvard University Press, 1998), x.
[26] Quintan Wictorowicz, "Anatomy of the Salafi Movement," *Studies in Conflict and Terrorism*, vol. 29, no. 3 (April-May 2016), 208.
[27] John A. Turner, *Religious Ideology and the Roots of the Global Jihad: Salafi Jihadism and International Order* (New York: Palgrave Macmillan, 2014), 11.
[28] Roel Meijer, *Global Salafism: Islam's New Religious Movement* (New York: Oxford University Press, 2013), 24.
[29] Ibid.
[30] Samir Amghar, *Salafism and Radicalization of Young European Muslims* (Brussels, Belgium: Centre for European Policy Studies, 2007), 38-51.
[31] Meijer, 270-272.
[32] Madawi Al-Rasheed, *Contesting the Saudi State: Islamic Voices from a New Generation* (Cambridge, UK: Cambridge University Press, 2007), 201.
[33] Gary R. Bunt, *iMuslims: Rewiring the House of Islam* (Chapel Hill: The University of North Carolina Press, 2009), 35.
[34] Major Cities Chiefs' Association (2008), *Twelve Tenets to Prevent Crime and Terrorism*, accessed on May 9, 2020, https://www.majorcitieschiefs.com/pdf/news/MCC_12TenetFinal52108.pdf.
[35] Mitchell D. Silber and Arvin Bhatt, "Radicalization in the West: The Homegrown Threat," accessed on May 9, 2020, https://seths.blog/wp-content/uploads/2007/09/NYPD_Report-Radicalization_in_the_West.pdf.
[36] Jerry H. Ratcliffe, *Intelligence-Led Policing* (Portland, OR: Willan Publishing, 2008), 6.
[37] Jerry H. Ratcliffe, *Intelligence-led policing: Trends & issues in crime and criminal justice,* Rand 248, 2003.
[38] David L. Carter, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, 2nd ed. (Washington, DC: U.S. Department of Justice, Office of Community Oriented Policing Services, 2009), 86.
[39] David Weisburd, Stephen D. Mastrofski, Ann Marie McNally, Rosann Greenspan, and James J. Willis, "Reforming to preserve: COMPSTAT and strategic problem solving in American policing," *Criminology and Public Policy* 2(3), 2003, 421-456.
[40] Mitchell D. Silber and Arvin Bhatt, "Radicalization in the West: The Homegrown Threat,".accessed on May 9 2020, https://seths.blog/wp-content/uploads/2007/09/NYPD_Report-Radicalization_in_the_West.pdf.
[41] David J. Kilcullen, *Out of the Mountains: The Coming Age of the Urban Guerrilla* (New York: Oxford University Press, 2013), 28.
[42] U.S. Army and U.S. Marine Corps, *Counterinsurgency*, FM 3-24/MCWP 3-33.5 (December 2006), 1-2.
[43] Jerry H. Ratcliffe, *Intelligence-Led Policing* (New York: Routledge, 2016), 150-153.
[44] Raphael Bertram, *The Thinking Computer: Mind Inside Matter* (San Francisco, CA: W.H. Freeman, 1976).
[45] Richard Bellman, *An Introduction to Artificial Intelligence: Can Computers Think?* (San Francisco, CA: Boyd & Fraser Pub. Co., 1978).
[46] John Haugeland, *Artificial Intelligence: The Very Idea* (London: MIT Press, 1989), 2.
[47] Jeremy G. Carter, *Intelligence-Led Policing: A Policing Innovation* (El Paso, TX: LFB Scholarly Publishing LLC, 2013), 52-53.
[48] Fred S. Siebert, Theodore Peterson, and Wilbur Schramm, *Four Theories of the Press: The Authoritarian, Libertarian, Social Responsibility, and Soviet Communist Concepts of What the Press Should Be and Do* (Urbana-Champaign: University of Illinois Press, 1984), 1.
[49] Bill Kovarik, *Revolutions in Communication: Media History from Gutenberg to the Digital Age* (New York: Bloomsbury Publishing, Inc., 2016), 571.
[50] Jim S. Dolwick. "The Social and Beyond: Introducing Actor-Network Theory," *Journal of Maritime Archaeology*, Vol. 4, No. 1 (June 2009), 36.
[51] Bruno Latour, *Reassembling the Social: An Introduction to Actor-Network Theory* (Oxford, UK: Oxford University Press, 2005).
[52] Paschal Preston, *Reshaping Communications: Technology, Information and Social Change* (New York: Sage Publishing, 2001), 216.
[53] Julia Schwanholz, Todd Graham, and Stoll Peter-Tobias, *Managing Democracy in the Digital Age: Internet Regulation, Social Media Use, and Online Civic Engagement* (New York: Springer International Publishing, 2017).
[54] David J. Kilcullen, *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One* (New York: Oxford University Press, 2019), 38.

Bruno Brkic is a former police official from Bosnia and Herzegovina with extensive experience working in the areas of law enforcement, criminal justice, and antiterrorism. He is a Senior Police Academy graduate and holds a BA in Criminal Justice. In addition to an MA in Criminology and Security from the Independent University of Banja Luka, he recently earned an MA in Cyber Intelligence from the Daniel Morgan Graduate School of National Security in Washington, DC. He also received training from the Diplomatic Academy of Vienna, conducted research as a Fellow with the Italian Department of Public Security in Rome, and completed an internship with the U.S. House of Representatives. Bruno spent eight years working in Bosnia and Herzegovina on European Union-related projects advancing law enforcement capabilities in fighting organized crime and terrorism. He is passionate about confronting violent extremism leading to terrorism and uses his knowledge and experience to enhance policing in urban areas. Bruno strongly advocates for private-public partnerships in protecting human rights and human lives.

Weaponizing Space:
It Was Just a Matter of Time

by Lt Col (USAF, Ret) James J. Rooney, Jr.

THE STRATEGIC BACKDROP

A strategic shock is an event, or series of events, often triggered by rapidly changing social conditions that completely disrupt the normal political, economic, and social trajectories of a state. The effects can be temporary or permanent. In the case of the Bubonic Plague, the Great Depression, and two world wars in one century, a strategic shock can have global effects. COVID-19 might well fit the definition. Across an international landscape, current and future plans, programs, policies, national economies, and the lives of tens of millions are being inextricably altered by a microscopic pestilence turned pandemic. At the macroscopic level, one could argue that another, more insidious strategic shock waits stealthily in the shadows, patiently biding its time and seeking but the opportunity to emerge.

INTRODUCTION

Over the last two decades an exponential growth in affordable and disruptive technologies has created unparalleled opportunities for states to build power-enhancing capabilities reflected in the magnified optics of a greater status on the world stage. Nowhere is this more salient than in the realm of outer space. What was once the clear dominion of the privileged few is now actively open to the many. As of 2018, over 1,800 active satellites are in orbit, owned and operated by over 50 countries and multinational organizations.[1] Nine countries and one international organization can independently launch spacecraft: China, India, Iran, Israel, Japan, Russia, North Korea, South Korea, the United States, and the European Space Agency (from French Guiana).[2] Space has joined the air, land, and sea as an operational medium and in the process has initiated an ongoing international debate about access and control. Ironically, the key elements of the argument are framed by those same few with the power to affect the outcome. At the moment, the United States is considered the world's preeminent space power; most of the civilized world is unopposed to that status, but there are those who would gladly alter that reality for their own agendas.

By its very nature, space provides a unique vantage point from which to project strategic and tactical power. From an intelligence perspective, space is the ideal environment to conduct collection operations and has been so for over sixty years. Others have a different opinion. The military and intelligence collection capabilities that government and commercial remote-sensing satellites provide are reducing the ability of all countries to remain undetected while performing sensitive testing and evaluation activities or military exercises and operations.[3] Orbital overflight with impunity may have strengthened nuclear deterrence frameworks during the Cold War, but given the current counterspace technological state of the art, this continued invasive practice is now considered by certain states as a power projection hindrance. The argument is that such overflight interferes with national intent, exposes key military facilities, identifies defensive forces, and reveals critical vulnerabilities that put the state at a distinct disadvantage to its adversaries. The reasoning is that overflight creates an unnecessary and costly self-defense issue. Given the counterspace capabilities in development or test, this overflight situation is generally less acceptable than just twenty years ago and certain states are posturing to alter the status quo. These sentiments are clearly expressed in the doctrinal, strategic, and policy documents of several U.S. adversaries. This evolving and dangerous attitude reflects a recognition of space as being fundamentally different than other mediums and speaks volumes about the relative importance of space control as it relates to the political, military, and economic instruments of national power.

Air, land, and sea dominance often reflect localized control and limited effects, whereas space dominance can potentially have global influence and more profound effects. As a consequence, control of outer space provides a potentially irresistible temptation to an audacious opponent, and a Westphalian disruptor to a wary current hegemon. Though international law (Outer Space Treaty, 1967) bans nuclear weapons in space, there is little, other than loosely agreed to international norms of behavior, that prevents the weaponization of space. The convergence of technology and operational capability is changing the cost, risk, and benefit calculus creating incentives to circumvent unwritten rules and establish a new puissance in space. This global

and pervasive operational medium is truly the new high ground; control of space and global domination may be in the offing. The backstory here is instructive.

THE 4TH OPERATIONAL MEDIUM

Space has never really been an operational sanctuary; evidence to the contrary was always part emotional myth, part cognitive fantasy. Since the Soviet Union orbited Sputnik in October 1957, space has been militarized. The only reason space was not weaponized was because it was technically beyond the state of the art at the time. Territorial overflight by orbiting spacecraft was tolerated by the two superpowers not because it was their first policy choice but because there was nothing they could do about it. Eventually the overflights became an integral part of a Cold War deterrence strategy involving the Soviet Union and the United States that quite literally held each other's civil populations hostage to nuclear annihilation. Deterrence worked because it had to; the alternative was too horrific to contemplate. Then again, the leaders of the Soviet Union and the United States were rational actors forged from a Western cultural model. Today, things are quite different; for one thing, there are more active players in the arena, and cultural imperatives play a more dominant role. How this new reality evolved is important to understand. The fall of the Soviet Union in the early 1990s saw the end of the Cold War and an all too brief global respite from the fears of a nuclear holocaust that had plagued the world for half a century.

Though existential fears subsided, peace was still elusive. The hope-filled perception of better days ahead was seriously flawed as regional and proxy wars continued unabated across the globe. Systemic cultural and theocratic forces liberated from colonialism, and existing just below the metaphorical waterline, were already posturing to have their message seared into the consciousness of an unsuspecting world. On September 11, 2001, at 8:46 a.m., American Airlines Flight 11 crashed into the North Tower of the World Trade Center. There were five Islamic hijackers onboard. The toppling of the Twin Towers in downtown Manhattan made clear the message that the United States faced a new kind of asymmetric enemy whose very existence flew in just under the radar. The events of 9/11 reverberated around the world while inside the halls of U.S. executive power the Global War on Terror (GWOT) took center stage in terms of policy focus, economic investment, and military commitment. Iraq and Afghanistan found themselves in the crosshairs of U.S. retribution. Preemption now redefined defense and American generals, first bloodied as junior officers in the jungles of Vietnam, were eager to demonstrate how a revitalized and restructured military could prosecute a new kind of war. Integrated, cross-domain joint operations clearly and emphatically produced the "shock and awe" required to win an Iraqi ground war in 100 hours. Unfortunately, this new framework did not produce a timely and expected victory against state- and non-state-sponsored radical Islamic terrorism in Iraq, Afghanistan, or Sub-Saharan Africa. The GWOT continues; its finality is elusive. Despite the issues associated with these types of conflicts, there were many notable American military successes in the Gulf Wars, and these did not go unnoticed. [Editor's Note: The formal term "GWOT" was eliminated during the Obama administration, mainly because of arguments over whether terrorism was the target of the war or just a tactic used to prosecute it. As a result, the term became highly politicized. Nevertheless, many pundits, especially those leaning to the conservative side, still choose to use it.]

There exists a very real power struggle among Russia, China, and the U.S. for global political, economic, and military dominance, and control of space might very well be the quintessential prize.

On the sidelines, others were quietly watching the continuous video feeds, listening to the constant social chatter, reading the incessant text threads, and drafting reams of notes on how a potential enemy conducts modern warfare. The emergent dossier included weapon types, force allocation priorities, operational tactics, communication protocols, intelligence-surveillance utilities, and integrated strategic employment concepts including "just in time" logistics. Unfortunately, the purview revealed not only the precepts of U.S. joint doctrine, but an unprecedented microscopic view into specialized resource and capability dependencies that are exploitable. The U.S. all but showcased its fully integrated use of satellites into its war conduct matrix. Satellites in space serve as global eyes, ears, networks, and timekeepers for U.S. forces.[4] Within the theater of conflict, intelligence, surveillance, and reconnaissance (ISR) sensors provide the big picture; the global positioning system (GPS) supplies navigation and timing to aircraft, tanks, and infantry; weather satellites (DMSP) produces invaluable meteorological data for planners, operators, and post-strike analysts; and communications systems (DSCS, MILSTAR, SDS, UHF F/O) furnish integrated broadband voice, video, text, and data to joint forces across multiple platforms, units, and domains. For an adversary, this was tantamount to a tutorial on how the United States intends to wage war; for a foreign strategic intelligence analyst this is an "Achilles Heel" moment, a vulnerability worth capitalizing on. Foreign adversaries began retooling and restructuring almost immediately.

Currently, a tripolar nexus has replaced bipolarism as the dominant international geopolitical framework. Given the nature, history, capabilities, and intent of the contenders, this does not bode well for the U.S. The emergence of Russia from the detritus of the Soviet Union and the rise of China as a global economic engine seriously threaten the power and influence of the United States on the world stage. There exists a very real power struggle among Russia, China, and the U.S. for global political, economic, and military dominance, and control of space might very well be the quintessential prize. The United States, tenuously holding on to its status as space hegemon, can ill afford to lose its preeminence; there is too much at stake. The militarization of space began with Sputnik and a Cold War was defined by it; the weaponization of space is commencing and a new kind of war awaits definition.

U.S. strategic intelligence reports that over the last five years Russia and China have rewritten or restructured their joint doctrine, grand strategies, operational tactics, integrated force structures, technology investments, and engagement policies so as to leverage an almost autonomic reflex designed to counter U.S. space capabilities and advantages. The DNI's 2019 *Worldwide Threat Assessment* notes that Russia and China are training and equipping their military space forces and fielding new antisatellite (ASAT) weapons to hold U.S. and allied space services at risk, even as they push for international agreements on the non-weaponization of space.[5] Adversary political and capital investments are paying large dividends as U.S. military domination is quickly eroding in the face of political and policy intransigence, and an evolving threat landscape.

POLITICAL AND POLICY INTRANSIGENCE

Over the last four decades the world methodically and exponentially evolved from analog to digital, from industrial to informational, from regional to global, and from terrestrial to outer space; the U.S. acted in a key leadership role at each step along the way. For most of that time, space was a benign environment where any nation with the necessary technical and fiscal resources could safely access and securely operate. For its part, when it came to space, the United States went all in. Politically, economically, militarily, and socially, the United States is now highly integrated with, and heavily dependent on, space systems to support national development, functionality, services, and growth. No part of modern American life is left untouched by the influence of satellites with banking, transportation, medicine, trucking, food production, product distribution, the Internet, global communications, and social media representing just the tip of an ever-expanding iceberg of relevant dependencies. Unfortunately, evidence would seem to indicate the space environment is becoming less benign over time. A recent DIA report acknowledges that, when it comes to Russia and China, both states are developing jamming and cyberspace capabilities, directed energy weapons, on-orbit capabilities, and ground-based antisatellite missiles that can achieve a range of reversible to nonreversible effects.[6] Since many commercial satellites also provide services such as communications and remote sensing to the military, they are now legitimate targets for counterspace operations. The internationally accepted attitude that "space is taken for granted," i.e., it will always be there and is being held hostage to emerging threats which seek to alter the status quo and create the next strategic shock in the process.

Over the last four decades the world methodically and exponentially evolved from analog to digital, from industrial to informational, from regional to global, and from terrestrial to outer space; the U.S. acted in a key leadership role at each step along the way.

The U.S. *National Strategic Space Strategy* clearly recognizes that space, "a domain that no nation owns but on which all rely," is becoming increasingly congested, contested, and competitive.[7] But what, if anything, are policymakers doing to manage this impending crisis realistically? History, experience, observation, and intelligence forewarn that the advantage the U.S. holds in space—and its perceived dependence on it—will drive actors to improve their abilities to access and operate in and through space.[8] This follows the long arc of history in which no medium determined useful by the military will remain benign for long. The air medium, first established in 1903, remained benign for a mere eleven years before Spads and Fokkers, piloted by men like Rickenbacker and Richthofen, wearing leather skull caps, goggles, and white silk scarves, engaged over the battlefields of France, creating a new lexicon that included terms like "dogfighting," "air supremacy," and "aerial bombardment." An arms buildup or war in space will undoubtedly create its own concordance of terms and a new generation of heroes.

Maintaining U.S. space hegemony requires policymakers to understand and appreciate fully the evolving forces and threats aligned against the total U.S. space architecture, including military and commercial space assets, and then take steps appropriate at least to sustain the architecture status quo. Space is not a static operational environment; hence, there is debate about

what the status quo even means. Space launch vehicles and satellites supporting dozens of mission types are constantly being updated and enhanced to improve performance and to lower costs. Consequently, maintaining the status quo is really about sustaining a snapshot of space capabilities at selected moments in time. What adversaries are most concerned about with respect to the U.S. maintaining the status quo is the insertion of "breakout" technologies that provide an immediate strategic or tactical advantage. Maintaining the status quo has its adherents in government and the military, but there are other voices. There are those who argue that the U.S. should actually enhance and expand its space capabilities footprint so as to clearly dominate the environment for the foreseeable future. Given the time horizons required to design, develop, test, procure, and deploy new space capabilities, it seems strategically unwise to allow adversaries to reach capability par. Such a reality would put the U.S. at a disadvantage in the event that it is an adversary which develops a "breakout" capability.

The* National Security Space Strategy *(NSSS) in particular needs updating with respect to an acknowledgment of current and evolving threats from Russia and China.

Current U.S. space policy and strategy documents lean toward the maintenance of the loosely defined status quo. A closer examination of these documents reveals threat knowledge gaps, questionable strategic intelligence, and a lack of flexibility in terms of action/reaction in countering adversary initiatives. This limits the utility of these documents in terms of posturing the U.S. to maintain its lead in technologies, space, and joint architectures and operations designed to maintain U.S. space hegemony in general, and space supremacy more specifically.

There are six major U.S. documents which refer to space (as an operational medium) either directly or indirectly:

1. *National Space Policy*, June 28, 2010
2. *National Security Space Strategy*, January 2011
3. *National Security Strategy of the United States*, December 2017
4. *Summary of the National Defense Strategy of the United States*, 2018
5. *National Intelligence Strategy of the United State*s, 2019
6. *The Grand Strategy of the United States*, October 2014

The *National Security Space Strategy* (NSSS) in particular needs updating with respect to an acknowledgment of current and evolving threats from Russia and China. Currently, the document refers to supporting national security space objectives including the need to strengthen safety, stability, and security in space; maintain and enhance the strategic national security advantages afforded to the United States by space; and energize the space industrial base that supports U.S. national security.[9] The document does not offer specifics on the process, the products, or the funding required to achieve these objectives. In fact, none of these documents provides an actual operationalized framework for maintaining U.S. dominance in space. The Trump administration's establishment of the U.S. Space Force (USSF) is an attempt to operationalize some of these objectives. USSF must deal quickly with the policy and strategy shortcomings of the last two decades, especially in light of its adversarial competition. Russian and Chinese policy and strategy documents are quite specific in terms of how space integrates with their current force structures and how space systems will be defended from interference by other states. The offensive use of counterspace strategies and weapons is clearly delineated and supported in documentation and in capital investment. Recognizing that there is a problem is important, but a strategy also needs to talk about ends, ways, and means. Therein lies the problem for the United States.

U.S. policies and strategies over the last twenty years are complicit despite strategic intelligence warnings to the contrary. Consequently, the U.S. now faces limited strategic options. In fact, in this current environment, U.S. space architecture configuration enhancements would, in all likelihood, trigger an immediate response from Russia and China even if those changes were defensive in nature. Because the technology gap has narrowed so significantly, a space arms race could well ensue, rendering the academic debate about weaponizing space moot. With limited political, military, and diplomatic options available, U.S. policymakers need to focus on methods and frameworks that offer tangible and realizable solutions with proscriptively positive outcomes for maintaining the space status quo. Policymakers must prevent strategic shock, and delay for as long as feasible the weaponization of space. Taking a page out of the Cold War playbook might be a good place to start.

Unquestionably, U.S. moves to enhance the capabilities of its space architecture with respect to its adversaries will trigger a response. This reality was observed during the Cold War, and the "action-reaction" dynamic was at the heart of a theory of deterrence that helped to prevent nuclear holocaust for over fifty years. Space is a unique

environment with specialized strategic and tactical vantage points. Platforms and sensors operating in space provide their host with capabilities and advantages not possible with terrestrial-based systems. Having that capability, while potentially depriving others of the same, is the basis of space supremacy and control. When coupled with diplomacy and the other instruments of national power, space supremacy is at the core of space hegemony.

Theories of air, land, and sea power were created out of experiential paradigms which evolved over time and were supported by actual combat operations. There has not yet been a battle fought in space.

Space capabilities, like their nuclear counterparts, provide status and prestige as well as real political, economic, and military power. Moreover, not unlike nuclear capabilities, space platforms manifest intrinsic deterrent attributes as adversaries or competitors develop similar capabilities. States like Russia and China, whose extrinsic capabilities are at, or near, par with the U.S., usually achieve deterrence equilibrium and for the most part enjoy crisis stability until one side or the other changes the threat landscape. President Reagan did just that when he supported the development of the Strategic Defense Initiative. This was exactly the tit-for-tat situation that existed between the Soviet Union and the United States during the Cold War. The efficacy of Cold War deterrence theory as it might apply in principle to space is constantly under debate by academics and intelligence practitioners. One of the few areas of agreement between the disparate parties is that 2020 is not 1965.

The circumstances today are quite different, the international tapestry has changed, and key geopolitical forces are emerging which create an arena for a new global hegemonic power struggle. The world is quickly moving toward a tripolar framework in which power projection capabilities, economic strength, global reach, and cultural imperatives will dictate new norms for international relations. A key battlespace in this new conflict is the realm of outer space, and the sparring has already begun. Russia is actively trawling U.S. NRO satellites, China is testing ground-based laser weapons, and both countries are investing heavily in "kinetic-cyber" (KC) and "lethal autonomous weapons systems" (LAWS) designed for both terrestrial and counterspace applications. Of the two, China is the most worrisome because of its total investment and commitment to development. Both of these technologies have the potential to create strategic shock not just from the space hegemony perspective but from a legal, ethical, and moral one. The world is privy to a clash of cultures where world view is focused through differing ethical and moral lenses using multi-layered geopolitical/legal filters. The U.S. cannot simply see and react to this condition as an extension of Cold War politics with an additional competitor. The rules of the game are dynamically evolving and the U.S., by and through its own policy and strategy documents, is seemingly already behind.

The almost total dependence of the United States on its space systems for maintaining its political, military, economic, and social infrastructures creates additional dynamics which offer opportunities for peer competitors to leverage and seek advantage. Deterring such aggressive activities is not an easy task. From the perspective of the United States, the importance of space deterrence and crisis stability takes on a dimension not experienced during the Cold War. Managing deterrence and crisis stability within the space environment will seriously challenge U.S. policymakers for the next decade. To prevent a global strategic shock and to delay the weaponization of space, U.S. policymakers need better decision-making frameworks, models, and enhanced analytical tools. To better manage these peer competitor relationships, a more thorough understanding of space deterrence and crisis stability at the elemental and foundational levels is required. The use of Cold War deterrence paradigms will not suffice; new theories of space deterrence are required. These new theories have to be based on doctrine and strategies designed to project power to, in, and from space. That implies that there is actually a general theory of space power, which, in truth, there is not; it simply does not exist. Theories of air, land, and sea power were created out of experiential paradigms which evolved over time and were supported by actual combat operations. There has not yet been a battle fought in space. Nevertheless, the elements of such a theory do exist indirectly through modeling, simulation, and wargaming. For the time being those artificial frameworks will have to suffice in supporting the development of doctrine, strategy, and policy models that, in turn, support the creation of space deterrence and crisis stability management tools. The need for these tools is underwritten by the seriousness of the threats now facing the United States against this national utility and operating domain of space. Russian and Chinese counterspace threats are real and evolving.

THE THREAT

On December 24, 2019, President Vladimir Putin announced that Russia had officially taken the lead in the global hypersonic arms race, saying that his is the only nation in the world to have already deployed hypersonic weapons.[10] If true, and there is little reason to doubt the veracity of the statement, then Russia will have taken the pole position in a new-era "arms race." Flying in excess of Mach 5, these "wave rider" designs are nuclear weapon-configurable and their velocity makes them virtually impossible to intercept using the modern missile defense systems employed by U.S. forces.[11] Given the 60-plus years of direct experience with intercontinental ballistic missiles (ICBM), this new class of hypersonic weapon can now reach and threaten U.S. space satellites and other assets including deployed naval fleets. On February 11, 2020, it was widely reported in the press that two Russian "inspection" satellites had modified their orbital ephemeris and were now in orbital synchronization with USA 245, a National Reconnaissance Office (NRO) KH-11 "spy" satellite. This action is "publicly" unprecedented; the behavior is politically destabilizing and threatening. Russia is now playing a dangerous cosmic game which threatens 63 years of relatively benign space operations. China is also experimenting with "inspection" satellites that clearly have a dual purpose and utility. The People's Liberation Army (PLA) is surging ahead with major investments in artificial intelligence and kinetic cyber, two technologies which can support the development and fielding of lethal autonomous weapon systems. Used in a counterspace mode, these threats are particularly worrisome for the United States, which has done very little to protect its very vulnerable space system architecture.

The United States, Russia, and China were always interested in acquiring such an anti-satellite capability; space was, after all, not just another operating medium but one with some rather unique vantage points. International overflight with impunity spawned a whole new approach to the gathering of strategic intelligence through satellite reconnaissance. The intelligence requirements triggered a revolution in applied technologies that included optical and signal sensors, computational and processor architectures, communications and networking protocols, and launch and payload designs and operations. The impunity was a function of capability and there were several anti-satellite experiments and tests conducted in the 1970s and early 1980s, but the resultant backlash from the community of nations made the costs, intrinsic and extrinsic, higher than the expected benefits. In 1967, more than one hundred nations signed the "Outer Space Treaty," which outlined a general framework for expected normative behaviors between civilized states in their conduct to, through, and from space. Most nations heeded the admonition, but state-sponsored R&D did not stop nor did the experiments. Control of space is just too tempting a prize. Unlike air supremacy, which tends to be localized and temporary, space supremacy could theoretically be global and more persistent if coupled with terrestrial actions designed to ensure total dominance. Both Russia and China have sophisticated counterspace programs.

The People's Liberation Army (PLA) is surging ahead with major investments in artificial intelligence and kinetic cyber, two technologies which can support the development and fielding of lethal autonomous weapon systems. Used in a counterspace mode, these threats are particularly worrisome for the United States, which has done very little to protect its very vulnerable space system architecture.

Russia

A common theme heard among the national security policy community is that space has now become a contested warfighting domain. This is not true, however; space has been a contested warfighting domain from the beginning.[12] The first anti-satellite (ASAT) weapon was tested by the United States in 1959, just two years after the launch of Sputnik, and both the Soviet Union and the United States continued developing and testing anti-satellite weapons of various kinds throughout the Cold War.[13] Russia claims to be developing missiles that can be launched from an aircraft in mid-flight to destroy American satellites. Russia has been conducting highly sophisticated on-orbit activities that could enable it to maneuver its satellites into close proximity to ours, posing unprecedented new dangers to our space systems."[14] Recent events would seem to bear this out. A direct-ascent ASAT weapon is designed to strike a satellite or other orbiting object using a trajectory that intersects the target without placing the interceptor into orbit. This, in some ways, simplifies the geometry problem associated with orbital mechanics. A "co-orbital" ASAT weapon is actually placed into orbit and then, upon command from the ground or its onboard programming, maneuvers into close proximity to the target where it can perform its covert mission immediately or it can remain dormant in orbit for days or even years before being activated.[15] Both types of weapons require sophisticated guidance systems that allow the weapon to detect, track, and navigate the weapon to its intended target.

Russia is developing, testing, and fielding several versions of kinetic kill counterspace weapons, some based on older Soviet-style configurations, but others of a more recent design. These weapons cover the spectrum from ground- and air-launched, as well as those that would co-orbit with their targets. In December 2018, Russia conducted its seventh test of the PL-19/Nudol direct-ascent ASAT system.[16] Russia has developed several surface-to-air missile systems that could easily perform double duty as a direct-ascent ASAT weapon. The only element missing is the high-precision targeting capability that has yet to be demonstrated via a destructive test.[17] At this juncture, Russia has several different direct ASAT options available that can reach targets from low earth orbit (LEO) all the way out to geostationary orbit (GEO). Some of these ASATs could contain multiple individual warheads in a single launch, posing a serious threat to satellites in GEO.[18] New analysis published in *Jane's Intelligence Review* in September 2018 suggests that Russia's newest co-orbital system may be designed specifically to target satellites in GEO.[19] This "dual use" on-orbit inspection system appears to be similar to Russian rendezvous proximity operations (RPO) in LEO in 2017 and 2018. Such a system was used recently when two of these inspection satellites trawled an NRO KH-11 satellite.[20] The implied threat is obvious.

Over the years, Russia has developed a significant cyber-attack capability across multiple domains. The country poses a significant threat to the U.S. in space.

In the last decade, Russia has revitalized and revamped its Soviet-era directed energy counterspace weapons programs. In direct response to the U.S. "Airborne Laser" program, the Russians now claim to have both airborne and ground-based lasers capable of counterspace operations. Such weapons could degrade other satellite systems including solar arrays depriving the satellite of electrical power. Intelligence has reported that Russian laboratories are also hard at work developing high-energy particle beam weapons for use in close-up RPOs.[21]

For over a decade Russia has been improving and enhancing its cyber capabilities, so much so that it is now considered one of the world leaders in cyber. Beginning Russian hackers, using malware called Turla, have commandeered an old-style commercial Internet satellite service that unfortunately used unencrypted C2 data links.[22] Using such experiences to their advantage, Russian hackers are some of the most prolific worldwide regardless of the operating medium. In 2007 Russia was blamed for cyberattacks against Estonia which paralyzed online banking services, government communications, and national media outlets.[23] Similarly, over the past few years, Ukraine has sustained thousands of Russian cyberattacks throughout the Crimean conflict.[24] Over the years, Russia has developed a significant cyber-attack capability across multiple domains. The country poses a significant threat to the U.S. in space.

China

In April 1970, China launched its first satellite and over the ensuing five decades has been posturing itself to be a dominating, world-renowned space power. Over the last two decades, the country has amassed an impressive list of space accomplishments including launching and operating two space stations and landing a lunar rover on the dark side of the moon. China had 30 launches in 2019, including 10 satellites for positioning, navigation, and timing (PNT), as well as a new launch capability, the Long March 11, via a sea-based platform.[25] China has literally taken half the amount of time to arrive at its current state of the art in launcher and satellite technology as any other nation on earth. Along the way, the Chinese have reorganized their military to include space at a fundamental and integral level across all force structure domains. This understanding has paved the way for a very focused and objective-oriented counterspace program designed to unseat the United States.

China has a proven track record when it comes to kinetic physical counterspace capabilities. The country has developed a wide range of single- and dual-purpose direct ASAT and RPO capabilities. Its midcourse ballistic missile interceptors can easily be adapted to the ASAT role. The current focus is to attack targets in LEO, but the country is within striking distance of hitting targets in GEO within five years. Because of China's economic superpower status, it has sufficiently deep pockets to make serious investments in these technologies and capabilities. At the moment, strategic intelligence sources cannot pin down whether it will become an operational capability in the near future.[26] Speaking in 2015, then-Lt Gen James Raymond (chief of the new U.S. Space Force and the first commander of U.S. Space Command, turned over in August 2020 to an Army general) stated at a conference that, because of China's investment in ASAT weapons, "soon every satellite in every orbit will be able to be held at risk."[27] A kinetic ASAT attack in GEO could be devastating for the United States and other space-faring nations because the debris it would produce could linger for generations in this unique region of space and interfere with the safe operation of satellites.[28]

China has not been reticent about developing and testing technologies and platforms supporting RPOs. To date no RPO has resulted in any verifiable degradation or destruction of an orbiting asset. As already stated earlier, co-orbital satellites can serve a dual purpose (inspector or ASAT), and it is next to impossible without close-up inspection of the device to ascertain for which purpose it is programmed. Between 2010 and 2018, China conducted more than a half dozen or so RPO experiments in both LEO and GEO. In one instance, in July 2013, the Chinese placed three satellites into a common orbit and made the claim they were conducting scientific experiments on space maintenance technologies.[29] U.S. strategic intelligence reported that one of the satellites had a remote manipulator arm for grappling. This capability could be used for securing a satellite for repair or for counterspace operations against an enemy satellite. The Chinese RPO events did little or no damage, but what worries experts are the intentions behind the experiments. Given China's history, it would be hard to make the case that these are for peaceful purposes only.

In 2018 the U.S. Director of National Intelligence stated that China was making advances in directed-energy technology that can "blind or damage sensitive space-based optical sensors, such as those used for remote sensing or missile defense."[30] Moreover, Chinese military and technical writings often reference directed energy as a key technology in a successful counterspace strategy.[31]

Beginning in the 1970s, the United States made the conscious policy decision to migrate the majority of strategic intelligence collection from terrestrial- and airborne-based systems to space systems. The National Reconnaissance Office (NRO) owes its very existence to that choice.

Over the last two decades, China has invested significant resources in developing a cyber capability in both the offensive and defensive modes. It is well established that Chinese hackers have broken into U.S. government servers as well as those of industry, academia, and even Hollywood. The wealth of intellectual property and other forms of information stolen is incalculable. China's efforts to attack and infiltrate space systems have received relatively less attention.[32] However, a quick scan of Chinese military writers reveals that, in a conflict, China would conduct cyberattacks against U.S. satellites, links, and supporting ground stations. Attacking an adversary's command and control network by cyber means is becoming a seminal tactical issue with the Chinese military. In addition, China is experimenting with kinetic cyber in the counterspace role. Coupled with artificial intelligence and lethal autonomous weapons systems, these represent some of the more serious threats facing the U.S. commercial and military space architecture in the coming decade.

The risks to the United States are as insidious as they are substantial. Without key commercial and military satellites, the ability of the U.S. to respond in kind, replenish lost space and terrestrial infrastructure, or support joint military force operations worldwide would be crippled. Such an attack could also create catastrophic effects that could devastate U.S. economic stability and the free movement of capital. Whole industries and services would come to a standstill. Suffice it to say that the weaponization of space is no longer a topic for academic debate. In truth, as soon as the technology became available and affordable, it was inevitable that nations would try and capitalize on the situation by making space-dominating overtures in the hope of controlling an environment on which the entire world now depends.

IMPACTS ON STRATEGIC INTELLIGENCE

Beginning in the 1970s, the United States made the conscious policy decision to migrate the majority of strategic intelligence collection from terrestrial- and airborne-based systems to space systems. The National Reconnaissance Office (NRO) owes its very existence to that choice. With limited funding available, other forms of intelligence collection have faded more into the background, including human intelligence (HUMINT). In the process, the United States has created the world's most impressive armada of multi-billion dollar, space-based intelligence systems. For over five decades these large, technically complex, stand-alone systems remained safe from attack. Assuming it would always remain so ignored history. Not unlike the assumptions that went into the French Maginot Line, certain assumptions about the sanctuary of space have been premature and are now proving just as fallacious. In the case of Europe in 1939, instead of attacking the French lines directly, the Germans invaded through the Low Countries, bypassing the Maginot Line altogether to the north.

Currently, Russia and China are leveraging revolutionary technologies to build counterspace systems that in a few years will be capable of laying waste to the NRO architecture as well as other commercial and military space systems so necessary for the conduct of modern war and everyday life. Should this happen, the cost to the strategic Intelligence Community will be incalculable. With other forms of intelligence collection pushed to the backburner, the Intelligence Community will find itself

scrambling with the rest of the joint force to make up for the losses. HUMINT would take at least a decade to reconstitute, especially in an analog world. The point here is that the maintenance of U.S. space hegemony is not really a plausible option unless the United States takes steps to ensure it. There is no second place in this competition; it is, quite literally, a "winner takes all" situation if either China or Russia proves to be a match for the U.S.

THE WAY FORWARD

In January 2001, the Rumsfeld-led Commission to Assess United States National Security Space Management and Organization made some salient points about the U.S. position in space. The United States must develop, deploy, and maintain the means to deter attack and to defend vulnerable space capabilities.[33] The report went on to recommend that the development doctrine, CONOPs, and specific space capabilities be pursued through the formulation of national security guidance and policy initiatives. Such policy should include space weapon systems ready to act in either a defensive or offensive manner depending on the need. Such space systems should continue to augment air, land, and sea forces. The Commission recognized the need for a strategic deterrence strategy for space which should be strengthened and supported by a broader range of space-based capabilities. In 2001 this was a real possibility due to the technology gap that existed between the U.S. and any potential rival. Today, with technology convergence, such overt moves by the U.S. would likely trigger a space arms race with Russia and China. The Commission described areas for improvement in the U.S. space posture:

- Assured access to space and on-orbit operations
- Space situational awareness
- Earth surveillance from space
- Global command, control, and communications in space
- Defense in space
- Homeland defense
- Power projection in, from, and through space.[34]

Some 19 years later, the situation remains virtually the same. These improvements are still needed, but the environment within which such changes or improvements could be made is now more tenuous and dangerous. Still, the U.S. must act in its own defense. A combination of diplomatic initiatives, the building of global alliances, international agreements on weapons in space, and policies that underwrite the development and procurement of modest changes to the U.S. space architecture must progress, less the U.S. continue to cede more fertile ground. Space deterrence and crisis stability management, along with incremental enhancements which continue to leverage the advantages offered by technological breakthroughs, must continue unabated.

The U.S. response to the Russian and Chinese threat, though initially muted, now includes the investiture of a United States Space Force (USSF). The Space Force's mission is to "organize, train, and equip space forces in order to protect U.S. and allied interests in space and to provide space capabilities to the joint force."[35] The USSF is charted to develop:

- Space superiority
- Space domain awareness (military, civil, and commercial)
- Offensive and defensive space control
- Command and control of space forces and satellite operations
- Space support to operations (e.g., satellite communications)
- Space service support (e.g., spacelift and space range operations for military, civil, and commercial operators)
- Space support to nuclear command, control, communications, and nuclear detonation detection
- Missile warning and space support to missile defense operations[36]

To the Russians and Chinese, these mission sets are provocative and potentially destabilizing from a geopolitical perspective. Yet, both Russia and China have completely reorganized their own militaries to integrate and incorporate space systems capabilities into their joint warfighting structures. In many ways, the formation of the USSF represents a recognition of this reality and a means devised to sustain the space hegemonic status quo. Creating a USSF and chartering it with heady responsibilities is one thing; having the funding to actually build a combat ready force is something else. Policymakers and legislators must converge on a USSF budget line that goes way beyond merely transferring assets from the USAF Space Command to USSF. If done correctly, the U.S. Space Force, coupled with deterrence and crisis stability management, will act to maintain the status quo while diplomacy, in concert with international treaties, agreements, and alliances, acts to minimize an adversary counterspace response.

CONCLUSION

Pondering "what-ifs," or second-guessing decades-old decisions about what could have been done to prevent the space threats that the U.S. faces today, will yield little by way of solutions for the future. Granted, the GWOT seriously distracted U.S. policymakers from keeping a wary eye on the growing space threats posed by Russia and China. U.S. policymakers and the senior leadership of the USSF must work together seamlessly to build a forward-looking roadmap for the maintenance of U.S. space hegemony. Given that the U.S. cannot simply and suddenly weaponize space without a major pushback and response from adversaries, the senior leadership needs to have an innate understanding of space deterrence and crisis stability in order to better manage these geopolitical relationships. Pure and simple, space is an operational medium; it always was. Over the next decade, the only question that remains open is who will dominate? As noted in the 2001 Rumsfeld Space Commission, "We are on notice, but we have not noticed."

NOTES

[1] Not all nations have launch capability, but they do build various kinds of satellites and sensors that are manifested as "ride along" payloads aboard other's launch systems. Intelligence Report, 2019, "Challenges to Security in Space." Defense Intelligence Agency. Washington, DC. January: iii, https://media.defense.gov/2019/Feb/11/2002088710/-1/-1/1/SPACE-SECURITY-CHALLENGES.PDF. See also, "Satellite Database"; Union of Concerned Scientists (UCS); https://www.ucsusa.org/resources/satellite-database.

[2] Of the nine countries with space launch capability, four—namely, Russia, China, Iran, and North Korea—are not concerned about the best interests of the United States. Iran and North Korea have a history of being openly hostile to the U.S. and its allies. "How Many Countries Have Rockets Capable of Reaching Space?" *Space Answers*; March 21, 2013, https://www.spaceanswers.com/%20how-many-countries-have-rockets-capable-of-reaching-space/.

[3] The military and intelligence communities are relying more and more on commercial entities to provide gap-filling services and capabilities to supplement DoD and IC space assets. The downside is that these same commercial companies have put their systems on the adversary's target list. Chin, Carrey, 2011, "A Study on the Commercialization of Space-based Remote Sensing in the Twenty-First Century and Its Implications to United States National Security," Naval Postgraduate School, June 7, https://core.ac.uk/download/pdf/36699341.pdf. Also see "Space – An Enabler" Army Space and Missile Defense Command, *Army Space Journal* 2003, https://www.dtic.mil/dtic/tr/fulltext/%20u2/a525767.pdf.

[4] Erwin, Sandra, 2020, "Satellites at war: A week of U.S.-Iran tensions sum up military reliance on space," *Space News*, January 27: 1, https://spacenews.com/satellites-at-war-a-week-of-u-s-iran-tensions-sum-up-military-reliance-on-space/.

[5] Report, 2019, "Worldwide Threat Assessment," Director of National Intelligence, Government Printing Office, Washington, DC, January 29: 17, file:///D:/DSI/Dissertation/Readings/2019%20Worldwide%20Threat%20Assessment%20-%20DNI.pdf.

[6] Intelligence Report, 2019, "Challenges to Security in Space," Defense Intelligence Agency, Washington, DC, January: iii, https://media.defense.gov/2019/Feb/11/2002088710/-1/-1/1/SPACE-SECURITY-CHALLENGES.PDF.

[7] Report, 2011, "National Security Space Strategy," DoD/DNI, Government Printing Office, Washington, DC, January: i, https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2011/item/620-national-security-space-strategy.

[8] Intelligence Report, 2019, "Challenges to Security in Space," Defense Intelligence Agency, Washington, DC, January: iii. https://media.defense.gov/2019/Feb/11/2002088710/-1/-1/1/SPACE-SECURITY-CHALLENGES.PDF

[9] The NSSS lacks specificity in terms of implementing the ideas and concepts embedded in the full document. See Report, 2011, "National Security Space Strategy," DoD/DNI, Government Printing Office, Washington, DC, January: i, https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2011/item/620-national-security-space-strategy.

[10] This is a dangerous precedent and a potential game-changer in the sense that these kinds of weapons are not yet covered by specific treaty language and can be purposed as counterspace weapons against targets in LEO. See Hollings, Alex, 2019, "Putin says Russia is leading the world in hypersonic weapons. Is he right?" *SOFREP*, December 27: 1, https://sofrep.com/news/putin-says-russia-is-leading-the-world-in-hypersonic-weapons-is-he-right/.

[11] Mach 5 represents five times the speed of sound, or roughly 3,836 miles per hour. This is a breakthrough technology and a game-changer if considering its potential impact to counterspace operations. Staff report, 2019, "Russia Deploys First Hypersonic Missiles," World News, *The Guardian*, December 27: 1, https://www.theguardian.com/world/2019/dec/27/russia-deploys-first-hypersonic-missiles-nuclear-capable.

[12] Covers more than just the threats posed by Russia and China, but also by Iran and North Korea. Harrison, Todd, et al., 2019, "Space Threat Assessment 2019," Center for Strategic & International Studies, April 4: 1-57, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/190404_SpaceThreatAssessment_interior.pdf.

[13] Bowman, Robert, 1986, *Star Wars: A Defense Insider's Case Against the Strategic Defense Initiative*, Tarcher Publications. Los Angeles, CA: 14.

[14] The Vice President clearly sees space as a potential battlefield in the not so distant future. See Pence, Michael R., 2018, "Remarks by Vice president Pence on the Future of the U.S. Military in Space (speech at the Pentagon, Arlington, VA), August 9: 1, https://www.whitehouse.gov/briefings-statements/remarks-vice-president-pence-future-u-s-military-space/.

[15] U.S. Congress, Office of Technology Assessment, 1985, "Anti-Satellite Weapons, Countermeasures, and Arms Control," U.S. Government Printing Office, Washington, DC: 7, https://apps.dtic.mil/docs/citations/ADA338027.

[16] The evidence is clearly mounting that these kinds of tests have been going on for decades. The technologies coming into being are accelerating the pace of their use. Macias, Amanda, and Michael Sheetz, 2019, "Russia Conducted Another Successful Test of Anti-satellite Missile, According to a Classified US Intelligence Report," CNBC, January 18: 1, https://www.cnbc.com/2019/01/18/russia-succeeds-in-mobile-anti-satellite-missile-test-us-intelligence-report.html.

[17] Though targeting satellites in GEO could be devastating from a capabilities perspective, the targets in LEO are easier to attack and can cause extensive additional collateral damage in terms of space debris. Report, 2018, "Russia's ASAT Development Takes Aim at LEO Assets," *Jane's Intelligence Review*, 1, https://www.janes.com/images/assets/591/81591/Russias_ASAT_development_takes_aim_at_LEO_assets.pdf.
[18] The Russians continue to make evolutionary enhancements to existing systems. See Zak, Anatoly, 2017, "Naryad Anti-Satellite System (14F11)," *Russian Space Web*, November 30:1, http://www.russianspaceweb.com/naryad. html.
[19] These co-orbital systems are particularly worrisome in that they can be sold to the public as benign space inspection satellite systems when in fact they are really dual-purpose and dangerous from a counterspace perspective. See Hendrickx, Bart, 2018, "Russia Develops Co-orbital Anti-satellite Capability," *Jane's Intelligence Review*, September 27: 1, https://www.janes.com/images/assets/463/83463/Russia_develops_co-orbital_anti-satellite_capability.pdf.
[20] Budryk, Zack, 2020, "Russian spacecraft tailing US spy satellite, top Space Force official says," *The Hill*, February 10: 1, https://thehill.com/policy/international/russia/482340-russian-spacecraft-trailing-us-spy-satellite-top-official-says.
[21] Matveyev, Vadim, 2015, "Russia threatened by weapons of the future," *Russia Beyond (Science & Technology)*, November 9: 1, https://www.rbth.com/defence/2015/11/09/rusia-threatened-by-weapons-of-the-future_538647.
[22] Nakashima, Ellen, 2015, "Russian hacker group exploits satellites to steal data, hide tracks," *The Washington Post*, September 9: 1-2, https://www.washingtonpost.com/world/national-security/russian-hacker-group-exploits-satellites-to-steal-data-hide-tracks/2015/09/08/c59fa7cc-5657-11e5-b8c9-944725fcd3b9_story.html.
[23] McGuinness, Damien, 2017, "How a cyber-attack transformed Estonia," *BBC News*, April 27: 1-2, http://www.bbc.com/news/39655415.
[24] Sukhankin, Sergey, 2017, "Russian Electronic Warfare in Ukraine: Between Real and Imaginable," *RealClearDefense*, May 26: 1, https://toinformistoinfluence.com/2017/06/11/russian-electronic-warfare-in-ukraine-between-the-real-and-the-imaginable/.
[25] China has invested heavily in new and improved launch vehicles and support infrastructure. See Jones, Andrew, 2019, "China Will Attempt 30-plus Launches in 2019, Including Crucial Long March 5 Missions," *SpaceNews*, January 29: 1, https://spacenews.com/china-will-attempt-30-plus-launches-in-2019-including-crucial-long-march-5-missions/.
[26] This is an excellent source of information on Russia and China counterspace systems, doctrine, and strategies. Weeden, Brian, and Victoria Samson, 2018, "Global Counterspace Capabilities: An Open Source Assessment," Secure World Foundation, Broomfield, CO: 1-11, https://swfound.org/media/206118/swf_global_counterspace_april2018.pdf.
[27] Clark, Colin, 2015, "Chinese ASAT Test Was 'Successful': Lt. Gen. Raymond," *Breaking Defense*, April 14: 1-2, https://breakingdefense.com/2015/04/chinese-asat-test-was-successful-lt-gen-raymond/.
[28] Harrison, Todd, et al., 2019, "Space Threat Assessment 2019," Center for Strategic & International Studies, April 4: 12, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/190404_SpaceThreatAssessment_interior.pdf.
[29] Operationally responsive space is a capability that China has been seeking for decades. These kinds of rapid launches are pushing China closer to that goal. Report, 2013, "China Successfully Launches Three Satellites," *Economic Times*, July 20: 1-2, https://economictimes.indiatimes.com/news/international/world-news/china-successfully-launches-three-new-satellites/articleshow/71096464.cms.
[30] Coates, Daniel R., 2018, "Worldwide Threat Assessment of the U.S. Intelligence Community," Defense Intelligence Agency, Washington, DC: 13, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR—SSCI.pdf.
[31] Chen, David D., 2017, "Opening Statement of Mr. David Chen," testimony before the U.S.-China Economic and Security Review Commission, February 23: 75, https://www.uscc.gov/sites/default/files/transcripts/China%27s%20Advanced%20Weapons.pdf.
[32] The interesting part of this report is the dichotomy in what the Chinese write about in their war colleges and other organizations and what they publicly state in official reports to the global community. Report, 2015, "China's Military Strategy," The State Council Information Office of the People's Republic of China, USNI News, https://news.usni.org/2015/05/26/document-chinas-military-strategy.
[33] This commission led by Donald Rumsfeld was filled with ideas and recommendations that, if followed, could have put the U.S. in a permanent state of space hegemony. The events of 9/11 and the GWOT derailed the strategy. Executive Summary, 2001, "Commission to Assess United States National Security Space Management and Organization," Government Printing Office, Washington, DC, January 11: 16, https://fas.org/spp/military/commission/executive_summary.pdf.
[34] Ibid., 16.
[35] "Fact Sheet" (https://www.spaceforce.mil/About-Us/Fact-Sheet), spaceforce.mil, 7,
"Comprehensive plan for the organizational structure of the US Space Force" (https://velosteam.com/wp-content/uploads/2020/02/Space-Force-Report.pdf) (PDF), velosteam.com, 2020.
[36] Ibid., 1.

Lt Col (USAF, Ret) James J. Rooney, Jr., is a doctoral candidate in the new Strategic Intelligence program at American Military University. His dissertation, "Seizing the Ultimate High Ground: An Assessment of China's Effort to Supersede the United States as Space Hegemon," is a timely and relevant study with long-term implications for the space and intelligence communities. He spent 28 years on active duty in the Air Force serving in several key leadership positions at the Pentagon, the Phillips Laboratory, the Space and Missile Center, and the Operational Test and Evaluation Center. He is a command pilot with over 3,500 flight hours. He is currently Senior Manager of the Guidance, Navigation & Control Subsystem aboard the International Space Station for a large global defense company. Jim has published several articles in Modern Diplomacy (EU).

The Strategic Intelligence Implications of Circular Causality

by Jordan R. Beauregard

OVERVIEW

The United States, and other governments, are at least partially responsible for the emergence of the national security threats they perceive, based on the notion of circular causality. Circular causality is an interdisciplinary principle arguing that the actions of one actor in a complex system influence what happens at and between other actors in a system, and then what happens at and between other actors in a system influences the subsequent actions of the initial actor in the system. Based on a review of literature from the physical and social sciences, as well as international relations and national security, circular causality in complex systems occurs because of the iterative interaction of five key elements: structures, perceptions, actions, reactions, and counter-reactions (SPARC). Using the SPARC framework, this article examines the literature on circular causality to explain how threats in the international system that governments face emerge and persist because of circular causality. In doing so, this analysis highlights that using analytic frameworks, like SPARC, to assess circular causality in strategic intelligence analyses could improve U.S. policymakers' understanding of threat environments. However, this review also highlights that current U.S. policy and Intelligence Community (IC) organizational factors limit the extent to which circular causality could become a formal component of strategic intelligence analysis. Without acknowledging circular causality in strategic intelligence analysis, this article argues that policymakers, and intelligence assessments, will perpetually place the United States at risk of repeating past errors, particularly if past decisions affected the current nature of threat environments.

INTRODUCTION

Threats emerge, at least in part, because of circular causality, where the actions of an initial actor influence the system, and the consequences of that action on the other elements within the system impact the initial actor. Circular causality is a fundamental theory in the field of cybernetics, which studies how various forces and actors function, interact, and are organized within a system.[1]

Circular causality claims that a system's organization is the result of the behaviors of all components in the system, and that each component influences the others. Rhetorically, A influences B, which influences A, which influences B, causing a circular pattern of causes and effects.[2] Each actor is responsible for the system's organization. Systems can be as large as the entire planet, or as individual as the human mind. Systems can be animate or inanimate. In the social sciences, circular causality focuses on how humans interact with each other and with their environments, and the potential consequences of those interactions.

Circular causality in complex physical and social systems can explain how circumstances in the international system and in military operating environments shape the threats that governments around the world perceive and encounter. As such, understanding the level of circular causality in global and domestic operating environments can help intelligence analysts provide more comprehensive and contextual assessments about national security issues to the policymakers and decision-makers they support.

However, the national security community, at least in the United States, does not seem to focus on circular causality when assessing threats. Given that U.S. Presidential administrations determine national security priorities, the U.S. national security focus is subject to political transition. As such, intelligence and national security policy limits a comprehensive understanding of threat environments, thereby positioning policymakers potentially to repeat past errors, especially if their own past errors contributed to the current threat environment.

Circular causality literature from various fields in the social and physical sciences depends on the interaction of five key elements, based on a review of literature from the social and physical sciences, international relations, and national security: SPARC. It stands for structure, perception, action, reaction, and counter-reaction. In this synthesis, structure refers to the distribution of power and positions in the system. Perception refers to the perspectives which actors have within the system, about the system, and about other actors in the system. Actions refer to how the actors enforce or manage their perceptions. Reactions are how the system,

and the other actors in the system, respond to the initial actor's actions. Counter-reactions are how the initiating actor responds to the system's reactions. The concurrent interactions among these components (SPARC) can explain how circular causality shapes the emergence of national security threats.

To synthesize the role of circular causality in threat emergence, this article will use the SPARC framework to communicate the theoretical schools of thought around circular causality. Theoretical examples come from psychology and cognition, cybernetics and physics, and even physiology and medicine. This analysis will also include theoretical and concrete examples of circular causality in the international system, coming directly from prominent international relations theories and military history. Thus, the notion that circular causality contributes to the emergence of national security threats has both theoretical and practical foundations pertinent to its incorporation into intelligence analyses.

STRUCTURE: POWER AND POSITION

"Where you stand depends on where you sit." This saying by Rufus Edward Miles, Jr., an American bureaucrat, became known as Miles' Law. Miles' Law communicates that one's level of influence and one's ideas emerge depending on that individual's position within the system. That position can determine power and access, and underpin the notion of structure as it relates to circular causality. This section does not attempt to argue the philosophical definitions of power, but that whatever defines power for a particular system can determine which actor(s) has more responsibility in shaping the system's organization.

Early concepts of circular causality literature implied that entities within a system could have equal influence on the other. In family systems, circular causality claims that each family member equally induces and is induced by the behavior of the other family members.[3] From this perspective, each member of the family has equal power over the situations influencing the dynamic of the family system.[4] For example, consider a child who is arguing with his or her parents. The parents yell at the child, prompting the child to isolate him/herself in the bedroom. In an effort to influence the child to come out, the parents pursue the child. However, the parents' pursuit further isolates the child, creating a circular pattern of advance and retreat.

Later notions of circular causality have incorporated the role that power can play in systems. In dynamic systems theory, circular causality is a process in which "a coherent, higher-order form or function *causes* a particular pattern of coupling among lower-level elements, while this pattern simultaneously *causes* the higher-order form."[5] In other words, there are superordinate (higher-level) and subordinate (lower-level) elements that influence each other. Family systems literature takes this superordinate- and subordinate-level characterization of circular causality further.[6] For instance, one report characterized family system power as "…the ability to get others to do, what you want them to do, either by persuasion or force."[7] In family systems therapy, the article noted, it would not be helpful to suggest or imply that a coerced family member was, at all, equally responsible as the coercer for the coercion he/she experienced.

Realism theory argues that nation-states act in accordance with their interests.

Even Newtonian physics, which highlights that every action has an equal and opposite reaction (Newton's Third Law of Motion), recognizes the role that power plays in physical systems.[8] Even when the opposite reactions are equal, factors like force, mass, velocity, and speed can make the effects of the reaction more than the original action.[9] Further, depending on some of those similar factors, objects at rest are likely to stay at rest, or objects in motion are likely to stay in motion, unless a more powerful force prompts a change in course (Newton's First Law of Motion).[10] Power is as fundamental a component of the physical world as it is of the social world.

Power structure and positioning are key components of several international relations and national security theories as well. Realism theory argues that nation-states act in accordance with their interests.[11] In accordance with this theory, nation-states seek power in the system relative to other nation-states under a zero-sum paradigm, believing that the more power they have the less other nation-states will have.[12] Realists see the world as anarchic, absent a central governing authority.[13] As a result, nation-states work to achieve power to ensure their survival.[14]

Principles of power in international relations theory also derive from the ideas of Karl Marx, which add dimensions of exploitation, subjugation, and contextual factors that lead to certain actions and reactions in the international system. Marxist international relations theory argues that the international system is composed of a small, consolidated elite that exploits the common people who, in reality, control the means and resources of production.[15]

One Marxist theory, World Systems Theory, frames the international economic system into three categories: the core, the periphery, and the semi-periphery. The core is composed of the elite, mostly democratic, economies (i.e.,

United States and Europe). The periphery is composed of the poorest economies (e.g., many countries in Africa). The semi-periphery straddles both reliance on the exportation of raw materials and contribution to elite social systems (e.g., Russia, China, and India). World Systems Theory argues that the core relies on this cycle of exploitation in the economic system to maintain hegemony, which is contingent upon the periphery's and semi-periphery's complicity.[16]

Though the majority of literature on structure in the system affords differing levels of responsibility to actors based on their position and power in the system, all of the literature also acknowledges the power of the weaker components of the system. Early family systems literature attests to the "power of the weak."[17] Dynamic systems literature denotes that even though there are levels (superordinate and subordinate) in a system, the actions at the subordinate levels influence the superordinate elements.[18] In Realism theory, weaker nation-states can increase their power relative to stronger states by forming coalitions and alliances.[19]

Last, and the most difficult to attain, is self-actualization, where individuals have creative freedom, self-awareness, and can achieve their full potential.

Antonio Gramsci's Marxist theory of cultural hegemony alludes to the power of the weaker elements of society. Cultural hegemony theory argues that the elites control the common elements of society not just by coercion or control, but also by proliferating its ideologies and cultures within civil society institutions.[2020]
Hobden and Jones, 147.

Concepts of self-identity and concepts of others' identities directly result from the pervasion of these ideas within institutions and, therefore, can shape the nature of political insecurity within societies.[21] Though powerful institutions rely on the subjugation of the common elements of society for dominance, Gramsci preferred the term cultural *hegemony* because it considers the power that the exploited members of the population have.[22] In social insurgency literature, "…poor people's movements…" succeeded because they used forums outside the elite's channels to levy grievances, creating such disruption to the elites' notion of society that they are induced to concede to the common people.[23] How the elite facilitate societal conditions can influence how the lower levels of society react.

Economic, political, and social subjugation very likely will, at some point, prompt a reaction from the exploited masses, and this is broadly based on Abraham Maslow's "Hierarchy of Needs." A psychologist, Maslow theorized that all people have needs, layered in tiers from the most basic, essential needs at the lower levels. The likelihood that higher-level needs are met depends on how many of the lower-level needs are met first.[24] Moreover, whether certain needs are met, and to what extent those needs are met, likely will reflect where in society an individual sits. The most basic needs are physiological (e.g., food, water, shelter). Next are safety needs (e.g., physical and financial security, protection). Third is love and belonging, when people feel they are adequately part of a community or have stable relationships. Fourth is esteem, feelings of pride and prestige. Last, and the most difficult to attain, is self-actualization, where individuals have creative freedom, self-awareness, and can achieve their full potential.[25] If populations lack adequate access to basic goods and services, there is higher likelihood of political, economic, and social instability.[26]

In summary, the literature on structure highlights that power, and the amount of it, can shape the nature of complex systems. The amount of power affects access to opportunities and services that satisfy critical needs. The structure of the system can shape ideologies and identity perspectives, which determine how the system is perceived and organized. Lastly, in certain circumstances, the less powerful elements of society can shape dynamics at the elite levels.

PERCEPTION: THE PRECURSOR TO ACTIONS AND REACTIONS

Perceptions influence actions and actions influence perceptions.[27] Therefore, in social systems, as in physical systems, circular causality derives not just from the actions, but also from the perceptions that prompt the actions. Consider the role of cognitive dissonance in human cognition. Imagine there are two products, A and B, and a person can choose only one. Both products have advantages and disadvantages but, for whatever reason, the person chooses Product A. Although the person chose Product A, the advantages of Product B do not simply vanish from the person's mind, producing dissonance. In response, the person rationalizes his/her choice to alleviate the discomfort surrounding the dissonance. For example, the person who chose Product A might try to persuade him/herself that Product B's advantages were not as attractive as he/she thought.[28]

The human mind is a complex system itself. When information is contradictory or challenges one's beliefs or ideas, it becomes a perceived challenge to balance the system. In response, humans might reject or "downplay" the information's relevance or ignore it (negative feedback). Less often, humans might change their minds to accommodate the new information (positive). In the absence of perceived knowledge about an issue, humans will rely on biases and heuristics to help

rationalize their thoughts and alleviate dissonance.[29] Once a human being develops a perspective on an issue, it becomes harder to change that perspective.[30]

Another method of managing cognitive dissonance is called motivated avoidance. Motivated avoidance occurs when people avoid engaging a complex or controversial topic for fear of having an uncomfortable conversation, precipitating a spiral of silence.[31] As a result, individuals leave it to governments or other authorities to engage the topic on their behalf.[32]

A notable concept in human perception is circular reasoning, a cognitive fallacy through which human beings justify conclusions based on the premises of the assumed conclusions themselves. "A convincing argument for conclusion can't rest on the prior assumption that C [is true.]"[33] Circular reasoning involves the "repetition of claims, but also that the arguer uses one repetition to support the other."[34] For example, Actor A claims that the government should make it illegal to destroy a city's old warehouses, because the warehouses are architecturally valuable. When asked to clarify the warehouses' value, Actor A argues that the warehouses give the city its distinctive character. When asked to justify how the warehouses give the city its distinctive character and why Actor A likes these warehouses so much, Actor A repeats the notion that the warehouses are architecturally valuable.[35] Circular reasoning implies that perceptions and actions are vulnerable to circular causality themselves.

The role of perception in shaping systemic phenomena is endemic in the physical sciences as well. For example, in quantum physics—a complex branch of physics that works to understand the foundational characteristics and behavior of matter and energy—there is one principle known as the observer effect. The observer effect argues that observation can affect events and phenomena simply by the act of watching them.[36] In addition, the longer an entity watches a phenomenon, the longer that phenomenon is altered.[37] This principle was famously visualized in an experiment in which electrons—negatively charged particles of matter—behaved as individual particles when under observation by an electronic detector, a device that can detect electrons, and as continuous waves when not observed by the detector.[38] In essence, observation can affect reality.

To ensure survival, human internal regulation systems are capable of "threat," or change, perception, which prompts the body's various systems to act. For example, human beings are healthy if they can maintain an internal body temperature of about 98.6°F. When the internal body temperature is at 98.6°F, the body temperature is in homeostasis, or homeothermia.[39] When humans enter an environment that causes the internal body temperature to change, the body becomes symptomatic and responds to restore the healthy temperature.

In the United States, the President has the legal authority to determine what national security threats are and their level of priority.[40] Therefore, national security threats depend on the perceptions of policymakers, even if others might disagree with those perceptions. In theory, those perceptions are driven by intelligence assessments and facts, but policymakers do challenge this information when it does not suit their interests.[41] The results include actions driven to execute policy agendas. Prussian General Carl von Clausewitz famously wrote, "War is the continuation of policy by other means."[42] Military action depends on threat perception, and threat perception depends on political perception. For instance, in realist international relations theory, weaker nation-states in the power structure can balance or bandwagon when they perceive that their power is low relative to another nation-state.[43] However, balancing or bandwagoning first requires threat perception.

National security threats depend on the perceptions of policymakers, even if others might disagree with those perceptions. In theory, those perceptions are driven by intelligence assessments and facts, but policymakers do challenge this information when it does not suit their interests.

In his book *Of Paradise and Power*, realist scholar Robert Kagan wrote that after World War II much of Europe relied on the United States for security assistance, especially as the Soviet Union consolidated its power. The perceived threat of communism was so salient in Europe that, when the United States enacted certain foreign policy decisions with which many European countries disagreed, those same countries remained silent, bandwagoning with the United States because they did not want to risk losing American protection.[44] As a result, U.S. policy went unchallenged and its relative power increased.[45]

Cultural hegemony also refers to the role of perception in influencing the behavior of a population. Elites do not rely, exclusively, on use of coercion and force to control populations. Rather, hegemony in society depends on the proliferation of culture, of ideas.[4646]
Jones, 41.

Therefore, perception is both a tool and a consequence of systemic power structures. Though cultural hegemony developed as a theory of intrastate politics, Marxist international relations theories apply this framework to the international system. The perceptions that develop as

a result of the legitimization of particular ideas and cultures then contribute to actions and inactions within the system. However, every action—and inaction—has a reaction.

ACTION AND REACTION: THE SUBSTANCE OF THE SYSTEM

Threat environments emerge because the interactions between one or more parties likely happened in such a way that the consequences were negative for at least one of those parties. According to David Belt of NIU, "[T]he political security of a state or group that we identify as a threat is paradoxically dependent upon its insecurity—upon the world of opposing or dangerous others or enemies."[47] Therefore, the development and identification of an entity as a threat depends on the level of opposition that entity faces. As a result, if one's own government or organization considers an entity as a threat, it is necessary to understand whether one's own government's opposition to that threat contributed to the emergence of that threat. Did one's actions produce the negative reaction—threat emergence—in the system?

The notion that actions have reactions is endemic in social environments and in the physical world. In both, there are feedback control loops, or feedback mechanisms. Feedback mechanisms occur when there is a change or threat to the system's balance or stability. Once the system identifies the change or threat, the system's elements respond to restore the balance. There are two types of feedback mechanisms: positive and negative. In positive feedback mechanisms, the response to the change further amplifies the effects of the event.[48] In realist international relations theory, the situation in which weaker states bandwagon with the more powerful state would be interpreted as a positive feedback mechanism because the actions of the weaker states amplified the stronger state's power and influence.

A negative feedback loop occurs when the system's response aims to counteract the changes in the system, and reduce the effect of the changes.[49] In realist international relations theory, the event in which weaker states balance with each other against the superior power would qualify as a negative feedback loop in the international system. Negative feedback loops, in particular, are critical to the survival of organisms. In the earlier example of how the human body maintains a steady internal temperature, negative feedback loops are essential. If the body's internal temperature falls too far below homeostasis, the body works to reestablish homeothermia using central, endocrine, and metabolic processes (i.e., shivers and sweat).[50]

Feedback mechanisms sometimes do not work, however. For example, some manifestations of cancer diseases occur because the body fails to detect and destroy damaged cells. When the body fails to implement these processes, the cell division processes result in the rapid increase of damaged cells.[51] Also, sometimes the feedback reactions are not strong enough to produce the needed effects. For example, although Newton's Third Law of Motion highlights that actions have equal and opposite reactions, the effects on the opposing forces are not equal, particularly when considering factors like mass, speed, velocity, etc. For instance, a human being pushing against a wall is unlikely to move the wall, but the force opposing the person from the wall is likely to push the person in the other direction.

On occasion, negative feedback mechanisms could inadvertently cause positive feedback responses, amplifying the consequences of the initial interaction. For example, in realist international relations theory, the act of weaker states forming a coalition might signal to the stronger state that it, also, should form a coalition, thereby maximizing the stronger state's power and creating more tension. Actions and reactions are essential and factual attributes of natural and social systems. However, how responsible actors respond and manage the consequences of actions can shape the future interactions between elements of the system.

COUNTER-REACTION: MANAGING THE REACTION SHAPES THE FUTURE

Literature so far has characterized the role of power structure, perception, action, and reaction in circular causality, all of which interact iteratively and simultaneously across various higher-order and lower-order systems. Additional literature describes one further dimension to circular causality: the counter-reaction. Even if the system's reaction is negative or resistant, the counter-reaction of the entity with the most power and influence in the system can determine the nature of subsequent interactions between different systemic elements.

Consider what happens when a company learns that one of its products has a defect. How the company manages the news of the defect will shape whether that company succeeds in maintaining its consumer base and its credibility.[52] In 1982 seven people died from ingesting cyanide-laced Tylenol. The Tylenol manufacturer, Johnson & Johnson, pulled all Tylenol products off the shelves and took the responsibility to engineer tamper-resistant packaging before resuming production and distribution. After the crisis, Johnson & Johnson gained positive attention for how it managed the crisis and 90 percent of people in polls did not blame the company for the crisis.[53] Though Johnson & Johnson did not lace its product with cyanide, it was the "responsible actor" within the system, with the most influence and authority over how the Tylenol product was distributed and manufactured. Had it attempted to deflect responsibility, it likely would have lost significant consumer loyalty.

In Ancient Greece, the city-states Athens and Sparta fought a nearly 30-year conflict known as the Peloponnesian War. The Peloponnesian War is used by military historians and strategists as a multifaceted, thematic conflict that highlights the role of physical and social interactions in the proliferation and conduct of war. In his history of the Peloponnesian War, Athenian General Thucydides claimed that Sparta started the war with Athens because Athens was a rising power and Sparta perceived a threat to its power; consequently, it went to war.[54] Thucydides theorized that Sparta's decision to war with Athens derived from three overarching perceptions: fear, honor, and interest.[55] According to Thucydides, as interpreted by later scholars, Sparta *feared* that Athens was rising to compete with Sparta. Because of Athens' rise, Sparta was concerned that its *honor* was at stake as leader of the Peloponnesian League, the alliance it led against the Athenian-led Delian League. If it did not respond to Athenian "aggression," Sparta perceived its leadership in the alliance, and the alliance's and Sparta's security net overall, would crumble. As a result, it was in Sparta's *interest* to go to war with Athens.[56] There is considerable debate, even today, over this assessment, for there were many isolated actions that precipitated conflict between Athens and Sparta and led both to declare war. However, evaluating this assessment falls outside of the scope of this article. Today, the assessment is known as the "Thucydides Trap," the belief and paradigm that an existing hegemon and rising power will inevitably go to war to compete for the "top spot."[57]

Though Thucydides' assessment about the Peloponnesian War is up for debate, fear, honor, and interest remain prevalent perspectives in realist international relations theory for why countries pursue power.[58] In contemporary national security circles, the Thucydides Trap alludes to the perceived hegemonic conflict between the United States and China, with the United States acting as the de facto existing hegemon, and China as the rising power.[59] In his book *Destined for War: Can America and China Escape Thucydides' Trap*, Harvard scholar Graham Allison presents how close the United States and China are to succumbing to this trap, despite the fact that literature indicates neither wants a war with the other.[60] In his book, Allison emphasizes that war is not inevitable, between the United States and China or between any actors in the international system, citing cases where global powers were able to maintain peace.[61] However, cooperation between actors with divergent interests relies on the actions of a "focal point" of cooperation.[62] In other words, a particular actor usually must exercise the willingness to cooperate to precipitate cooperation and this actor is usually the most powerful in the system. Therefore, whether tension escalates between actors depends on the counter-reactions of the responsible actors.

The counter-reaction is an evident principle in war theory. In *On War* Clausewitz wrote, "...even the ultimate outcome of a war is not always to be regarded as absolute. The defeated state often considers the outcome merely as a transitory evil, for which a remedy may still be found in political conditions at some later date."[63] In other words, Clausewitz asserted that the events at the conclusion of a war can precipitate the conditions for future conflict. In principle, even if the reactions to particular circumstances are negative, the responsible actor can decide to take an action that elicits more positive interactions in the future. The outbreak of war is an inarguably negative reaction to something that occurred in the international system. How the victor or other powerful actors respond to the war, and the victory, can either mitigate or promote future conflict. This is the case even if the responsible actors were not directly fighting the war. In the Johnson & Johnson case, even though the company was not responsible for poisoning its product, it responded to the "conflict" in such a way that built credibility.[64]

The notion of how the powerful or superior actor manages the conflict with the adversary in a given scenario even resides in Sun Tzu's *The Art of War*. "Do not thwart an enemy returning homewards. To a surrounded enemy you must leave a way of escape. Do not press an enemy at bay."[65] These passages are not saying that an advancing force should not do what is necessary to defeat the adversary. Rather, the passages are advising not to do *more* than necessary. If the counter-reaction to an adversary's likelihood of defeat is to advance violently without restraint, there is a risk that "…they will turn on us and fight to the death."[66]

U.S. Senator William Marcy from New York once remarked, "To the victor belong the spoils of the enemy."[67] [Editor's Note: Marcy, a veteran of the War of 1812, was also a governor of New York, Secretary of State, and Secretary of War.] In other words, the victor in a competition or conflict can make decisions and take advantage of benefits that come from victory over the loser. Upon such victory, the balance of power in the system—the structure—shifts in favor of the victor over the others. Although the victor *can* take all the benefits it wants, the question becomes *how* and *to what extent* it takes the benefits. At this point, it becomes the "focal point" of cooperation.[68] When the victor attains a higher level of power in the system over others, how does it use that power? Does the victor work to create a system in which all parties can move forward with dignity—a "way of escape"—or does it pillage the defeated adversary for everything it is worth? In the SPARC framework, war is the reaction. The counter-reaction is how the powerful or victorious actor manages the war and its outcomes. The counter-reaction which the victor chooses can determine the likelihood that war will occur again.

IMPLICATIONS FOR STRATEGIC INTELLIGENCE ANALYSIS

Clausewitz wrote, "War is never an isolated act…it must be remembered that neither opponent is an abstract person to the other... War never breaks out wholly unexpectedly, nor can it be spread instantaneously." By this, Clausewitz highlights there is context that leads to the outbreak, conduct, and exacerbation of war and other conflict. War does not simply emerge. It comes from the context of interactions between states. Most importantly, war between certain parties is not random. If certain parties are going to war, they have interacted with each other in the past, the actions precipitated negative perceptions from the perspective of at least one of those actors, and the reaction was war. As such, if a particular actor perceives the threat of conflict with other actors, that actor has somehow interacted with the system and its elements, contributing to the risk of conflict. This is the underlying principle of circular causality. The level of circular causality a particular actor experiences, however, depends on the circumstances.

Structure, perception, action, reaction, and counter-reaction (SPARC) provide an effective framework for understanding when, and to what extent, circular causality influences the nature of a threat environment and the responsibility of individual actors in shaping the threat environment. This article focused on the theory and science around circular causality to legitimize the rationale for its role in nature and in social systems. Although some concrete examples were included throughout this evaluation, circular causality research, particularly in the national security field, would benefit from deeper research on the potential role that circular causality plays in conventional and non-conventional threats—perhaps using the SPARC framework—in history, the present day, and in the future. Bolstering the theoretical validity of the SPARC components of circular causality could involve individual examinations of the factors of each component (i.e., deeper research into the theoretical underpinnings of structure, perception, action, reaction, and counter-reaction). In general, circular causality research in national security environments could benefit from a more in-depth analysis of the organizational factors that would promote or limit its understanding in national security contexts.

In the U.S. Intelligence Community, analysts are required to adhere to certain standards. Codified in Intelligence Community Directive 203, these standards aim to ensure that analysts are objective and independent of political considerations.[69] These standards, in theory, encourage analysts to provide policymakers and decision-makers with the most comprehensive picture possible of national security threats and issues. A framework like SPARC, which could formally incorporate the role of circular causality into analyses, would add more context to strategic intelligence analyses, potentially even indicating whether U.S. actions have impacted, or could impact, the nature of the threats it perceives.

Another intelligence field that would benefit from circular causality analysis is counterintelligence (CI), the practice of preventing and mitigating an entity's vulnerability to espionage or compromise.

Nevertheless, there are organizational factors limiting the contextual awareness that could come from circular causality frameworks. For example, in the field of operational environment intelligence analysis—which aims to understand and communicate the physical and cultural impacts of national security issues—there is a policy focus on the *current* nature of particular threats and adversaries.[70] However, the current nature of a threat environment, as alluded to in various social and physical interactions, derives from historical and external elements.[71] Therefore, the current nature of an issue is not actually current. Failing to apply contextual frameworks to operational environment analyses perpetually provides policymakers and military decision-makers with a manipulated and limited lens through which to interpret reality, potentially positioning them to repeat their own or others' past errors.

Another intelligence field that would benefit from circular causality analysis is counterintelligence (CI), the practice of preventing and mitigating an entity's vulnerability to espionage or compromise. CI professionals understand that there are reasons why people turn to espionage, against their own government or others. In one framework, CI professionals synthesize the drivers as MICE (Money, Ideology, Coercion/Compromise, or Ego).[72] One article advocates for the RASCLS framework (Reciprocation, Authority, Scarcity, Commitment and Consistency, Liking, and Social Proof) rather than MICE. The article claims that the RASCLS framework better characterizes the factors which describe human motivation.[73] However, this framework sets up CI organizations to continue to face CI challenges because it fails to address why human beings become vulnerable to the motivational factors in the RASCLS framework in the first place. The MICE framework, though broad, highlights how contextual factors, like those from Maslow's Hierarchy of Needs, affect an individual's vulnerability to the persuasion and motivation factors in the RASCLS framework.[74] Surveillance and enforcement are necessary, but insufficient, in reducing CI threats. Organizations can mitigate the CI threat only by addressing the contextual drivers behind a person's vulnerability to turn spy.[75]

Although helpful in understanding the operational threat environment or CI issues, circular causality is unlikely to become a mainstream component of strategic intelligence analysis unless organizations can accept its utility and communicate a "convenient" framework. There are organizational challenges that likely will inhibit broad application of circular causality frameworks, like SPARC. First, understanding circular causality in threat environments may require a deep understanding of the unique drivers behind threat perceptions and conditions, which would require historical analyses that existing policy does not prioritize. This is likely due, in part, to the short-range political cycles through which national security threats and priorities are determined. Second, intelligence analysts commonly resist the implementation of structured analytic techniques, even if they help overcome biases, because they do not perceive they have enough time in their organizational settings to utilize these techniques fully.[76] However, unless IC organizations formally recognize circular causality and incorporate it into their analyses, even if the circular causality refers to U.S. actions, intelligence assessments will almost certainly remain incomplete.

CONCLUSION

Based on the systemic role of circular causality in the social and natural aspects of the world, the literature suggests that circular causality has a role in the emergence of threats which humans and governments perceive and experience. Specifically, the literature even implies that one's actions—or one's own country's actions—are, in part, responsible for its own threats. Circular causality does not judge whether those actions were "right" or "wrong," just that those actions have consequences and those consequences elicit reactions. Neglecting this possibility because of policy priorities regarding the current nature of threats, or the perceived lack of time to understand the potential circular nature of issues, leaves governments perpetually blind to their potential roles in the systems in which they operate and the threats they might influence.

[Author's Note; The views expressed in this article are those of the author and do not reflect the official policy or position of the Department of Defense, the Defense Intelligence Agency, or the U.S. government.]

NOTES

[1] Francis Heylighen and Cliff Joslyn, "Cybernetics and Second-Order Cybernetics," in R.A. Meyers, ed., *Encyclopedia of Physical Science and Technology*, 3rd ed. (New York: Academic Press, 2001), 2.
[2] Thomas Fischer, "Blind Spots Obscuring Circular Causality in Design and Elsewhere," *Kybernetes* 44, no.18/19 (2015), 1233-1234.
[3] Daniel Willbach, "Ethics and Family Therapy," *Journal of Marital and Family Therapy* 15, no. 1 (1989), 44.
[4] Christine E. Murray, "Controversy, Constraints, and Context," *The Family Journal: Counseling and Therapy for Couples and Families* 14, no. 3 (July 2006), 234.
[5] Marc D. Lewis, "Bridging Emotion Theory and Neurobiology Through Dynamic Systems Modeling," *Behavioral and Brain Sciences* 28 (2005), 174.
[6] Willbach, 44; Murray, 235.
[7] Willbach, 44; Murray, 235.
[8] Isaac Newton, *Mathematical Principles of Natural Philosophy*, translated by Andrew Motte (Rough Draft Publishing, 2011).
[9] Newton, Law III.
[10] Newton, Law I.
[11] Tim Dunne and Brian C. Schmidt, "Realism," in *The Globalization of World Politics: An Introduction to International Relations*, 6th edition, eds. John Baylis, Steve Smith, and Patricia Owens (Oxford, UK: Oxford University Press, 2014), 101.
[12] Dunne and Schmidt, 110.
[13] Dunne and Schmidt, 101.
[14] Dunne and Schmidt, 108.
[15] Stephen Hobden and Richard Wyn Jones, "Marxist Theories of International Relations," in *The Globalization of World Politics*, 143.
[16] Hobden and Jones, 146.
[17] Willbach, 44.
[18] Lewis, 174.
[19] Dunne and Schmidt, 101; Lorenzo Cladi and Andrea Locatelli, "Bandwagon, Not Balancing: Why Europe Confounds Realism," *Contemporary Security Policy* 33, no. 2 (2012), 264.
[20] Hobden and Jones, 147.
[21] David D. Belt, "An Interpretive Sociological Framework for the Analysis of Threats," *American Intelligence Journal* 32, no. 1 (2015), 52.
[22] Steve Jones, *Antonio Gramsci* (New York: Routledge, 2006), 41; Lewis, 174.
[23] Doug McAdam, "Tactical Innovation and the Pace of Insurgency," *American Sociological Review* 48, no. 6 (December 1983), 736.
[24] Stoyan Stoyanov, *An Analysis of Abraham Maslow's A Theory of Human Motivation"*(London: Macat International, 2017), 37.
[25] Goede and Boshuizen van Burken, "A Critical Systems Thinking Approach to Empower Refugees Based on Maslow's Theory of Human Motivation," *Systems Research and Behavioral Science* 36 (2019), 719.
[26] Office of the Director of National Intelligence, *Worldwide Threat Assessment of the Intelligence Community* (Washington, DC, 2019), 21.
[27] Richard M. Perloff, *The Dynamics of Persuasion*, 6th edition (New York: Routledge, 2017), 87; David Vernon, "Embodying Cognition and Circular Causality: On the Role of Constitutive Autonomy in the Reciprocal Coupling of Perception and Action," *Frontiers in Psychology* 6, no. 1660 (October 2015), 1.
[28] Leon Festinger, "Cognitive Dissonance," *Scientific American* 207, no. 4 (October 1962), 95, https://www.jstor.org/stable/pdf/24936719.pdf,accessed on February 8, 2020.
[29] Richards J. Heuer, Jr., *The Psychology of Intelligence Analysis* (Washington, DC: Central Intelligence Agency, 1999), 10.

[30] Richards J. Heuer, Jr., *The Psychology of Intelligence Analysis* (Washington, DC: Central Intelligence Agency, 1999), 10.
[31] Steven Shepherd and Aaron C. Kay, "On the Perpetuation of Ignorance: System Dependence, System Justification, and the Motivated Avoidance of Sociopolitical Information," *Journal of Personality and Social Psychology* 102, no. 2 (November 2011), 265, https://www.apa.org/pubs/journals/releases/psp-102-2-264.pdf., accessed on February 8, 2020; Edward Maibach, Anthony Leiserowitz, Seth Rosenthal, Connie Roser-Renouf, and Mattew Cutler, *Is There a Climate "Spiral of Silence" in America?* (New Haven, CT: Yale Program on Climate Communication, 2016), https://climatecommunication.yale.edu/publications/climate-spiral-silence-america/, accessed on February 8, 2020; Elisabeth Noelle-Neumann, "The Spiral of Silence: A Theory of Public Opinion," *Journal of Communication* 24, no. 2 (June 1974), 43.
[32] Shepherd and Kay, 265.
[33] Lance J. Rips, "Circular Reasoning," *Cognitive Science* 26 (2002), 767.
[34] Rips, 768.
[35] Rips, 768.
[36] Weizmann Institute of Science, "Quantum Theory Demonstrated: Observation Affects Reality," *Science Daily* (February 27, 1998), https://www.sciencedaily.com/releases/1998/02/980227055013.htm, accessed March 25, 2020.
[37] Weizmann Institute of Science.
[38] Weizmann Institute of Science.
[39] Terrien, Perret, and Aujard, 1428.
[40] 50 U.S.C. §3003(5)(A); Office of the Director of National Intelligence, *Intelligence Community Directive 204: National Intelligence Priorities Framework* (Washington, DC, 2015), Section D(2).
[41] Mark M. Lowenthal, "Tribal Tongues: Intelligence Consumers, Intelligence Producers," in *Intelligence: The Secret World of Spies, An Anthology*, eds. Loch K. Johnson and James J. Wirtz (New York: Oxford University Press, 2015), 199.
[42] Carl von Clausewitz, *On War*, eds. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 87.
[43] Dunne and Schmidt, 101; Cladi and Locatelli, 264.
[44] Robert Kagan, *Of Paradise and Power* (New York: Random House, 2004), 109.
[45] Robert Kagan, *Of Paradise and Power* (New York: Random House, 2004), 109.
[46] Jones, 41.
[47] Belt, 52.
[48] Roz Dixon, "Systemic Thinking: A Framework for Research into Complex Psychosocial Problems," *Qualitative Research in Psychology* 4 (2007), 152; Heylighen and Joslyn, 11-12; Lewis, 174.
[49] Heylighen and Joslyn, 11-12; Lewis, 174.
[50] Terrien, Perret, and Aujard, 1428.
[51] John C. Reed, "Dysregulation of Apoptosis in Cancer," *Journal of Clinical Oncology* 17, no. 9 (September 1, 1999), 2941.
[52] Perloff, 297.
[53] Perloff, 297.
[54] Bonnie S. Glaser, "U.S.-China Relations: Managing Differences Remains an Urgent Challenge," *Southeast Asian Affairs* (2014), 82.
[55] Robert B. Strassler, ed., *The Landmark Thucydides: A Comprehensive Guide to the Peloponnesian War* (New York: Touchstone, 1996), 43.
[56] Strassler, 43; Donald Kagan, *On the Origins of War and the Preservation of Peace* (New York: First Anchor, 1996), 57.
[57] Glaser, 82.
[58] Dunne and Schmidt, 101.
[59] Glaser, 82.
[60] Belfer Center of Science and International Affairs, "Can America and China Escape Thucydides's Trap?" Harvard University Kennedy School of Government (2020), https://www.belfercenter.org/thucydides-trap/case-file, accessed March 28, 2020.
[61] Belfer Center of Science and International Affairs, 2020.
[62] Thomas C. Schelling, "Bargaining, Communication, and Limited War," *Journal of Conflict Resolution* 1, no. 1 (March 1957), 23.
[63] Clausewitz, 80.
[64] Perloff, 297.
[65] Sun Tzu, *The Art of War*, translated by Samuel B. Griffith (London: Oxford University Press, 1963), 109-110.
[66] Sun Tzu, 110.
[67] Roy F. Nichols, book review, *The Victor and the Spoils: A Life of William L. Marcy*, by Ivor Debenham Spencer, *Pennsylvania Magazine of History and Biography* 84, no. 2 (April 1960), 244, https://journals.psu.edu/pmhb/article/view/41573/41294, accessed April 17, 2020.
[68] Schelling, 23.
[69] Office of the Director of National Intelligence, *Intelligence Community Directive 203: Analytic Standards* (Washington, DC, 2015).
[70] Joint Chiefs of Staff, *Joint Intelligence Preparation of the Operational Environment* (Washington, DC, 2014), xiv.
[71] Belt, 52.
[72] Randy Burkett, "An Alternative Framework for Agent Recruitment," *Studies in Intelligence* 57, no. 1 (Extracts, March 2013), 9-11.
[73] Burkett, 11-16.
[74] Burkett, 9-11; Goede and Boshuizen van Burken, 719.
[75] Roelien Goede and Christine Boshuizen van Burken, "A Critical Systems Thinking Approach to Empower Refugees Based on Maslow's Theory of Human Motivation," *Systems Research and Behavioral Science* 36 (2019), 719.
[76] Robert Z. George and James B. Bruce, eds., *Analyzing Intelligence: National Security Practitioners' Perspectives*, 2nd ed. (Washington, DC: Georgetown University, 2014), 242.

Jordan R. Beauregard is an intelligence analyst with the Defense Intelligence Agency, specializing in operational environment analysis and organizational change management. He earned the Master of Science of Strategic Intelligence degree from the National Intelligence University in 2020 and is a student in the Fleet Seminar Program at the Naval War College.

A Brief History of Cyber Intelligence: How Did Computer Data Evolve to Be Used for Intelligence Operations

by Gueorgui Dimitrov

OVERVIEW

The development of technology brought many possibilities, among which are to preserve and disseminate data. People today live in an interconnected world, where information—be it personal, administrative or even governmental—is now transferred and stored in cyberspace. This, in turn, means that we must find ways to secure such information from falling into the wrong hands. This article examines how the evolution of computer data enabled intelligence agencies to employ it within their operations. Looking at the evolutionary process through the years, the research findings of the article indicate that using computer data for intelligence practices has taken more than 50 years to develop. The beginning of this process can be traced back to the first computer prototypes used at the end of the Second World War and the early stages of the Cold War. This implies a significant effect on the Intelligence Community by connecting it with the rise of cyberspace throughout the years. By analyzing this connection, the article claims that the "cyber domain" originates from the evolutionary process of computer data. The concluding results indicate that the future of intelligence will increasingly rely on cyberspace to maintain a strategic and tactical advantage.

INTRODUCTION

The immense development in technology over the past decades is now extensively affecting our everyday life. In fact, this impact has been so colossal that many refer to it as an information revolution, at the forefront of which are information and communications technologies (ICT). Today, people have data creation and processing capabilities, which was unimaginable just 30 years ago. Along with that, networked connections worldwide have linked people to one another via the Internet, allowing them to create, access, keep, and share large volumes of data. This rapid technological spread has spawned an alarming expansion of cyber vulnerabilities that could be exploited. Even people who do not own a computer might be exposed to risk, underlining the evolution of computer data. There are constantly reported cases of some new "hack" into a corporate or sensitive government network that stole valuable information. Foreign cyber actors, such as "hacktivist" groups or even nation-states, might use stolen data to break into banking systems, power grids, or telecommunications infrastructure. This corresponds to the second part of Michael Warner's (2002) definition of intelligence being "a secret, state activity to understand or influence foreign entities."[1]

This article is going to show how states use computer data for intelligence operations. It will claim that this is not a new practice at all, but rather a process which has taken more than half a century to develop. This evolutionary process has had a tremendous effect on the Intelligence Community, broadly conceived. The article is going to provide indications that the evolution of computer data is one of the reasons behind the rise of cyberspace and the connection of billions of Internet Protocol (IP)-enabled devices, which necessitate that the future of intelligence will increasingly rely on cyberspace to maintain a strategic and tactical advantage. To provide effective evidence of computer data turning into means of cyber intelligence operations like espionage, this study is concentrated on the evolutionary process in six structured parts.

The first part is going to clarify the terminology used in the article. It will define and explain what is meant by phrases such as "computer data," "information," "cyber domain," "cyber warfare," etc. The second paragraph is going to lay out the foundations of the computer data evolutionary process throughout the years. It will demonstrate that using computer data for intelligence is not something new by providing evidence from the early years of computer development and the first cases of computer espionage, which sets the beginning of the computer data evolutionary process in relation to intelligence operations. The third section will examine the Cold War period in its digital aspects. It will look at the issue of computer data security throughout this conflict. The fourth section will focus on the rapid development of ICT after the Cold War and the interest of the military in weaponizing computer data. The fifth section will follow the evolution of computer data to contemporary times, which by now has expanded to the

extent of causing collateral damage. It will demonstrate the link between this evolutionary process and the rise of the cyber domain, as well as the excess of information it holds. The final section will speculate on the future of intelligence. It will provide theoretical assumptions about the future of the field, concluding that it is very likely intelligence will increasingly rely on cyberspace to maintain a critical and tactical advantage.

DEFINING TERMINOLOGY

This article uses terminology related to computer data, cyberspace, and intelligence, which may require further explanation. For example, the term "data" is broad enough to encompass both the digital and the single unit meaning of it. The *Oxford Dictionary* defines "data" as "any sequence of one or more symbols given meaning by specific act of interpretation."[2] It becomes clear by this definition that a single unit of data does not equate to information. In order for data to become information, it needs interpretation. Information is usually defined as single unit data + meaning and—according to the school of thought—is truthful (data + meaning). In other words, data is only the raw and unorganized bits of facts that need to be processed to become meaningful information. Computer or digital data is different than single unit data. By definition, it is information processed or stored by a computer.[3] This information may be in the form of text documents, images, audio clips, software programs, or other types of files. Computer data differentiates from single unit data because it is already processed by the computer's central processing unit (CPU), giving it the status of meaningful information. It is then stored in files and folders on the computer's hard disk, where people can access it. The single unit data definition may apply to computer data only in its unprocessed state, which is called the binary format. In this case, computer data is just a bunch of ones and zeros. All computer data is in binary format before it has been processed by a CPU. Because of this binary state, computer data can be easily created, processed, saved, and stored digitally. This also allows data to be transferred in a straightforward manner from one computer to another using a network connection or various media devices. It also does not deteriorate over time or lose quality after being used multiple times, as is the case of written paper data for instance.[4]

When it comes to terms like "cyber domain," "cyberspace," or "cyber warfare," they might be more familiar to readers, although they are quite recent. According to U.S. military doctrine, there are five recognized dimensions of warfare, namely: Land, Sea, Air, Space, and Cyber.[5] The last one is defined by the U.S. Department of Defense (DoD) as "a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[6] This definition is also shared by the North Atlantic Treaty Organization (NATO). Within such a warfare domain, military and intelligence forces must be able to defend and conduct operations. This effectively means that intelligence agencies can conduct operations exclusively within cyberspace with different purposes such as obtaining data/information or conspiring against an adversary. Such operations may fall under the category of "cyber warfare," which is considered the use of technology to attack a nation, causing comparable harm that leads to actual warfare.[7] There is significant debate among academics regarding the definition of cyber warfare, and whether it even exists. One view is that the term is a misnomer, since no offensive cyber actions to date could be described as having led to an actual war.[8] Nevertheless, all this terminology remains significant within the Intelligence Community, broadly conceived. Hence, it will be used in this study to help describe the evolution of computer data and how it became viable in intelligence operations.

EVOLUTIONARY PHASES OF COMPUTER DATA

Computer data has developed throughout the years following a coherent path, which can be characterized in four consecutive evolutionary phases: (a) sharing data; (b) protecting data; (c) weaponizing data; and (d) realization. The first one became known when computers began to share data between each other in the 1960s.[9] In order to make use of data stored in a 1960s computer, one had to either move to the site of another computer or have magnetic tapes storing that data sent by mail.[10] This possibility of sharing information through computers also meant that sensitive data could be accidentally or deliberately spilled, and therefore it had to be secured. The second phase was set in the 1970s when it became evident that foreign actors could attack computers and steal valuable data.[11] The third phase can be observed in the following decades (1980s-1990s), when primarily the U.S. military began to use computers, and the data they stored and shared, as weapons.[12] The final step of this evolutionary process was the realization and implementation of the previous three, which is happening in contemporary times.[13] Indeed, sensitive computer data could be compromised, which makes it a matter of national security. Each of these evolutionary phases reflects a precondition for setting new standards within the broader intelligence field, as practical evidence would verify in the following paragraphs.

The purpose of computer data in the intelligence field could be traced back even further, highlighting this article's argument that concern about cyber is not a recent phenomenon. Intelligence operations such as code-breaking or calculations associated with the delivery of ammunition were implemented by early versions of computers as far back as the Second World War. According to Sinclair McKay, the British code-breaking enterprise had more than 10,000 code-breakers using early similar versions of computers to decipher encrypted messages.[14] Later, a significant level of efficiency was achieved with the first programmable computers, Colossus Mark 1 and 2, resulting in an increasing volume of data merging with programmable analytic capacity. The application of computers expanded and became of critical importance in the 1950s. At the time, computers were mainly employed for processing scientific and mathematical data for defensive purposes, unlike newer versions designed for commercial purposes such as business and banking. For example, computers in the 1950s provided scientists with the tools to predict how different structures of nuclear weapons would perform.[15]

From the early years of the National Security Agency (NSA), for instance, the development of intelligence operations heavily relied on computers. Declassified documents published by the Agency[16] provide some understanding about the importance of improving digital computers to the evolutionary process of computer data. For instance, most of these devices were systems focused on cryptanalysis efforts, which is the decryption and analysis of codes, ciphers, or encrypted text. Accordingly, the development of computer systems that process data to facilitate intelligence analysis has been the ultimate goal.[17] One of the first such devices, which is more commonly associated with the roots of contemporary machine learning, was the Stochastic Neural-Analog Reinforcement Computer, or SNARC.[18] Marvin Minsky's research laid the foundation for multi-programmed computer systems that employed data analysis, thus fostering a combination of machine learning and pattern recognition into a single device.[19]

Both hardware and software industry companies like IBM followed this invention to meet the requirement for "parallel computation" established by SNARC. This allowed computers to run different tasks simultaneously with other users and, in theory, ensured that the computer would not allow one user to see data belonging to someone else. However, the work of Bernard Peters[20] later concluded that security cannot be completely guaranteed in a multi-programming computer system. This is because such systems allow features that decrease the degree of security, such as many programs running at the same time and many users interfering with these programs. Therefore, it is possible for any sensitive data stored in such systems to be compromised through human, hardware, or software vulnerabilities. According to William Ware,[21] the importance of these vulnerabilities depends on the level of data sensitivity, the class of users, the operating environment, and the network that has been designed. The systems might need to be secured against all these types of intrusion. As people with access to stored and shared computer data grew, the possibilities for malicious activity, such as espionage, increased exponentially.

The first recorded case of cyber espionage is West Germany's police action against an East German spy who tried to steal data from IBM's German headquarters in 1968.[22] This indicates that cyber intelligence is not solely a modern-day type of operation but has been around for at least a half century. Since the early 1960s, actors with different motives had found methods to compromise, corrupt, or even steal sensitive data, as will be laid out in the following paragraphs.

DIGITAL ASPECTS OF THE COLD WAR

As the first section mentioned, computer data security depended on physical control rather than hardware and software, leading to several innovations in the 1970s and 1980s. They focused on improving security by introducing tools such as administrator privileges, hashed passwords, and access rights to file systems. Perhaps the most important invention of this period was the encryption of data.[23] It originated from IBM and was eventually adopted as the Digital Encryption Standard, which is a symmetric-key algorithm for the encryption of digital data.[24] NSA implemented a slightly modified version of this encryption method. It highlighted the capability of the Agency to play a major role in government computer data security, as it was created to deal with communications intelligence in the first place.[25] It also shows how the evolutionary process of computer data had advanced toward the cyber domain, since the Agency was established to conduct communications intelligence and, due to this evolution, it began to deal with computer data. However, accusations emerged against NSA, claiming that its digital encryption standard was manipulated to install back doors, which would allow it to spy on U.S. citizens by decrypting their computer data. Allegedly, NSA established a way to crack a shared secret between two external parties that can be used for secret communications or exchanging data over a network. A special investigation initiated by the U.S. Senate found the claims unjustified, but the report is still an excellent example of how intelligence agencies become involved in computer data during this period.[26]

In the 1980s and 1990s, computer networks became commercial and publicly accessible. This massively increased the amount of data production, as well as the level of involvement of different actors. Consequently, new threats against, and vulnerabilities of, computer data emerged. It was clear that information systems were still vulnerable to both remote and insider intrusions. An appropriate example could be found in a 1979 article published by the U.S. Air Force. It demonstrated several methods for getting remote access to its systems, based on simulations that tested the security of its sensitive computer data.[27] The author remarks how easy it would be if an outsider wanted to penetrate actual military systems holding sensitive computer data. NSA used similar tests to put in practice the progressive idea of a single database that would allow intelligence analysts to access the collective data of the entire U.S. Intelligence Community. This notion of data sharing among different intelligence agencies predated the more recent calls to unite the Community and cease obstructing analysis. However, the tests failed to establish a single database, as Thomas Johnson later commented: "By the time the test attacks terminated, the penetration was so thorough that a penetrator at a distant remote terminal could have had actually seized control of the whole system. DIA never got its accreditation, and the results of the exercise made many at NSA skeptical that multilevel security could ever be achieved."[28] This indicates not only that data could be stolen, but it could also be manipulated to gain control over government systems. Thus, from that moment on, computer data integrity came to be a major aspect of the security problem during the Cold War.

With the spread of computer technology and the closing stages of the Cold War, people in general became more aware of how important sensitive data is. According to an article published by *The New York Times*, Donald Latham, a national security expert, remarked: "Some hackers spend 12 hours a day trying to break into computers at the CIA or the Pentagon. There will be more of these attacks, and we are going to have to deal with their increasing sophistication."[29] Although there was no publicly available evidence at the time that the Soviet Union had attempted cyber espionage, the reality of the situation was effectively very different. To prove this argument, a system administrator at Lawrence Berkeley Lab, who was investigating a financial incompatibility, discovered that a group of West German intruders had managed to get access to DoD networks as well as their contractors. It was later established that these "hackers" were funded by the KGB.[30] This shows how every aspect of governmental sensitive data was at risk of being compromised by adversaries. Hostile governments and non-state actors were indeed using digital vulnerabilities to collect data from the U.S. government, as well as from private corporations.

POST-COLD WAR INTELLIGENCE OPERATIONS

The idea that, in a conflict between states, one of the sides could penetrate the systems used by the opponent, steal its data, and disrupt its command and control systems was rapidly emerging in the military realm in the aftermath of the Cold War. Indeed, many computerized systems that stored valuable data represented a promising target. According to Thomas Reed, the Reagan administration had confirmed this statement by ordering certain modifications to computers ascribed to the Soviet Union that would allow it to collect data remotely.[31] These computers were delivered to the USSR by Canadian and British technical suppliers in the late 1980s. The Soviets claimed that one of these compromised computer systems allowed U.S. intelligence agencies not only to spy on it, but also caused a major explosion of a Siberian gas pipeline by manipulating data and disrupting the command and control process. There were public accusations against U.S. intelligence agencies claiming they had planted "units and viruses" that would collect data from computers acquired by the USSR and then make them completely non-functional in order to cover their tracks.[32] However, there are no sufficient publicly available sources to prove this claim; the truth remains unclear.

The rapid development of data has brought forth a new frontline—the cyber domain.

By this stage, the rapid development of ICT had allowed computer data to evolve to a degree where it was used not only for intelligence operations such as espionage but also in an offensive, covert action way, causing real physical damage to an adversary, such as in the alleged Siberian pipeline case. This has been recognized and employed by intelligence agencies, as well as the military. Perhaps the most evident example at the time of the military weaponizing data was Operation DESERT STORM. A report by Chairman of the Joint Chiefs of Staff Colin Powell suggested that this operation was indeed the first cyber warfare action that caused physical damage, since the main objective stated in this report was to "…decapitate the enemy's command and control structure from its body of combat forces."[33] This indicates the high level of importance that the evolution of computer data had at this point. Data had developed from a simple way of storing and sharing information to a weapon capable of espionage and even physical damage.

The evolution of computer data was evident not only in the United States. Foreign militaries also took notice, especially after the first Iraq War. Both the armed forces and the intelligence agencies of China and Russia were incapable of producing technology equivalent to Western standards.[34] They were practically forced to obtain American computer systems if they wanted to participate in the global information revolution. James Adams follows this process by examining the Russian side. He published several interviews with ex-Soviet officials who express a concern about their information infrastructure. An appropriate example could be a remark made by Vitali Tsygichko, who served as vice chair of the International Committee of the Federation Council of Russia: "Now we use all Western equipment for our infrastructure, from telephones to satellites. These systems come from Western firms, but nobody knows what programs might be hidden inside. Those companies will not give us the specifications."[35] Similar concerns emerged in China among military officials in the mid-1990s. The Chinese intelligence agency published several reports[36] on cyber operations led by the U.S., focusing on computer viruses that were able to destroy critical data of Iraq's air defense system during the Gulf War, concluding that China must not fall behind. Regardless of these concerns, the world was now adapting to a new kind of battlefield after the exhausting conflict of the Cold War. The rapid development of data has brought forth a new frontline—the cyber domain.

CONTEMPORARY STATE – CYBER INTELLIGENCE

Today, the evolutionary process of computer data is at a stage where it is of critical importance to national security. It can be safely argued that data can be manipulated by intelligence agencies for espionage or covert actions, potentially destroying digital and physical infrastructure as was shown by the Operation DESERT STORM example in the previous section. Computer security debates have been circulating around the safety and integrity of data and its transmission through networks. These networks became interconnected with the introduction of the Internet, which poses threats of its own. An appropriate example could be found in a report by the General Accounting Office [now the General Accountability Office] which warned the U.S. government about the problems troubling regular people on the Internet, such as identity theft and virtual intrusion. These malicious activities increasingly established themselves as threats to DoD's information systems as well. The report argued that DoD networks are attacked with the aim of being infiltrated over a million times a week, concluding that "…these attacks are a multimillion-dollar nuisance to Defense. At worst, they are a serious threat to national security. Attackers have seized control of entire Defense systems, many of which support critical functions, such as weapons research and development, logistics, and finance. Attackers have also stolen, modified, and destroyed data and software."[37] This strongly suggests that the rise of cyberspace could not occur without the evolution of data. Moreover, the recently recognized cyber domain could easily represent this evolutionary process by itself.

Turning computer data into a weapon could also describe this evolutionary process. Explosives and flammables, for instance, are recognized terrorist tools. However, in modern times the right data command delivered through a network to a critical infrastructure's command and control system could be more devastating than any terrorist attack. Furthermore, the person responsible would be even more difficult to track and identify. The swift expansion of computer-educated individuals around the world assures that there are going to be many more threats of this kind that could potentially endanger the national security of states. Martin Gill[38] notes that the Internet and its related functions are of increasing importance both within the Intelligence Community and the field of academic studies. He also argues that nobody could have predicted the dramatic impact that the expansion of the Internet would have on intelligence.[39]

Cisco estimated that between 2008 and 2009 the Internet of Things (IoT) for the first time exceeded the number of human beings on the planet.

According to statistics from Internetlivestats.com,[40] in 2009 there were an estimated 1.77 billion people online. By the end of 2016 this number had nearly doubled to more than 3.5 billion and at the time this article was drafted there were exactly 4,185,134,492 people using the World Wide Web. Yet, what is even more remarkable is not the number of users going online, but rather the increase in the number of Internet-enabled devices that received IP addresses. Cisco estimated that between 2008 and 2009 the Internet of Things (IoT) for the first time exceeded the number of human beings on the planet.[41] This massive expansion of Internet users and devices would significantly amplify the quantity of data being produced and distributed around the world. On the one hand, this poses an opportunity for intelligence agencies to collect more data from different sources, which would benefit their reports and therefore would help policymakers make more informed decisions. On the other, it presents a new kind of challenge that requires dealing with the immense

amounts of data and information being generated. Margaret McDonald and Anthony Oettinger address this particular challenge in their work, stating that "the intelligence community no longer suffers from information scarcity but from information overload."[42] David Donohue and Peter Murphy also recognize that information overload is a significant problem for intelligence analysts.[43] The common recognition by so many academics on this issue indicates that it is of major importance. Indeed, every form of digital intelligence from SIGINT, MASINT, and IMINT or GEOINT, including the emerging fields of CYBINT and SOCINT, is expanding at exponential rates. The usable to unusable ratio within data is very low, and therefore vast collection of information makes quality analysis very difficult but crucial for protecting digital infrastructure and national security overall.

THE FUTURE OF INTELLIGENCE WITHIN THE CYBER DOMAIN

When theorizing about the future of intelligence, it would be unreasonable to overlook the issue raised in the previous section, i.e., the extensive amounts of data being generated. According to Aaron Brantly, the current state of data generation is only a small fraction of the data that will be generated in the coming decades.[44] Consequently, the capacity of doing real-time intelligence analysis of large data might be inefficient, as the data generated continues to increase at a geometrical rate overall.

This issue is likely to change in the near future due to the introduction of new technologies, such as advanced machine learning and artificial intelligence (AI). Lu Liu, Richard Hill, and John Panneerselvam[45] support this assumption, arguing that agencies will face an increasing variety, volume, and velocity of data, which will leave them to struggle in focusing on the perspective. Regardless of their structured analytical techniques and other reliable methods, intelligence analysts will become progressively dependent on technologies to assist with scrutiny of the increasing volume of computer data. This validates the problem of data overload that intelligence analysts will most likely face in the future. It might also bring other issues to the surface, such as lack of information accuracy or privacy and civil liberties concerns, resulting in an increasing number of civil-military confrontations. Such problems suggest the necessity of maintaining a critical and tactical advantage in cyberspace. Although various factors might introduce substantial data challenges, such as the aforementioned data overload or securing this "big data," the capability to automate the collection of information into robust data servers is likely to improve in the coming decades. Since the Internet and its related technologies continue to grow, data collection will increase in all associated areas. In addition, massive data accessibility is an advantage that is likely to be a powerful driver of intelligence analysis. Indeed, the use of computer data is already recognized as an important tool that helps intelligence analysts, but in the future it might be even more important because of the increasing role that computers play in general. One way to deal with the increasing overload of data is machine learning, which refers to the automated detection of meaningful patterns in data.[46] In such cases, both human and computer analysis must be focused on making accurate predictions in the different stages of the intelligence cycle. However, analysis of data collected and processed by an underdeveloped machine learning system is likely to produce low-quality reports which might damage national security by misinforming policymakers. In order to facilitate quality intelligence analysis, the machine learning algorithm must sustain its learning structures and consider numerous possible pitfalls in a similar way that structured analytic techniques serve intelligence analysts. Joseph Gartin[47] acknowledges the role of machine learning and AI in the future of intelligence analysis by providing an example of techniques like facial and voice recognition that use algorithms to identify the same person in multiple but seemingly unrelated images and videos.

As more and more systems are automated on an artificial intelligence level, becoming increasingly "smarter" every day, they will require guardians entrusted with ensuring that values, ethics, laws, and policies are followed.

Nevertheless, with the growing incorporation of machine learning, evading biases in algorithms will become more and more significant. Algorithms that are written on a biased basis would most likely produce inaccurate analysis. A skilled human analyst can distinguish biases, but underdeveloped automated learning algorithms hardly possess this corrective adjustment, which might lead to vital errors. Usually such errors arise unintentionally during the training session of machine learning systems due to incorrect data input. Alternatively, they can occur during a later stage of the utilization process within a specific algorithm as data structures could be changed. With the advancement of machine learning systems, data is gradually being computer-processed before being provided to analysts.[48] Therefore, it is very important for analysts today and in the future to have extensive knowledge of machine learning and algorithm functions.

To comply with these sets of rules in an evolving data collection world, the automated systems gathering and analyzing computer data through machine learning must be constructed to avoid unauthorized collection and analysis. In such cases, contemporary law and policy provide little help in efficiently solving the legal and ethical issues concerning the evolution of computer data in terms of what should and should not be collected and analyzed. As more and more systems are automated on an artificial intelligence level, becoming increasingly "smarter" every day, they will require guardians entrusted with ensuring that values, ethics, laws, and policies are followed.[49]

These theoretical assumptions raise many issues. First, there is the problem with disruptive changes in analytical sources and methods and the ways the Intelligence Community has dealt with them in the past. Second, there is the role of analysts in a world of ubiquitous information of enormous scale, velocity, and complexity. Also, the intelligence of the future will reflect 50 or 100 billion devices all feeding back information to be analyzed, creating an overload. Ensuring analytical integrity while increasing efficiency will surely be a challenge. Laws and policies not matching the reality of an increasingly connected world may introduce another set of problems, such as constraints imposed by laws and policies that hamper the incorporation of the variety and volume of new sources. All these problems are being analyzed by experts in the field, but the collective evident factor is that intelligence is at the dawn of a new epoch. A digital era in which everything from computers and systems to refrigerators and coffeemakers can produce data that can be collected, analyzed, and used for intelligence purposes. This variety of sources, which is about to form an all-source cyber intelligence community, should not occur in the absence of theory and oversight by existing expert practitioners.

CONCLUSION

Computer data technology is undeniably a significant aspect that can impose essential changes and provide convenient tools to improve intelligence practices. This article has examined the evolutionary process of computer data, establishing its relationship to the Intelligence Community. There is a common misperception present that using computer data for intelligence services is a new practice. Given the analyzed examples, however, extensive evidence suggests that computers were capable of intelligence functions before the Cold War. Other examples showed how computer data became of vital importance for the national security of states. The nature of threats endured a significant adjustment accordingly, ever since the issue of computer data security emerged. The rapid development of technology characterized another aspect of computer data evolution. Both the intelligence and military communities used it as a weapon for their operations. The contemporary stages of this evolutionary process allowed offensive intelligence practices to create a new battlefield within cyberspace, where states are able to attack each other in a way that has not been seen before, thus introducing "cyber warfare." We are entering a phase in which threats are emerging constantly and shifting toward causing damage greater than imagined.

Digital espionage, missions to damage critical infrastructure, and targeted attacks in relation to states are among the issues that have emerged within the cyber domain, and national security agencies must find an efficient way to prevent them. Excessive amounts of data need to be handled effectively, hence relying on automation. We must establish adequate security solutions to identify threats more rapidly than before and block possible attacks. It is uncertain what the future holds, but one can assume that the evolutionary process of computer data will follow the rapid development of technologies, making it very likely that intelligence operations will have to rely on these digital innovations to maintain a critical and tactical advantage.

NOTES

[1] Michael Warner, "Wanted: A Definition of 'Intelligence'," *Studies in Intelligence* 46, no. 3 (2002): 18-22.
[2] Data Noun – Definition, Pictures, Pronunciation and Usage Notes, *Oxford Advanced Learner's Dictionary*, 2020, at Oxfordlearnersdictionaries.com, 2020, https://www.oxfordlearnersdictionaries.com/definition/english/data?q=data.
[3] Per Christensson, "Data Definition," *TechTerms*, 2006, https://techterms.com/definition/data.
[4] Ibid.
[5] Glenn Alexander Crowther, "The Cyber Domain," *Cyber Defense Review* 2, no. 3 (2017): 63-78.
[6] United States, Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms* (Washington DC: Staff Report, 2020).
[7] Peter Collier and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014).
[8] James A. Green, *Cyber Warfare: A Multidisciplinary Analysis* (London: Routledge, Taylor & Francis Group, 2016).
[9] Michael Warner, "Cybersecurity: A Pre-History," *Intelligence and National Security* 27, no. 5 (2012): 781-799.
[10] Leonard Kleinrock, *Communication Nets: Stochastic Message Flow* (New York: McGraw-Hill, 1964).
[11] Michael Warner, "Cybersecurity: A Pre-History," *Intelligence and National Security* 27, no. 5 (2012): 781-799.
[12] Ibid.
[13] Ibid.

[14] Sinclair McKay, *The Secret Lives of Codebreakers* (New York: Penguin Group, 2012).
[15] Richard Rhodes, *The Making of the Atomic Bomb* (London: Simon & Schuster, 2012).
[16] National Security Agency, *It Wasn't All Magic: The Early Struggle to Automate Cryptanalysis, 1930s-1960s* (Fort Meade, MD: Center for Cryptologic History, 2003); National Security Agency, *Before Super-Computers: NSA And Computer Development* (Fort Meade, MD: Center for Cryptologic History, 2003).
[17] Ibid.
[18] Marvin Minsky, "Steps Toward Artificial Intelligence," *Proceedings of the IRE* 49, no. 1 (1961): 8-23.
[19] Ibid.
[20] Bernard Peters, "Security Considerations in a Multi-Programmed Computer System," *Proceedings of the April 18-20, 1967, Spring Joint Computer Conference –AFIPS '67 (Spring)* 30, no. 3 (1967): 283-286.
[21] William Ware, "Security and Privacy In Computer Systems," RAND Corporation, 1967, https://www.rand.org/pubs/papers/P3544.html.
[22] Alle Rechte, "SPIONAGE/COMPUTER: EDV Abgezapft – DER SPIEGEL 16/1969," 1969, https://www.spiegel.de/spiegel/print/d-45702341.html.
[23] Michael Warner, "Cybersecurity: A Pre-History," *Intelligence and National Security* 27, no. 5 (2012): 781-799.
[24] Whitfield Diffie and Martin E. Hellman, "Special Feature: Exhaustive Cryptanalysis of the NBS Data Encryption Standard," *Computer* 10, no.6 (1977): 74-84.
[25] Thomas L. Burns, "The Origins of the National Security Agency," *United States Cryptologic History* 5, no.1 (1990): 107-108.
[26] United States Senate, *Unclassified Summary: Involvement of NSA in the Development of the Data Encryption Standard* (Washington, DC: Staff Report, 1978).
[27] Roger R. Schell, "Computer Security: The Achilles Heel of the Electronic Air Force," *Air University Review* 30, no. 2 (1979): 160-168.
[28] Thomas R. Johnson, *American Cryptology During the Cold War, 1945-1989*, Book IV: *Cryptologic Rebirth*, 4th ed. (Fort Meade, MD: Center for Cryptologic History, 1999).
[29] William J. Broad, "Computer Security Worries Military Experts," *Nytimes.Com*, 1983, https://www.nytimes.com/1983/09/25/us/computer-security-worries-military-experts.html.
[30] Clifford Stoll, *The Cuckoo's Egg* (New York: Pocket Books, 2005).
[31] Thomas Reed, *At the Abyss* (New York: Ballantine Books, 2005).
[32] Nikolai Brusnitsin, *Openness and Espionage* (Moscow: Military Publishing House, USSR Ministry of Defence, 1990).
[33] Michael Warner, "Cybersecurity: A Pre-History," *Intelligence and National Security* 27, no. 5 (2012): 790.
[34] Jurgen Ruland, Theodor Hanf, and Eva Manske, *U.S. Foreign Policy Toward the Third World: A Post-Cold War Assessment* (New York: Routledge, 2006).
[35] James Adams, *The Next World War* (New York: Simon & Schuster, 1998).
[36] Wang Pufeng, "The Challenge of Information Warfare," Federation of American Scientists, 1995, https://fas.org/irp/world/china/docs/iw_mg_wang.htm.
[37] U.S. Congress, General Accounting Office, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks* (Washington, DC: Technical Report GAO/AMID-96-84, 1996), https://fas.org/irp/gao/aim96084.html.
[38] Martin Gill, *The Handbook of Security*, 2nd ed. (London: Palgrave Macmillan, 2014).
[39] Ibid.
[40] https://www.internetlivestats.com/, 2020.
[41] Dave Evans, "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything," *Cisco Internet Business Solutions Group (IBSG)* 3, no. 12 (2016): 3-6, https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.
[42] Margaret S. MacDonald and Anthony G. Oettinger, "Information Overload: Managing Intelligence Technologies," *Harvard International Review* 24, no. 3 (2002): 44; Alan Dupont, "Intelligence for the Twenty-First Century," *Intelligence and National Security* 18, no. 4 (2003): 15-39.
[43] David P. Donohue and Peter M. Murphy, "Supporting Competitive Intelligence at DuPont by Controlling Information Overload and Cutting Through the Noise," *Journal of Information & Knowledge Management* 33, no. 1 (2016): 165.
[44] Aaron F. Brantly, "When Everything Becomes Intelligence: Machine Learning and the Connected World," *Intelligence and National Security* 33, no. 4 (2018): 562-573.
[45] Lu Liu, Richard Hill, and John Panneerselvam, in *Application of Big Data for National Security*, 1st ed. (Oxford, UK: Butterworth-Heinemann, 2015), 3-14.
[46] Shai Shalev-Shwartz and Shai Ben-David, *Understanding Machine Learning* (New York: Cambridge University Press, 2016).
[47]Joseph Gartin, "The Future of Analysis," *Studies in Intelligence* 63, no. 2 (2019): 3-4.
[48] Michael Warner, "Cybersecurity: A Pre-History," *Intelligence and National Security* 27, no. 5 (2012): 790.
[49] Amitai Etzioni and Oren Etzioni, "Designing AI Systems that Obey Our Laws and Values," *Communications of the ACM* 59, no. 9 (2016): 29-31.

Gueorgui Dimitrov, who hails from Sofia, Bulgaria, is a student in the International Master in Security, Intelligence, and Strategic Studies (IMSISS) program at Dublin City University. He obtained his BA in History and Politics from Coventry University in the UK. His research interests include cybersecurity, cyber intelligence, and data analytics. He has interned for several non-profit organizations and worked for a couple of online gambling companies as an analyst, positions that have dealt with cyber fraud and data theft. He is interested in how states use computer data that ordinary people produce, which has led his research into the related fields of military and civil intelligence.

A New Hub for American Climate Security: Strengthening the Intelligence Community's Role in Meeting the Threat of Climate Change

by Diego H. Nuñez

EXECUTIVE SUMMARY

The intersection of national security policy and climate change has undergone a rapid transformation during the Trump administration. Even as the President has taken great care to remove the U.S. from headline initiatives like the COP 21 Paris Climate Agreement and the Obama administration's Clean Power Plan, the national security community has steadily maintained its focus on mitigating the effects of anthropogenic climate change in several successive iterations of the National Defense Authorization Act. This article investigates the possibilities available to the recently created Climate Security Advisory Council slated to be housed in the Office of Director of National Intelligence, and makes the case that the Council should look to the nascent set of climate risk models being developed by the private sector to gain a holistic understanding of the realities it faces.

INTRODUCTION

In her opening statement during the February 13, 2020, hearing of the Senate Democrats' Select Committee on "Understanding and Combating the Security Risks of Climate Change," Senator Tammy Duckworth (D-IL), a former lieutenant colonel in the U.S. Army, laid out the following paradox:

> [T]he Department of Defense has long acknowledged that climate change poses a grave risk to our military readiness and global stability. Yet a report by the Army War College [has stated], "the Department of Defense is precariously unprepared for the national security implications of climate change induced global security challenges." They further observe that "DoD must now promulgate a culture of environmental stewardship across the force. Lagging behind public and political demands for energy efficiency and minimal environmental footprint will significantly hamstring the department's efforts to face national security challenges."[1]

After recounting how damage to Camp Lejeune and other Marine Corps installations in North Carolina from the 2018 hurricane season are estimated to have cost $3.6 billion, and how estimates of the repair of Tyndall Air Force Base in Florida devastated by Hurricane Michael that same year are projected to cost $5 billion over five years, Duckworth forcefully emphasized the loss of training and readiness of the force in quoting a letter from the Commandant of the Marine Corps, who concluded that as a result of the storms in 2018 "one-third of the entire combat power of the Marine Corps has been degraded and will continue to degrade."

Senator Duckworth's example is bolstered by an earlier House Intelligence Committee hearing from June 2019, in which committee chairman Rep. Adam Schiff (D-CA) similarly identified climate change as the greatest long-term national security threat to the United States, "which will affect every dimension of our national life for decades and possibly centuries."[2] The recognition that the security implications of climate change pose grave risks to American security are nothing new. Although discussions about climate security have been ongoing in the Intelligence Community for decades, the issue is increasingly seen as a bipartisan issue whose profile in public venues like Congressional hearings and legislative proposals has risen substantially since the 2018 mid-term elections.[3] Despite the periodic ebb and flow of political influence in dictating climate policy to the broader federal government—and especially the executive branch—the Department of Defense (DoD) has developed a firm grasp of the threat climate change poses to U.S. national security interests and shows no signs of letting go. This article looks at the intersection of national security policy and climate change through the lens of a specific provision in the 2020 National Defense Authorization Act (NDAA), which mandates the creation of a Climate Security Advisory Council within the Office of the Director of National Intelligence (ODNI). I argue that one of the most powerful functions the new council could serve is as a coordinating body for the U.S. whole-of-government approach to quantifying and disclosing climate risk, and that ODNI has an opportunity to integrate existing private sector knowledge to make this happen.

Section 5321 of the NDAA states that the Director of National Intelligence shall establish a Climate Security Advisory Council for the purpose of assisting intelligence analysts with respect to analysis of climate security, facilitating coordination among the elements of the Intelligence Community (IC) and the federal government, and ensuring that the IC is adequately prioritizing climate change in carrying out its activities. The law further directs DoD to develop tools for measuring risks associated with climate change and extreme weather. Coming as it does in the third year of the Trump administration, it is at first glance surprising that such a body was able to win Congressional approval, but a look at climate provisions in the previous few NDAAs shows it to be part of a broader pattern: provisions from the 2018 NDAA, passed shortly after Hurricane Harvey hit Houston, Texas, prohibited military construction inside so-called "100-year floodplains," and a requirement for the 2019 defense spending bill ordered DoD to provide a report ranking the military installations most vulnerable to climate change.

This article also attempts to move the discourse around climate security past the foundational idea of climate change as a "threat multiplier" that was formulated in a groundbreaking 2007 report by the think tank CNA.[4] Per CNA's analysis, those governments that are already unable to provide basic needs like food, water, shelter, and stability to their populace face grave dangers from climate change because of the likelihood that the effects of the buildup of global greenhouse gas emissions might exacerbate governance problems which could lead to greater internal conflict, extremism, and other negative outcomes.[5] In attempting to develop a more dynamic conceptual framework for climate security, this article makes the case that a look at private sector risk models might be a useful corrective because these models offer a quantitative element sorely lacking from the threat multiplier formulation. Their ability to price some of these risks transparently has snowballed into recent legislative proposals such as Senator Elizabeth Warren's (D-MA) Climate Risk Disclosure Act, which would empower climate regulators and the Securities and Exchange Commission (SEC) to issue rules for every public company to disclose its direct and indirect greenhouse gas emissions, the total amount of fossil fuel-related assets it owns or manages, how its valuations would be affected if climate change continues at its current pace or if policymakers successfully restrict greenhouse gas emissions to meet the 1.5 degrees Celsius goal, and its risk management strategies related to both physical and transition risks (both defined below) posed by the climate crisis.[6]

In addition to customizing disclosure requirements for different industries, the SEC would also subject energy companies exploring and drilling for new hydrocarbons to further oversight. This is far closer to being a reality than is commonly thought; financial regulators and central banks have been carrying out climate-related stress tests since 2017,[7] and last year the Bank of England introduced a framework for its own climate-related stress tests.[8] Given the diversity of companies that have to pay taxes to the federal government, climate-related financial disclosures and associated accounting standards will need to aim for a universal transferability across the entire economy in order to ensure that risk is accurately modeled across not just each individual company but within each asset held by those companies. One could easily envision the same process being carried out across DoD, which is the world's largest institutional user of petroleum and single largest producer of greenhouse gases in the world,[9] and indeed across the entire federal government.

This article also turns to the 2020 NDAA for the definition of "climate security" it provides: "the effects of climate change on the national security of the United States, including national security infrastructure, subnational, national, and regional political stability, the security of allies and partners of the United States, and ongoing or potential political violence, including unrest, rioting, guerrilla warfare, insurgency, terrorism, rebellion, revolution, civil war, and interstate war."[10] Another concept central to the treatment of climate risks in the private sector models discussed here is the distinction between *physical risks*—the costs associated with damage from increasingly severe weather events and cumulative deterioration—and the costs associated with *transition risk*—the adjustments that will necessarily be embedded in getting to a lower-carbon economy. To the extent that risk assessment is a core element of defense planners, the IC can take advantage of significant public-private transferability in this distinction and related methodologies because each asset that an individual entity or organization owns bears physical risk with the physical structures or vehicles that it maintains. A key part of my argument in this article is that the IC and the Pentagon more broadly need to be thinking about the most efficient way to quantify and disclose their risk—if not publicly then at least internally for the purposes of optimally efficient resource allocation. Just as in the private sector, risk exposure that is not understood by regulators and that is not measured through widely disseminated examination practices opens up a glaring blind spot to DoD's ability to understand the nature and scope of the risks it faces.

Fundamental to understanding how the Pentagon models climate risk is its adherence to the scenarios drawn up by the United Nations' Intergovernmental Panel on Climate Change (IPCC). The IPCC has developed a number of plausible future atmospheric greenhouse gas concentrations whose labeling is based on each scenario's projected effect in the year 2100. Known as "Representative Concentration Pathways" (RCPs), these projections are commonly used to

illustrate the drastic variability of future global climate scenarios dependent on the speed and thoroughness of collective action to reduce greenhouse gases in the atmosphere. RCP labels correspond to the amount of heat in the atmosphere and illustrate the difference between sunlight absorbed by the earth and energy radiated back to space in each scenario. At the highest end of the IPCC's most recent assessment, RCP 8.5 serves as the hottest commonly modeled scenario and represents a continuation of recent global emissions growth rates with atmospheric concentrations of carbon dioxide reaching 940 parts per million (ppm) by the year 2100.

While rapid economic growth absent any global action to reduce emissions could lead to a situation higher than RCP 8.5, it is not commonly modeled. Instead, the next commonly modeled scenarios are RCP 6.0 and RCP 4.5, which would represent a gradual shift away from fossil fuels and/or a modest slowdown in global economic growth. Under RCP 6.0, CO2 concentrations stabilize in the middle of the 22nd century around 750 ppm and in RCP 4.5 CO2 concentrations will stabilize to around 550 ppm by the end of the 21st century. At the bottom end, RCP 2.6 would see atmospheric CO2 concentrations remain below 450 ppm, but would only be achievable if the world were to carefully orchestrate an aggressive reduction in global emissions and achieve an overall drawdown in greenhouse gases out of the atmosphere by the end of this century.

SECURITIZATION, CONFLICT-CLIMATE LINKAGES, AND THE TRANSFERABILITY QUESTION

A long-running debate has transpired about the connection between changes in the earth's climate and human conflict. While some conflict researchers' efforts are decried as being overly reliant on backward-looking data and overly influenced by the field of civil conflict studies, out of which environmental conflict studies emerged, others continue to forge ahead in their pursuit of the right mix of explanatory variables.[11] A recent expert elicitation analysis in the journal Nature identified four drivers as being particularly influential to date for conflict risk, but these variables could well apply outside a climate-driven conflict setting. They include low socioeconomic development, low governance capabilities, intergroup inequality, and a recent history of violent conflict.[12] To make matters more confusing, the study found significant uncertainty for how highly these variables ought to be weighted and it ranked climate variability low on the list of secondarily influential conflict drivers, although the study's participants all agreed that climate change would amplify conflict risks in the future. While lack of a direct relationship between security concerns and climate change in the literature means that persistent questions about the utility of the concept of climate security will remain, a trove of intelligence reports and worldwide threat assessments suggests that, even barring a relationship that is statistically significant, a great number of decision-makers still subscribe to the climate security framing.[13] In a 2018 House Armed Services Committee hearing, retired Rear Admiral David Titley emphasized this point when he asserted, "Climate change is a readiness issue. It is not a partisan or political issue or a desire to appear green."[14]

A long-running debate has transpired about the connection between changes in the earth's climate and human conflict.

Equally fraught for the purposes of this analysis is the utility of transferring risk management principles from the private sector to the work of the national security community. However, in testimony for the Senate Democrats' Climate Crisis Committee's hearing on the "Economic Risks of Climate Change" held on March 12, 2020, the Chairman of the Commodity Futures Trading Commission's Climate Risk Working Group, Bob Litterman, laid out a set of fundamental principles of risk management that security analysts would be foolish not to consider: first, that risk management should be guided by a set of "extreme, but plausible" worst- case scenarios; second, that the purpose of risk management is not to minimize risk, but rather to recognize risks and to warn when they are not being priced appropriately; third, that given enough time virtually any problem can be addressed; and fourth, that the relationship between risk and uncertainty is not always one-to-one and that, even if quantitative models can give us measures of risk, what is ultimately of more concern is uncertainty.[15] Litterman closes his testimony by noting how badly investors want to be able to price climate risks into their investments.

Another witness from the same hearing, Sovereign Wealth Fund Research Initiative founder Frédéric Samama, explained how "central banks now recognize that climate change threatens financial stability [and that to] preserve financial stability. . .two steps are needed."[16] First, traditional backward-looking risk models need to be updated to capture future risks, including scenario analysis or climate stress tests. Second, central banks (and presumably other regulators depending on the country's financial system) must play an additional role by helping to coordinate the measures to fight climate change. Proper calibration of climate risk is not just some altruistic undertaking done to save the planet, but a judicious way to save assets from ruin. For the purposes of the analysis in this article, pricing in

climate risk to every asset under DoD ownership is thus a clear analogue to carbon pricing in the financial system. There are signs that DoD is already heading in this direction: just as climate-related stress tests of insurance companies and financial institutions have proliferated in the last few years, so have the Pentagon's vulnerability analyses of individual installations across the world discussed in detail below. Unfortunately, the Federal Reserve Board is not stepping up to the plate as are regulators like the Bank of England, the European Central Bank, and many others.

...in 2016 the U.S. National Intelligence Council identified various pathways through which climate change would challenge national security interests including threats to the stability of countries, heightened social and political tensions, adverse effects on food prices and availability, increased risks to human health, negative impacts on investments and economic competitiveness, as well as potential climate discontinuities and related second- and third-order effects.

In place of a governmental authority like the Federal Reserve developing a regulatory environment for climate disclosures, a number of private companies and nonprofit organizations such as the Sustainability Accounting Standards Board (SASB) and the Task Force on Climate-Related Financial Disclosures (TCFD) have stepped up in the past decade to push this process along. The TCFD was established to help companies better understand what financial markets need from disclosures in order to measure and manage climate risks, and the SASB was established to develop sustainability accounting standards across a number of industry-specific measurements. Among the sustainable accounting frameworks that have emerged, those developed by the SASB and TCFD are understood to be two of the most complementary and readily adoptable available.[17] From a defense management perspective, because the Pentagon's operations are sprawling and extend into so many divergent avenues from housing and infrastructure to transportation and healthcare for millions of employees and dependents, TCFD and SASB standards offer an ideal framework to help DoD quantify climate risk for the wide variety of business activities and emissions cases without having to invent a totally new framework on its own.

Apart from harmonizing accounting standards, a number of private research and corporate intelligence firms have been busy developing climate risk models that seek to deliver ever more granular data predictions to their clients. Often using the most cutting-edge machine learning technologies to perform predictive analysis on physical risk, these models have the potential to change perhaps the biggest problem in the climate-conflict research project: the oft-lamented historical bias in how climate change and conflict are related. One notable partnership furthering this conversation is the Rhodium Group's work with the asset management firm BlackRock alongside academic institutions such as the University of California, Berkeley, the Energy Policy Institute at the University of Chicago (EPIC), and Rutgers University to develop proprietary models under the auspices of the Climate Impact Lab at RCP 2.6, RCP 4.5, RCP 6.0, and RCP 8.5. Rhodium's recent report cites recent advances in econometric research, data processing, and scalable cloud computing as making its asset-level accounting of physical climate risk across assets like municipal bonds, commercial real estate, and electrical utilities possible for the first time in line with TCFD guidance.[18]

EXISTING DEFENSE DEPARTMENT VULNERABILITY RISK INDICES

Turning once again to the work of the Department of Defense and the specific role of the Intelligence Community, in 2016 the U.S. National Intelligence Council identified various pathways through which climate change would challenge national security interests including threats to the stability of countries, heightened social and political tensions, adverse effects on food prices and availability, increased risks to human health, negative impacts on investments and economic competitiveness, as well as potential climate discontinuities and related second- and third-order effects. Even as the debate about the linkages between violent conflict and climate change continue unabated, there are a number of other elements of the climate security discussion to which climate risk modeling has the potential to contribute—the most concrete of which from DoD's perspective is the resilience of U.S. military installations and assets.

Late in the Obama administration, after the release of DoD's 2014 Climate Change Adaptation Roadmap and its 2015 review of climate risks to the combatant commands, Congressional leaders voted to commission a full-scale assessment of the threat posed to U.S. military bases globally that would require the Pentagon to survey all foreign and domestic installations. The Department's researchers evaluated over 3,500 installations over a projected 20-year time frame across five major risks: recurrent flooding, drought, desertification, wildfires, and thawing permafrost. A *Washington Post* story released during the assessment's drafting process revealed that officials removed dozens of references to climate change in early drafts, which raised the profile of the study even as the

assessment had not yet been officially released.[19] The results took nearly three years to materialize and an interim report was released in 2018 which showed that over half of these installations were exposed to at least one impact and many were subject to multiple climate risks. Drought was projected to be a recurrent feature at 22 percent of all bases (782 facilities in all), while impacts from strong winds were expected to affect 763 installations. Though only 210 facilities were seen as likely to suffer from recurrent wildfires, over 700 were in danger of severe flooding.[20]

The results of the initial study led to the desire for a follow-on report authorized into law by the 2018 NDAA, and when that subsequent document focusing on what DoD identified as the highest priority installations domestically was released early in 2019, the newly elected Democratic leadership was incensed by the report's omission of several pieces of information that had been required by law. Highlighting the fact that the 20-year projection window again used in this report was quite narrow for the purposes of military planners, the report's conclusion remarked that about two-thirds of the 79 installations addressed in the report were vulnerable to current or future recurrent flooding, more than one-half were vulnerable to current or future drought, and about one-half were vulnerable to wildfires.[21] For contingency purposes, the report discussed only domestic installations; hence, the extent of climate vulnerabilities for foreign bases is not publicly known, but in Senate Armed Services Committee testimony from April 2019, then-Secretary of the Army Mark Esper was asked to rank the ten Army bases most vulnerable to climate risks, as the other service heads were queried later that year. While Secretary Esper of the Army and the Secretary of the Air Force complied, the Secretary of the Navy, overseeing both the Navy and the Marine Corps, opted to disclose their respective lists without ranking installations in any particular order.[22]

In both public statements and Congressional testimony, the Pentagon openly identifies two agencies as spearheading the work of evaluating climate impacts on DoD: the Strategic Environmental Research and Development Program (SERDP) and the Environmental Security Technology Certification Program (ESTCP), which frequently act in tandem and form interagency research programs with the Environmental Protection Agency and the Department of Energy. While these offices both maintain robust research programs on resource conservation, installation energy and water programs, environmental restoration, and cleanup of sites contaminated with pollutants and other hazardous chemicals, they also convene partnerships and collaborations with academia, industry, the military services, and other federal agencies to invest in research focused on improving DoD understanding of environmental risks to installations and missions from climate change. Especially in the latter half of the Obama administration, installation vulnerability assessments fell under the SERDP/ESTCP's purview and their joint infrastructure resiliency program area, which maintains a suite of region-specific tools and models to better predict climate change impacts.

In a publicly available SERDP and ESTCP presentation of April 2016 titled "Use of Climate Information for Decision-Making and Impact Research," a team of five researchers presented its methodology of using input variables such as temperature, precipitation, sea level, and frequency or intensity of extreme events in evaluating decision around infrastructure design and maintenance, emergency response management, and long-term investment and planning. The team further specified two approaches to scaling the overarching climate models known as a general circulation model (GCM) into actionable insights at impact-relevant scales: dynamic downscaling and statistical downscaling. While dynamic downscaling draws more information from higher-resolution climate modeling, statistical downscaling incorporates more information from historical data sets and station-specific observations, which unfortunately often limits them to temperature and precipitation variables only. While dynamic models are computationally expensive and require additional bias correction from a statistical perspective, they have the added benefit of being able to fill in gaps in observed data and do not need to assume that variable measurements are being made from a stationary observation point.[23]

In a separate, publicly available presentation of October 2016 titled "DoD Decision Making and Climate Change," Richard Moss of Pacific Northwest National Laboratory and Casey Brown of the University of Massachusetts, Amherst, laid out principles of vulnerability assessments and resilience planning for DoD's Decision Framework Climate Risk Assessment and Adaptation Planning, and used the case study of four military installations in the Mid-Atlantic region to illustrate how these assessments are carried out. In conjunction with the IPCC's assessments and the federal government's Climate Resilience Toolkit, the model documentation they shared identified a climate model developed by the Argonne National Laboratory known as GATOR (Geospatial Analysis Tool Kit for Regional Climate Datasets), which used historical data from 1995-2004 to look forward toward RCP 4.5 and RCP 8.5 projections across the time periods 2045-2054 and 2085-2094 (respectively), taking into account the following variables on a daily basis: precipitation, solar radiation, maximum temperature, minimum temperature, and wind speed.[24] GATOR itself was developed in the wake of the following six General Circulation Model tests: two iterations of the Community Climate System Model Version 4 (Uncorrected and Bias Corrected), two iterations of the Geophysical Fluid Dynamics Laboratory Earth System Model Version 2G (With and Without

Nudging), the Hadley Global Environment Model 2 – Earth System, and the National Centers for Environmental Predictions – Department of Energy, Reanalysis 2. After the model has had a chance to run, the analysts conducting the vulnerability study assess how individual missions might be affected given the consequences of potential impacts in conjunction with the expert judgment of site/asset managers.[25] The presentation further articulates how the SERDP and ESTCP conduct the Pentagon's version of climate stress tests, which they call "decision scaling" for vulnerability assessment using case studies on water supply risk management in Colorado Springs, Colorado, and on extreme fire risk at Edwards Air Force Base in California. In the conclusion to the presentation, the authors note that decision scaling can be tailored to any number of DoD use cases beyond individual installations such as particular mission types and weapons systems. They also noted that, while an avenue for further research was when the technical capacities of the SERDP and ESTCP were abundant, more effort is required to organize, share, and provide an evolving guide to resources to improve stakeholder engagement, climate information, and the estimation/ modeling of impacts.

SERDP and ESTCP were obvious agencies to lead this review process because past SERDP/ESTCP initiatives included studies to understand and assess environmental vulnerabilities across a range of conditions. They included drought risk on installations in the southwest desert, a Fire Science Strategy developed in 2014 focusing on improved modeling of smoke management and fire planning on DoD installations, studies of changes to the Arctic terrestrial environment relevant to DoD infrastructure, and the Air Force 14th Weather Squadron's provision of authoritative datasets and tailored decision aids to the combatant commanders. The SERDP and ESTCP are further spearheading a number of Arctic-related research projects such as a shoreline erosion prediction model for the North Slope region of Alaska, investigating solutions for damage caused by thawing permafrost on de-paved runways at Thule Air Base, Greenland, and the Office of Naval Research's Arctic and Global Prediction Program to predict environmental conditions and disruptive weather events several weeks and months in advance. Separate from the SERDP and ESTCP, climate resilience work is pursued internationally through the Defense Environmental International Cooperation program, in which the combatant commands work with partner nations on a host of projects. The U.S. Africa Command's water security engagements range throughout the Chad Basin and Tanzania; U.S. Europe Command's water workshop operates in the Czech Republic; and U.S. Northern Command partners with several Scandinavian countries for its Arctic mission analysis.

While the work of the SERDP and ESTCP has proven immensely useful to DoD's ability to respond to legislative requests quickly, the output of their work is not perfect, as the political theater of 2019 shows. A Government Accountability Office report from June of that year detailed some of the inner workings of the government's climate analysis processes and reiterated previous calls for the creation of a national climate information system that could assist policymakers at the federal, state, and local levels in making informed decisions about climate risks. The GAO noted that agencies across the federal government collect and manage many types of climate information, including observational records from satellites and weather monitoring stations on temperature and precipitation, among other things; projections from complex climate models; and tools to make this information more meaningful to decision-makers.[26] One clear recommendation the SERDP and ESTCP could pursue would be to extend the analyses already completed out into the future to at least 2100, and to include all four RCP scenarios in line with the IPCC's methodologies.

Additional climate risk models frequently employed include vulnerability mapping, which traces out subnational vulnerabilities to identify the locations of likely security threats or humanitarian emergencies and disasters. One notable set of vulnerability maps developed for DoD's Minerva Project identifies physical exposure to climate hazards, population density, household and community resilience, and governance as the four processes driving its assessment.[27] As discussed above with traditional vulnerability assessments, these models face a common challenge in "downscaling" global climate processes into regional or local impacts, and then identifying where climate impacts in one region may pose security risks to another. They are also often hampered by the fact that certain regions do not have high-resolution climate projections on a micro scale, which then feeds uncertainties on the second and third order about political instability, economic reporting, and non-climate environmental changes. However, advances in data science show some promise on this point. Depending on their methodologies, traditional vulnerability assessments may also experience difficulties in assessing risks of abrupt climate changes, as these non-linear events are difficult to predict with any accuracy.

Additional models in use include "dark reports" that identify what is not yet known about the subject and why it is not known, and communicate these findings to help planners anticipate potential risks associated with this uncertainty.[28] In addition, there are table-top gaming and scenario analyses developed in conjunction with academia such as the 2011 volcanic ash scenario developed by the U.S. Air Force alongside NASA scientists, DoD tropical storm and tsunami games centered on the Hawaiian Islands, and DoE exercises on methane mining off the coast of Japan in 2009, which

proved to be invaluable for responding to the Fukushima nuclear accident in 2011.[29] One final real-time technique is earth observation satellite-based models. These extend to both non-profit organizations and private entities that are unrelated to the groups referenced earlier. Among these are groups such as the UN Institute of Training and Research's food supply chain analysis, which uses satellite images in conflict areas like Syria and South Sudan to analyze how much of the farmland in a given area will be able to be harvested in a particular growing season dependent on a number of micro-scale variables, and the company TellusLabs, which uses satellite imagery and machine learning predictions of economic and environmental future conditions. Largely focused on the commodities industry, TellusLabs is working with government agencies to predict crop yields across the United States and aims to expand to international markets, eventually creating a global grain supply prediction model to locate and prevent weaknesses in the global and local food supply chain.

THE CLIMATE SECURITY COUNCIL AND THE NEW GEOPOLITICS OF CLIMATE

Separate from the consideration of military installation vulnerability, a thorough study of the methodologies being utilized by private sector climate risk models shows great promise in overcoming the historical bias of the climate-conflict nexus and reevaluating the utility of existing intelligence work on climate in several ways. From a realist perspective, there is a demonstrable benefit to be had in the improved resilience of military assets, installations, and personnel to a changing climate that can strengthen U.S. force posture. From a liberal institutionalist perspective, U.S. leadership in developing climate risk models will have a natural standardizing effect on climate security discussions internationally and would significantly restore U.S. global leadership in the estimation of allies and partners. In allowing the Pentagon to align resources better in a time of overextended defense budgets, it would also allow policymakers to take advantage of the relative lack of political gridlock in the defense community's judgment—especially compared to the logjam represented by electoral politics.

The work road ahead for ODNI's new Climate Security Advisory Council occupies a strange no man's land between secrecy and transparency. Although so much of the data that will inform its actions is already publicly available, the work of the Council is not mandated to be circulated widely and it is likely not feasible to expect it to act as a repository for all DoD logistics and basing standards. Nevertheless, to the extent it can help the federal government calibrate its own climate risks, it should build on the work of the SERDP and ESTCP and lobby forcefully for the most wide-ranging climate disclosure possible. Rather than waiting for policymakers to announce their requirements for deliverables like climate vulnerability analyses before engaging in existing assessment processes, the new Council should recognize that adoption of TCFD- and SASB-aligned standards is vital to the task of providing comprehensive reporting on climate risks and in helping determine which elements of the cumulative DoD climate risk should be publicized. There is already some precedent for this with the Pentagon's 2014 Climate Change Adaptation Roadmap, whose goals included the identification and assessment of the effects of climate change on the Department, the integration of climate considerations across the Department, and collaboration with internal and external stakeholders.[30] However, there are some legislative proposals in the mix that go much further: The Department of Defense Climate Resiliency and Readiness Act would require the Pentagon to achieve net zero energy use by installations that do not support combat operations by 2030, to create new Assistant Secretary posts for Energy and Climate Resiliency within the Office of the Secretary of Defense as well as under the Secretaries of each of the service branches, and further consider the effects of climate change and contractors' energy efficiency performance among a slew of other key performance indicators.[31]

In keeping with the SERDP's and ESTCP's recognition that there is no "one size fits all" approach to understanding climate risk, and especially because of its only temporary four-year authorization in the NDAA, the Climate Security Advisory Council should carefully consider all information channels it can utilize to source observational data, including Federal Emergency Management Agency floodplain maps, data from the National Oceanic and Atmospheric Administration, and data from the National Institute of Standards and Technology, so that it can begin looking at installation vulnerability data as quickly as possible rather than waiting for the development of its own tool. In light of the temporary mandate given to the Council by the NDAA, it should also follow the counsel of former ODNI leaders who have lobbied for the creation of a more permanent climate security infrastructure, including a task force composed of analysts from across the IC but housed within the CIA to write a National Intelligence Estimate on Climate Change with a specific focus on national and international security implications.[32] Similar structures could be set up across many of the 17 agencies under ODNI oversight, especially within the Department of Energy's Office of Intelligence and Counterintelligence, the National Geospatial-Intelligence Agency, and the State Department's Bureau of Intelligence and Research—which last year became the object of another media firestorm when the Trump administration ordered an analyst briefing the House Intelligence Committee to alter his written testimony in order to diminish the threat posed by climate disruptions.[33]

The Climate Security Advisory Council should also vigorously pursue research in climatic variables that are only beginning to be understood, such as atmospheric rivers, and push the research agenda of climate-related security concerns past the present focus on the Arctic as a strategically vital area to include regions like the Tibetan plateau in Asia, the Northern Triangle countries of Central America, and Pacific Island nations presently being courted by the Chinese.[34] Although the creation of the Advisory Council falls short of the recommendations of some analysts, such as for the Center for Climate and Security to create a permanent interagency Climate Security Crisis Watch Center within ODNI or to appoint a Senior Director for Climate Security in ODNI, the recommendations above would be in keeping with the Center's suggestion to pursue climate security infrastructure assessments and mission impact assessments as part of a robust research agenda.[35] The Center's Director—and former Principal Deputy Under Secretary of Defense (Comptroller)—has emphasized that this agenda is only in the earliest stage and that the dialogue between domain experts and security professionals is still running into bottlenecks where the two sides are unaware of the fact that they are asking vastly different questions of one another.[36] As the experience of intelligence reform in the early 2000s demonstrates, the IC is capable of making remarkable changes in a short period of time. It will need to do so again with the issue of climate change as the bipartisan agreement about the threats it poses extends beyond the security community and into the broader public.

Being able to meet the threats that may come from America's competitors and adversaries in the future will require at the very least that the U.S. is capable of fielding its armed forces at full strength, and might even require significant modification to how the Intelligence Community frames the new geopolitics of climate where carbon emissions do not respect physical borders or established constraints on state sovereignty. Regardless of the outcome of the climate change-armed conflict discussion or the mandate of the Climate Security Advisory Council, there are risks to U.S. force posture *now* that the Department of Defense can work to fix even though its leaders at present are not doing so. Any further delay cannot be tolerated.

NOTES

[1] Tammy Duckworth, "Opening Statement (as prepared): Understanding and Combating the Security Risks of Climate Change," Senate Democrats Special Committee on the Climate Crisis hearing, February 7, 2020, https://www.schatz.senate.gov/imo/media/doc/Sen.%20Duckworth%20Opening%20Statement%20Understanding%20and%20Combatting%20the%20Security%20Risks%20of%20Climate%20Change.pdf.

[2] Adam Schiff, "Opening Statement at Hearing on National Security Implications of Climate Change," U.S. House of Representatives, Permanent Select Committee on Intelligence Hearing, June 5, 2019, https://docs.house.gov/meetings/IG/IG00/20190605/109197/HHRG-116-IG00-MState-S001150-20190605.pdf.

[3] John Conger, "Climate Security Consensus Breaks into the Open," Center for Climate and Security blog, March 14, 2019, https://climateandsecurity.org/2019/03/14/climate-security-consensus-breaks-into-the-open/.

[4] Josh Busby, "It's Time We Think Beyond 'Threat Multiplier' to Address Climate and Security," New Security blog, January 21, 2020, https://www.newsecuritybeat.org/2020/01/its-time-threat-multiplier-address-climate-security/.

[5] CNA Military Advisory Board, "National Security and the Threat of Climate Change" (Alexandria, VA: CNA Corporation, 2007), p. 44, https://www.cna.org/CNA_files/pdf/National%20Security%20and%20the%20Threat%20of%20Climate%20Change.pdf.

[6] Office of Senator Elizabeth Warren, "The Climate Risk Disclosure Act of 2019," July 10, 2019, https://www.warren.senate.gov/imo/media/doc/The%20Climate%20Risk%20Disclosure%20Act%20of%202019%20-%20One%20Pager.pdf.

[7] Bank of the Netherlands, "Increasing Climate-Related Risks Demand More Action from the Financial Sector," October 5, 2017, https://www.dnb.nl/en/news/news-and-archive/dnbulletin-2017/dnb363837.jsp.

[8] Caroline Binham, "Bank of England to Set Up Tough Climate Stress Tests," *Financial Times,* December 18, 2019, https://www.ft.com/content/bacdb162-217e-11ea-92da-f0c92e957a96.

[9] Neta Crawford, "Pentagon Fuel Use, Climate Change, and the Costs of War," Watson Institute of International and Public Affairs, Brown University, June 12, 2019, https://watson.brown.edu/costsofwar/files/cow/imce/papers/2019/Pentagon%20Fuel%20Use,%20Climate%20Change%20and%20the%20Costs%20of%20War%20Final.pdf.

[10] "National Defense Authorization Act for Fiscal Year 2020," Conference Report to Accompany S. 1790, p. 931, https://www.congress.gov/116/bills/s1790/BILLS-116s1790enr.pdf.

[11] Emily Meierding, "Disconnecting Climate Change from Conflict: A Methodological Proposal," in *Reframing Climate Change: Constructing Ecological Geopolitics*, Shannon O'Lear and Simon Dalby, eds. (London and New York: Routledge, 2016), p. 56.

[12] Katherine Mach et al., "Climate as a risk factor for armed conflict," *Nature*, No. 571, June 12, 2019, https://www-nature-com.proxy.library.georgetown.edu/articles/s41586-019-1300-6#Sec8.

[13] See Daniel R. Coats, "Worldwide Threat Assessment of the US Intelligence Community, Statement for the Record," Senate Select Committee on Intelligence, May 11, 2017, pp. 13-14, https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf; Coats, "Worldwide Threat Assessment of the US Intelligence Community, Statement for the Record," Senate Select Committee on Intelligence, February 13, 2018, pp. 16-17, https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA—Unclassified-SSCI.pdf; and Coats, "Worldwide Threat Assessment of the US Intelligence Community, Statement for the Record," Senate Select Committee on Intelligence, January 29, 2019, p. 23, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR—SSCI.pdf.

[14] Conger, March 14, 2019.

[15] Robert Litterman, "Climate Change Is a Risk Management Failure that Can and Must Be Fixed Immediately," Senate

Democrats' Special Committee on the Climate Crisis hearing, March 12, 2020, https://www.schatz.senate.gov/imo/media/doc/Litterman%20Testimony%20short%20version%20.pdf.
[16] Frédéric Samama, "Climate Change Is a Risk Management Failure that Can and Must Be Fixed Immediately," Senate Democrats' Special Committee on the Climate Crisis hearing, March 12, 2020, p. 3, https://www.schatz.senate.gov/download/fred-samama-testimony-03-12-20.
[17] Personal interview with Hajin Kim, April 9, 2020.
[18] Rhodium Group, "Clear, Present and Underpriced: The Physical Risks of Climate Change," April 2019, https://rhg.com/wp-content/uploads/2019/03/RHG_PhysicalClimateRisk_Report_April_Final.pdf.
[19] Chris Mooney and Missy Ryan, "Pentagon revised Obama-era report to remove risks from climate change," *The Washington Post*, May 10, 2018, https://www.washingtonpost.com/news/energy-environment/wp/2018/05/10/pentagon-revised-obama-era-report-to-remove-risks-from-climate-change/?utm_term=.363e23710466.
[20] Michael Klare, *All Hell Breaking Loose: The Pentagon's Perspective on Climate Change* (New York: Metropolitan Books, 2019), p. 16.
[21] Office of the Under Secretary of Defense for Acquisition and Sustainment, "Report on Effects of a Changing Climate to the Department of Defense," January 2019, https://partner-mco-archive.s3.amazonaws.com/client_files/1547826612.pdf.
[22] Paulina Glass, "Lawmakers Tell Pentagon: Revise and Resubmit Your Climate-Change Report," *Defense One*, February 5, 2019, https://www.defenseone.com/threats/2019/02/lawmakers-tell-pentagon-revise-and-resubmit-your-climate-change-report/154657/
[23] Rao Kotamarthi, Linda Mearns, Katharine Hayhoe, Christopher Castro, and Donald Wuebbles, "Use of Climate Information for Decision-Making and Impacts Research: State of Our Understanding," SERDP-ESTCP Webinar #30 presentation, April 7, 2016, https://www.serdp-estcp.org/content/download/38659/365338/file/Final%20-%20SERDP%20ESTCP%20Webinar%20#%2030%20(RC%2004072016)%20V4%20(4).pdf.
[24] James Kuiper, Veerabhadra R. Kotamarthi, Andrew Orr, and Jiali Wang, "Geospatial Analysis Tool Kit for Regional Climate Datasets (GATOR): An Open-source Tool to Compute Climate Statistic GIS Layers from Argonne Climate Modeling Results," Argonne National Laboratory, Environmental Science Division, August 2017, pp. 15-16, https://www.serdp-estcp.org/content/download/46232/430589/file/RC-2242%20User%20Manual.pdf.
[25] Richard Moss and Casey Brown, "DoD Decision Making and Climate Change," SERDP-ESTCP Webinar #41, October 20, 2016, pp. 26-38, https://www.serdp-estcp.org/content/download/40566/388573/file/SERDP%20ESTCP%20Webinar%20#%2043%20V6.pdf.
[26] U.S. Government Accountability Office, "Climate Resilience: DOD Needs to Assess Risk and Provide Guidance on Use of Climate Projections in Installation Master Plans and Facilities Designs," June 2019, GAO-19-453, https://www.gao.gov/assets/700/699679.pdf.
[27] Joshua Busby, "Mapping Epicenters of Climate and Security Vulnerabilities," in *Epicenters of Climate and Security: The New Geostrategic Landscape of The Anthropocene*, eds. Caitlin E. Werrell and Francesco Femia, June 2017, p. 124, https://climateandsecurity.files.wordpress.com/2017/06/15_mapping-epicenters.pdf.
[28] Chad Briggs, "Foresight Tools & Early Warning Systems: Vulnerability Assessments for Abrupt and Non-linear Climate Risks," in *Epicenters of Climate and Security: The New Geostrategic Landscape of The Anthropocene*, eds. Caitlin E. Werrell and Francesco Femia, June 2017, p. 118, https://climateandsecurity.files.wordpress.com/2017/06/14_foresight-tools.pdf.
[29] Amy Luers and Bessma Mourad, "Tools for Understanding Systemic Risks like Climate Change" in *Epicenters of Climate and Security: The New Geostrategic Landscape of The Anthropocene*, eds. Caitlin E. Werrell and Francesco Femia, June 2017, pp. 110-112, https://climateandsecurity.files.wordpress.com/2017/06/13_tools-for-understanding-systemic-risks.pdf.
[30] Climate Change Adaptation Working Group, "Department of Defense 2014 Climate Change Adaptation Roadmap," Senior Sustainability Council, Department of Defense, pp. 4-14, https://www.acq.osd.mil/eie/downloads/CCARprint_wForward_e.pdf.
[31] Office of Senator Elizabeth Warren, "The Department of Defense (DoD) Climate Resiliency and Readiness Act Section-by-Section Summary," May 15, 2019, https://www.warren.senate.gov/imo/media/doc/Warren-DoDClimateResiliencyandReadinessAct%20Section-by-Section%20Summary.pdf.
[32] Electronic correspondence with former DNI James Clapper, February 3, 2020.
[33] Juliet Eilperin, "Intelligence aide, blocked from submitting written testimony on climate change, resigns from State Dept." *The Washington Post*, July 10, 2019, https://www.washingtonpost.com/climate-environment/2019/07/10/intelligence-aide-blocked-submitting-written-testimony-climate-change-resigns-state-department/.
[34] Scripps News, "New Scale to Characterize Strength and Impacts of Atmospheric River Storms," University of California, San Diego, Scripps Institution of Oceanography, February 5, 2019, https://scripps.ucsd.edu/news/new-scale-characterize-strength-and-impacts-atmospheric-river-storms.
[35] John Conger, Francesco Femia, and Caitlin Werrell, "A Climate Security Plan for America: A Presidential Plan for Combating the Security Risks of Climate Change," The Climate and Security Advisory Group, September 24, 2019, pp. 19-22, https://climateandsecurity.files.wordpress.com/2019/09/a-climate-security-plan-for-america_2019_9_24-1.pdf.
[36] Personal interview with John Conger, March 12, 2020.

Diego H. Núñez is an MA degree candidate in the Security Studies Program at Georgetown University's School of Foreign Service, where he concentrates on U.S. national security policy. Formerly an editor at the Viking imprint of Penguin Random House, he has served as an advisor to a number of political campaigns at the federal and state levels and is currently active in state-level COVID-19 response coordination. His research interests include the intersection of national security and climate change, defense innovation, and U.S.-China relations. A native of Los Angeles, Diego holds an AB in History and Literature, as well as Economics, from Harvard College.

Uncertainty Is What You Make of It: How It Affects Conflict and Perception in Intelligence

by Javier Martínez Mendoza

OVERVIEW

Reducing uncertainty has been deemed the main objective of intelligence practice. However, uncertainty remains a core factor of intelligence and international politics. As a result, intelligence practitioners can assess it only in terms of estimates. Also, it is possible to analyze and address its effects on intelligence and conflict. Namely, it can drive practitioners and policymakers to make decisions based on personal assumptions that might lead to conflicting behavior. Nevertheless, if properly handled, uncertainty can lead to improved communication that helps intelligence practice and dispels conflicting misperceptions through reassurance.

INTRODUCTION

There is a common expectation among officials that the most important goal of the practice of intelligence is deepening policymakers' understanding so they make *better* decisions, and this is achieved by reducing uncertainty and identifying risks and opportunities.[1] This notion that uncertainty reduction is at the core of intelligence, however, falls short in describing a world whose understanding thereof is uncertain in nature.[2]

Indeed, the ordinary world is defined by complexity, uncertainty, and ambiguity. Consequently, these features condition policymaking, military operations and, ultimately, national security. It is under this non-receding environment that Carl von Clausewitz discussed "fog and friction,"[3] through which intelligence and security practitioners carry out their work, collecting and analyzing information that enables decision-makers to elaborate sound and adequate policies despite uncertainty. Nonetheless, their endeavor does not go unaffected by uncertainty. Clausewitz's "fog of war" as a universal property of reality can occasionally lead to intelligence products characterized by ambiguous and misleading information. Likewise, strategic uncertainty has often made decision-makers fall into committing mistakes when formulating policy, as they base it on flawed assumptions and priorities. Thus, the Intelligence Community's most evident challenge posed by uncertainty takes form in intelligence failures that can shake up intelligence practice (including its ways and structures) and international politics.[4]

Ever since its institutionalization during the Cold War, the Intelligence Community—broadly conceived—and its practices have undergone a series of transformations and embraced new technologies in order to keep up with the logics and dynamics of international politics. However, the nature of intelligence has not changed and uncertainty has remained a constant and defining factor of international politics and, as a result, intelligence activity. For instance, the frequency and impact of intelligence failures between the 9/11 terror attacks and the invasion of Iraq can be attributed to the effect of the uncertainty produced by the collapse of the Soviet Union, the end of the Cold War world order, and the incapacity of the Intelligence Community to adapt to those changes in a timely fashion.[5]

Nowadays, after a series of radical reforms have taken place in order to reduce intelligence failures, intelligence in the post-9/11 era finds itself at a new crossroads propelled by the aftermath of the Arab Spring, China's economic surge, and Russia's hostile re-emergence. These geopolitical developments pose new challenges and questions regarding the relation between intelligence and uncertainty. Namely, what is the role of uncertainty in intelligence and security in terms of its effects on the latter, and how can intelligence and security practitioners address it?[6]

As this article will elaborate thoroughly, when uncertainty takes over the intelligence and decision-making processes, ambiguity and speculation will determine the policies pursued. Policymakers will base their formulations on personal, cultural, and situational factors, as well as worst-case scenarios that most probably will end up in self-fulfilled prophecies that spark conflict.[7]

This article explores the impact of uncertainty on intelligence and conflict, basing its argument on the core idea that uncertainty can increase the possibility of intelligence failure and conflict onset by provoking misperceptions and leading

decision-makers to indulge in personal biases and impulses. Its first two sections discuss what uncertainty is and the effects it has on intelligence practice in terms of its propensity to cause intelligence failures and increase the likelihood of conflict. The third section addresses how to deal with uncertainty in intelligence and security practice by seeing it as a matter of communication and perception. Then, the intelligence failures that led to the invasion of Iraq and the management of arms races will be used as empirical evidence to support the arguments presented in the previous sections. Finally, the concluding remarks elaborate on the way a new approach to uncertainty can help intelligence and security practitioners prevent intelligence failure and conflict.

UNCERTAINTY AND INTELLIGENCE

First, let us start from a general overview of what uncertainty is. Any accurate definition must acknowledge that it is a central and ever-present characteristic of international politics. It is rooted in human nature and its need to make sense of reality, making every political and social act part of uncertainty's domain.[8]

Theoretically, uncertainty implies being unsure of what is true or false about a determined set of statements. It is both a personal and a social phenomenon insofar as people experience it individually, and they are never certain or uncertain about the same facts nor to the same degree. Ultimately, uncertainty surpasses what one knows, as it surrounds and influences everyday life and, especially, future events. This in turn provides its foundations as a source of uneasiness, which forces people to overlook it or try to supress it when making choices. Regardless, every decision is ultimately reached accounting for uncertainty, either consciously or unconsciously.[9]

Scholars and practitioners have defined uncertainty in different and often inconsistent ways. Coming back to the international relations tradition, it is possible to find that definitions depend on which theory's lenses are used:

> [R]ealists generally define uncertainty as *fear* induced by the combination of anarchy and the possibility of predation; rationalists as *ignorance* (in a non-pejorative sense) endemic to bargaining games of incomplete information and enforcement; cognitivists as the *confusion* (again non-pejoratively) of decision making in a complex international environment; and constructivists as the *indeterminacy* [sic] of a largely socially constructed world that lacks meaning without norms and identities.[10]

Yet, these definitions lack the practicality needed to apply them to the intelligence tradecraft. Considering the analysis by Robert Jervis of Alexander Wendt's application of quantum theory in social sciences, it could be argued that each theory's definition of uncertainty is part of a broader understanding of the concept.[11] Where realism and rationalism see a problem of lack of information, cognitivism and constructivism emphasize perception and interpretation, but both perspectives should complement each other depending on every manifestation of uncertainty at a determined time.[12]

Uncertainty can refer both to events that are unknown, like future developments and outcomes, and those only understood in general terms but without knowing their specific manifestation. Instead, what can be known is the variety of possible results and their probability of occurring. It can originate from various sources, including the very event in question and the reaction of other actors depending on one's actions. Moreover, sources of strategic uncertainty, more related to realism and the security dilemma, consist of asymmetric information regarding other actors' traits and intentions.[13] However, the existence of a "fundamental" source of uncertainty attributed to randomness and "stochastic features" in international politics has led scholars to come up with definitions based on the application of quantum theory to social sciences and centered on probabilities.[14] For instance, Jervis considers that uncertainty not only encompasses ignorance of what an event is, but also everything that could be known about it.[15] Then, he stresses that uncertainty is different from risk insofar as probabilities are known for risk, contrary to uncertainty. Risk can thus be considered as a measurable instance of uncertainty.[16]

These remarks on uncertainty start shedding light on how it affects intelligence. The complexity of uncertainty's probabilistic nature makes it prone to misunderstanding. Consequently, when dealing with it, practitioners are exposed to an ever-present risk of blurring Jervis' considerations and must analyze the probabilities of usually only one possible outcome. As uncertainty is subjective, they can also base their assumptions on their personal takes of historical successions of events, unaware of their own uncertainty. This, in turn, can result in reports and policies that are filled with personal and cultural biases and base likelihood on personal confidence and categorical judgments.[17]

Furthermore, Peter Jackson proposes that uncertainty manifests in four interrelated factors: "time and space, organization, politicization, and cognition."[18] Regarding the first variable, political existence is transitory; nothing is solid or stable, but bound to change. Thus, by the time

a situation is addressed and information is gathered, most likely it has already evolved, adding a sense of hesitation to intelligence practice.[19]

The other three obstacles are key to understanding the role that uncertainty plays in intelligence. As Howlett et al. would argue, "Political institutions and practices [politicization], governance capacities [organization], and problems with knowledge or uncertainties underlying processes and practices [cognition]"[20] are the cause of intelligence failure. Uncertainty is the permissive variable that sets the interplay in motion.

In order to understand this mechanism, and how it transcends to the security realm, it is important to analyze the cognitive obstacle discussed by Jackson: human intelligence is not perfect. Its rationality has limits, which derive from its need to simplify complex realities in order to make sense of them and leads analysts to create a set of assumptions and beliefs that determines the way intelligence practitioners gather and analyze information.[21] Also, when irrationality takes over, a political actor might act against its interests or yield to ill-fated strategies.[22] On the other hand, organization as an obstacle refers to how intelligence agencies and their practitioners can share information in the most effective way. It can be associated with how to avoid the politics of uncertainty and blame, which arguably inhibits analysts from openly sharing their views on probabilities of outcomes and developments in order to avoid criticism.[23]

Regarding politicization, its link with threat perception should be stressed, as it is the intelligence obstacle that lets uncertainty's impact reach the security realm. Human beings are both social and political beings. As a result, threat interpretation cannot be understood except as a social and political phenomenon, in which political ideologies and beliefs determine what is perceived as a threat. Amid uncertainty, political actors allocate a political identity (a psychological act) and attribute a threat to another actor—a social act.[24]

Political actors are naturally inclined to fall into cognitive biases—so much so that even the analysts must follow structured analytic techniques to avoid them. If a deviation from rationality meets misperception of one's capabilities or the certainty of the information, a serious risk to peace can be posed. Uncertainty will lead the political actor to fall into a habit of assuming worst-case scenarios and thus move more closely to conflict. Thus, uncertainty in international politics can ground radical developments, destabilizing the system, increasing the chance of conflicts based on personal and political convictions instead of sound strategy that avoids unnecessary fights.[25]

UNCERTAINTY, PERCEPTION, AND CONFLICT

Thomas Hobbes traced the origin of conflict between humans (and, thus, of war) back to uncertainty. Following his line of thought, several scholars from a realist-leaning tradition have pointed out that, notwithstanding the possibility that most actors are well-intentioned and averse to aggression and power accumulation, it is their inability to fully grasp others' real intentions that drives them to embrace a defensive behavior which could turn into a preemptive attack. In short, fear caused by uncertainty pushes actors toward conflict-prone actions.[26]

From a rationalist perspective, war is neither the most efficient nor the most desired outcome. However, states still go to war, and uncertainty can explain the reasoning that makes them deem it as desirable. During a dispute over a good, bargaining will be affected by the actors' lack of knowledge about the other's capabilities and preparedness for war. This ignorance can lead them to overconfidence regarding their own capabilities and make them overly optimistic about the prospects of an impending war, driving them closer to this outcome.[27]

Uncertainty over other aspects, like the conflict's result, the costs of it, and the rival's resolve, also influences the war's onset. Supposedly, the higher the costs of war and the greater access to information, the less likely conflict will be. Nevertheless, scholarly work is split on whether lack of information directly increases the risk of engaging in violent conflict, or if it drives the parties involved toward more precautious behaviors. With regard to the former, uncertainty can incentivize misrepresentation and cause serious miscalculations and information asymmetries that ultimately raise the likelihood of war due to mutual optimism.[28] On the other hand, the literature also suggests that arguments relating to uncertainty over outcome with war propensity are based on bilateral models that do not correspond with the real world. Instead, proponents argue that increased uncertainty can induce actors to adopt more peaceful ways. Accordingly, when looking at the variables that condition uncertainty, external ones like the polarity of the system and capabilities distribution can directly increase estimation complexity and expected costs of war, thus increasing actors' caution and diminishing the probability of the war sparking. Indeed, the more uncertain future changes in power distribution are, the less inclined actors will be to take advantage of a sudden change, whether it is in their favor or not. On the contrary, the more closely the actors approach a state of parity in their capabilities, the broader the information gap between them and the more imminent an attack will be.[29]

Instead of refuting each other, these contrasting views might suggest that actors behave in different fashions depending on whether they are accounting for uncertainty, and on how or what kinds of uncertainty they are considering. Hence, it is argued this will be determined by how decision-makers react to uncertainty. Just looking at the systemic level of analysis would be short-sighted, making it necessary to address how decision-makers respond to the external stimuli from an anarchic and uncertain international in the form of policy.[30]

Consequently, the need arises to understand the role of perception in policymaking and conflict. From a psychological approach to uncertainty, it could be pointed out that conflicts emerge from a misperception about critical information. This misperception, which can be understood as "the gap between the world as it actually exists and the world as it exists in the mind of the perceiver,"[31] could be caused by cognitive biases, like the obstacles discussed in the previous section of this article.[32]

International politics pundits and decision-makers similarly assume that the latter's perception of the world is objective and at most times flawless, but this is not the case. Moreover, policymakers usually and wrongly believe that, notwithstanding the difficulty to trace their homologues' preferences and intentions, theirs should be crystal clear to the rest. This also shows an underlying assumption that others perceive the world, as well as one's actions, just as one perceives them. However, human beings, and thus political actors, perceive the world around them in ways that differ both with everyone else's perception and with the way reality presents itself, or the "objective" realm. Hence, the need to distinguish between the world as seen by policymakers—psychological and subject to perception—and the world where their policy will be enacted becomes evident.[33]

This is the psychological setting in which intelligence practitioners and decision-makers must respond to threats, along with the perpetual presence of uncertainty. When they assess risks and probabilities in the light of events of uncertain likelihood, they will base their analysis and choices not just on their goals and calculations but also on their perception. To overcome this situation, given human nature, their judgment might use heuristics or inferential rules that simplify mental hurdles but, when it comes to policymaking, can give in to biases that compromise the decision-making process by fostering conflict, distrust, and miscalculation.[34]

Indeed, intelligence practitioners and decision-makers' response to uncertainty goes hand in hand with the psychological impact it has on them, and it cannot be fully understood but as an intricate connection between cognition and emotion. On the one hand, in their attempt to fill in the missing pieces of information, they will resort to cognitive images that create stereotypical models, which in turn will shape their emotional and strategic responses. In the case of intelligence practitioners, this is particularly concerning as they run the risk of jumping to conclusions, identifying non-existent patterns, and attributing faulty judgments from an extract of information that needs further information or the recognition of an underlying logic. Intelligence failure can thus occur due to misinterpretation, wrong assumptions, and the overlooking of warnings and developments.[35]

On the other hand, despite the usual attribution of intelligence failures to practitioners, in the end their only mission is to inform and drive policymaking; it is decision-makers who determine the course of action.[36] They can also engage in self-defeating heuristics and stereotypical cognitive images. Most importantly, when facing uncertainty in a decision-making process, policymakers can become impulsive and overconfident, indulging their individual desires instead of choosing the most appropriate and sound policy. Likewise, in extreme situations, such as those of increased uncertainty, they can give in to compulsive behavior and restrict themselves from looking at alternative courses of action based on a subjective sense of determinacy [sic—we in the U.S. would probably use the word "determinance"], which also acts as a psychological relief from their actions.[37]

ADDRESSING THE PROBLEM OF UNCERTAINTY

The previous sections of this article have dealt with the logic that makes uncertainty a permissive cause of conflict based on its effect on decision-makers' perceptions. If uncertainty has such an undesirable role in decision-making, the first way to deal with it that comes to mind is reducing it. Indeed, Thomas Fingar insists on how much effort the U.S. government exerts to carry out such a task, which he considers intelligence's ultimate purpose.[38] In order to fulfill this objective, a practitioner must have good analytical skills, and the ability to understand the target audience and what it needs. Practitioners must also follow a general integrity of ethics, to give only what they believe as true as much as possible. Fingar's view of intelligence seems optimistic, as he assumes that a smarter and more collaborative Intelligence Community with access to better technologies will deliver better and faster intelligence. This will increase knowledge and, thus, reduce uncertainty. However, Jervis reconsiders Clausewitz's assumptions about "fogginess," claiming that more knowledge will only lead to more uncertainty.[39] For instance, practitioners should be aware of the risk that intelligence reports can end up increasing uncertainty if

the information provided generates more questions and causes friction in policymakers' cognitive processes, instead of dispelling the "fogginess" that surrounds the viability of a determined policy.

Arguably, reducing uncertainty has been at the core of intelligence practice ever since the notion was installed in U.S. intelligence by Sherman Kent in the 1940s. Nonetheless, it was Fingar who introduced another approach to uncertainty as a way of communicating uncertainty through verbal representations of likelihood and the use of subjective probabilities. He separated the understanding of uncertainty reduction between the decrease of ignorance and ambiguity—unachievable in terms of quantum theory and probabilities—and the building of resilience against ambiguity, achieved through probabilistic estimates and analysts' take on the information presented.[40]

It is possible to identify a shift from the assumption that uncertainty can be eliminated to an understanding that, instead, it should be accounted for and assessed. Through estimations, analysts recognize the uncertainties surrounding a situation, and instead of looking for a single answer seek a diverse set of possibilities, even if that increases uncertainties. It is likely that such openness about acknowledging uncertainty will be met with resistance on the part of the Intelligence Community. However, after the intelligence failures that defined the first years of the 21st century, it is important to express any divergence about levels of uncertainty and perception.[41] This renewed requirement for openness should be taken seriously to avoid overconfidence when presenting a hypothesis, keeping the main message as concise and simple as possible—without complicating it by adding other scenarios—and refraining from sharing predictions when there is not enough certainty. Intelligence practitioners can also establish standardized tools and vocabulary to represent uncertainty. For instance, measurable uncertainty in the form of risk has been used in order to assess unmeasurable uncertainty.[42]

Another key development in addressing uncertainty in intelligence should focus on strengthening the sense of community among intelligence practitioners, agencies, and decision-makers. Only through a community-oriented intelligence process with decision-making authority distributed among various officials can we welcome debate and sharing while drawing changes in responsibility distribution and tools from other disciplines. Adjustments to new geopolitical developments and their uncertainties will be faster and will come without destabilizing intelligence failures.[43]

Furthermore, when carrying out intelligence analysis, practitioners account for information gaps, namely the difference between what is known and what needs to be known in order to implement a policy reliably, which considers the effects of uncertainty on every specific goal. Finally, every risk and probability assessment involving uncertainty has to be carried out following differentiated approaches instead of sticking to standardized practices, since each problem presents challenges of a distinct nature and their implications to policymaking will also be different.[44]

As to how intelligence can deal with uncertainty's role in conflict onset, it will be argued that actors can use it as an opportunity for communication through signalling. In a setting of mutual uncertainty, there are no incentives for misrepresentation, thus enabling actors to show their true intentions and paving the way to credible signalling and the opportunity to cease conflict or cooperate.[45] Even during war, actors can still communicate and signal their preferences and capabilities, as well as updates on them, thanks to disclosures of private information. War thus provides an opportunity to learn and provide information that could lead to peace. Moreover, through their wartime behavior, actors can inform power hierarchies or take steps toward a settlement. Also, if they misrepresented information before war, the new state of conflict can provide incentives to stop this action and bargain instead.[46]

Nonetheless, this can all be avoided if actors are perfectly transparent about investments and changes in their capabilities, motivated by the threat of preventive war, namely deterrence.[47] Following this logic, deterrence constitutes an optimal opportunity for signalling. In order to work, the threat must be credible and capable, aspects that depend both on information regarding the costs of war and perception all the same.[48]

Just as uncertainty can lead to intelligence failures and even costly wars, intelligence can prove key in overcoming the risks posed by uncertainty and help avoid unnecessary conflicts. This is achieved by the fundamental role intelligence plays in deterrence and reassurance. Indeed, when practitioners embark on their collection activities, intelligence practitioners participate in signalling and communication that can inform decision-makers from both sides about preferences and capabilities. Therefore, intelligence practice influences the processes of deterrence and reassurance, not just through the collection of information but through asserting credibility and producing knowledge.[49]

Before going further, three points need to be stated. First, it is necessary to acknowledge the simultaneous existence of an objective reality and multiple subjectively perceived realities. Second, in deterrence theory, any political actor must have both the willingness and the opportunity to achieve credibility, since every political behavior depends on the probabilistic occurrence of intent and circumstances. Finally, the security dilemma on which deterrence is founded conceives a well-defined notion of uncertainty.[50]

Considering the security dilemma and deterrence theory, the key to countering the conflict-driving effect of uncertainty is shifting perceptions using reassurance.[51] To realize successful reassurance, decision-makers and intelligence practitioners need to think about and perceive the world in terms of the others, so that they can interpret their actions and build the most accurate external image according to their interests. This means deepening one's understanding of the others' set of values, beliefs, and perceptions and, at the same time, making one's external image, including beliefs and values, as transparent as possible. This demonstrates the usefulness of applying political psychology to intelligence analysis when dealing with uncertainty, especially in times of looming conflict.[52]

CASE STUDIES

In order to ground the empirical soundness of the arguments already considered, the following lines will be devoted to the intelligence failure surrounding Iraq's purported weapons of mass destruction (WMD) program that led to its invasion, to pinpoint the relation among uncertainty, intelligence, and conflict onset. Similarly, arms control during the Cold War will be covered to address the contributions of intelligence and signalling to deterrence and reassurance.

Iraq's Alleged WMD Program

According to Richard Immerman, intelligence work prior to the 2003 invasion of Iraq was flawed and fell short of addressing the uncertainty and the resulting ignorance surrounding the Saddam Hussein regime's possession of weapons of mass destruction.[53] However, Immerman argues that, even had intelligence been sound, policymakers did not actually let it guide their decision-making process. They simply did not feel the need to follow the intelligence.

Indeed, the intelligence practitioners believe that, regardless of the flaws and rushed preparation which defined the now infamous National Intelligence Estimate (NIE) assessing Iraq's possession of WMD, its content did not end up influencing the decision to invade in any significant way. President George W. Bush's resolve to proceed with the invasion was already clear before actual efforts to justify its direness were undertaken. Despite common belief among the Intelligence Community that, at the time, Iraq posed no real threat and the most likely course of action was not engaging in war, decision-makers from the coalition countries did everything in their power to alter the intelligence cycle in favor of supporting the invasion.[54]

In addition, according to Fingar's observations of the intelligence at the time, it was stained by deep uncertainty, as officials were trying to make sense of past mistakes, specifically the failure to foresee the 9/11 attacks.[55] As a result, intelligence practitioners believed they had to embolden their probability assessments and communicate worst-case scenarios with more emphasis. This occurred simultaneously with the pressures of U.S. Vice President Dick Cheney's so-called one percent doctrine and its demand for deeming "'low probability, high impact' events as if they were certain."[56]

Considering the prevailing circumstances at the time, according to the U.S. government's perspective, invading Iraq encompassed less uncertainty than not engaging in war. Plus, it represented an opportunity to take the initiative had Iraq heightened its WMD program or perpetrated an attack. Not invading Iraq was a scenario that accounted for more outcomes and their cost, and was more robust to uncertainty. Still, Bush's administration considered it could not afford even the minimal possibility of a change in the status quo. The U.S. Intelligence Community thus faced the challenge of having to prove that Iraq did not have and would not have WMD. Since proving a negative is immensely difficult to accomplish, and the Community admittedly did not have the capabilities to make a judgment on such terms, it was ultimately unable to overcome this overwhelming uncertainty.[57]

Three uncertainty obstacles can be observed in the intelligence that led to the Iraqi WMD failure: politicization, since political leaders had already made up their minds regarding their resolve to invade Iraq;[58] the Intelligence Community's structural flaws, as they were not prepared to assess post-Cold War threats during their winding adaptation to a 21st century world; and, finally, cognitive biases on the part of practitioners, who did not assess more than one possible outcome in their reports prior to the 2001-2003 period, and decision-makers, as their will to attack Iraq was rooted in personal assumptions and a rationale based on worst-case scenarios.

Both the U.S. and Iraqi governments misperceived each other ahead of the 2003 invasion. Even the aftermath of the 1990-1991 Gulf War was misinterpreted by Hussein's side, as he deemed it as beneficial for Iraq's strategic position. He also failed two times to acknowledge the perils of engaging in combat against the U.S. Finally, not only did he underestimate the significance for the U.S. of the end of the Cold War and the 9/11 attacks, but he overestimated the shared interests that could avoid conflict with the sole superpower.[59]

Following Duelfer and Dyson's line of argument, there was a misperception on the U.S. side regarding how Saddam Hussein interpreted the outcome of the Gulf War, and how he did not perceive the U.S. as an existential threat or an enemy he would be willing to attack in the immediate future, since his main concern at the time was Iran. Furthermore, back in the U.S., the Iraqi regime's hostilities ever since the Gulf War were portrayed as imperialistic instead of as a response to grievances rooted in the Iraq-Iran war of the 1980s. In the end, despite Hussein being

an actual enemy, the imminence of the threat he posed was the result of a perception process experienced by American decision-makers.

Western decision-makers were excessively certain that Iraq had an extensive amount of WMD and the will to use it against them. Uncertainty is not just about lack of information, but also about excess of misinformation. This could have been the case for Western political leaders' decision to invade Iraq. Their personal assumptions fell into an obstacle of time and space that was uncovered after the WMD intelligence became evident. Both George W. Bush of the U.S. and Tony Blair of the UK argued that, had they known before that the Iraqi WMD threat was overestimated, they would have still carried out the invasion, signalling a cognitive obstacle that denies the role of timely and sound information in policymaking.[60]

Arms Control in the Cold War

Regarding the possibility of reassuring the use of deterrence and the security dilemma, it is necessary to consider that arms races are carried out by rational states based on threat perceptions, which means that when an actor perceives another building up an arsenal it will respond likewise. In other words, behind increasing military capabilities as a strategic policy there is not only the logic of deterrence but also a process of communication in response to perceived threats.[61] However, considering the opportunities raised by uncertainty, political actors can interact following the same logic, but in reverse, using arms control as a form of communication. Human agency in the form of sound intelligence and skillful negotiators was key in turning external factors into incentives that led the Soviet Union and the U.S. to commit themselves to arms control during the Cold War, de-escalating tensions between them and improving communication.[62]

Montgomery considers reassurance as a method of signalling and communication that can help understand the other's preferences and thus help reduce uncertainty.[63] In order to achieve effective deterrence and reassurance efforts during the Cold War, intelligence proved to be an indispensable element. Intelligence capabilities and activities on both sides represented both a threat and a factor of reassurance to the superpowers. By collecting information, intelligence practitioners informed their side on their rival's capabilities and preferences while keeping the rival threatened. However, by continuing with collection efforts, the rival was also reassured that the other side was cautious and feeling threatened, turning this into reassurance that there was no significant advantage on the rival's part. Furthermore, intelligence activity was crucial in providing arms control efforts with legitimacy and credibility.[64] Intelligence thus constituted the bridge between deterrence and the possibility to "pursue arms control agreements, cap military spending, avoid proliferation policies, and…seek compromise."[65]

Thanks to the work of the Intelligence Community, deterrence and perception worked effectively in dealing with uncertainty and warding off conflict, and ultimately interpreting Mikhail Gorbachev's reassurance efforts, which ultimately contributed to the end of the Cold War. Western allies' interpretation of the Intermediate-Range Nuclear Forces (INF) treaty and the Conventional Armed Forces in Europe (CFE) treaty, which practically eliminated any Soviet material capacity to carry out an attack on Western Europe, was informed by timely and sophisticated intelligence tradecraft.[66]

A WAY FORWARD

Uncertainty is a defining feature of reality. Trying to reduce it or eliminate it is ill-fated, as its nature is not related just to lack of information but also to imperfect information, overconfidence, and probabilities of everything that could be. Thus, uncertainty is preferable to ignorance, and the only goal one can aim for is coping with it.[67]

Intelligence in the 21st century has been given the task of tackling the risk of unforeseen events and thus making the world more predictable. However, one cannot just expect uncertainty to be fully overcome in intelligence practice nor in international politics. Through the challenge of uncertainty, intelligence tradecraft has the opportunity to maintain its key role not only in decision-making, but in international politics, by seeing uncertainty as an opportunity instead of a liability, and using it to adapt and transform the way intelligence practitioners and decision-makers interact and communicate.[68]

On the other hand, in order to boost predictability and tackle the effect of uncertainty in the human mind, technology and fuzzy methods have been developed for artificial intelligence to account for uncertainty and humans' perception of it. The application of artificial intelligence to address uncertainty is undeniably ground-breaking, but it should not replace humans in intelligence practice or it would run the risk of missing cognitive processes that are vital for decision-making.[696]

As the philosopher Luciano Floridi stated, "Uncertainty can be harnessed in order to restrain the power that comes with information or constrain it to make it perform better."[70] Likewise, it is possible to witness uncertainty's potential to enable meaningful communication that can help override misperceptions and improve intelligence practice through community intelligence, estimative assessment, and questioning personal assumptions. Uncertainty, therefore, is what intelligence practitioners and decision-makers make of it.

NOTES

[1] Immerman, R.H. (2016). Intelligence and the Iraq and Afghanistan Wars, *Political Science Quarterly,* 131:3.

[2] Jervis, R. (2017a). One World or Many? *Critical Review*, 29:2, p. 176.

[3] Payá Santos, C.A. & Delgado Morán, J.J. (2017). Incertidumbres del análisis dimensional de la inteligencia, *Revista Lationamericana de Estudios de Seguridad,* 21, pp. 226, 233. Jackson, P. (2010). On Uncertainty and the Limits of Intelligence. In L.K. Johnson (ed.), *The Oxford Handbook of National Security*. Oxford, UK: Oxford University Press, p. 454.

[4] Jervis, R. (2006). Reports, politics, and intelligence failures: The case of Iraq, *Journal of Strategic Studies*, 29:1, pp. 11, 13. Heazle, M. (2010). Policy Lessons from Iraq on Managing Uncertainty in Intelligence Assessment: Why the Strategic/Tactical Distinction Matters, *Intelligence and National Security*, 25:3, p. 291. Mayer, M. (2015). Strategic Uncertainty and Missile Defence: Revisiting the 1999 National Intelligence Estimate, *Contemporary Security Policy*, 36:3, p. 450.

[5] Santos, Payá, & Morán, Delgado (2017), p. 226. Jackson (2010), p. 454. Javorsek II, D., & Schwitz, J.G. (2014). Probing Uncertainty, Complexity, and Human Agency in Intelligence, *Intelligence and National Security*, 29:5, p. 643.

[6] Javorsek II & Schwitz (2014), p. 653.

[7] Jackson (2010), p. 454. Jervis (2017a), p. 176. Mayer (2015), p. 450.

[8] Rathbun, B.C. (2007). Uncertain about Uncertainty: Understanding the Multiple Meanings of a Crucial Concept in International Relations Theory, *International Studies Quarterly*, 51:3, p. 533. Bas, M.A., & Schub, R. (2017a). Theoretical and Empirical Approaches to Uncertainty and Conflict in International Relations. *Oxford Research Encyclopedia of Politics*. Retrieved from https://oxfordre.com/politics/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-537. Sluga, H. (2014). *Politics and the Search for the Common Good*. Cambridge, UK: Cambridge University Press, pp. 231-232.

[9] Lindley, D. (2014). *Understanding Uncertainty.* Hoboken, NJ: John Wiley & Sons, pp. 1-12.

[10] Rathbun (2007), pp. 533-534.

[11] Jervis (2017a), p. 171.

[12] Rathbun (2007), p. 537.

[13] Bas & Schub (2017a). Santos, Payá & Morán, Delgado (2017), p. 233.

[14] Bas & Schub (2017a).

[15] Jervis (2017), pp. 175, 178.

[16] Phythian, M. (2012) Policing Uncertainty: Intelligence, Security and Risk, *Intelligence and National Security*, 27:2, p. 193.

[17] Javorsek II & Schwitz (2014), pp. 641, 644. Jervis (2017a), pp. 175, 177, 179. Alvarez, R.M., & Franklin, C.H. (1994). Uncertainty and Political Perceptions, *The Journal of Politics,* 56:3, p. 672.

[18] Jackson (2010), p. 454.

[19] Sluga (2014), p. 233.

[20] Howlett, M., Ramesh, M., & Wu, X. (2015). Understanding the persistence of policy failures: The role of politics, governance and uncertainty, *Public Policy and Administration,* 30:3-4, p. 215.

[21] Jackson (2010), p. 456.

[22] Santos, Payá, & Morán, Delgado (2017), p. 230.

[23] Jackson (2010), p. 464. Friedman, J.A. (2019). *War and Chance: Assessing Uncertainty in International Politics*. Oxford, UK: Oxford University Press.

[24] Jackson (2010), pp. 458-459. Bellin, S. (2019). Embracing Uncertainty: Primo Levi's Politics of the Human, *Paragraph,* 42:1, p. 54. Vitriol, J.A., Tagar, M.R., Federico, C. M., & Sawicki, V. (2019). Ideological uncertainty and investment of the self in politics. *Journal of Experimental Social Psychology,* 82. Gurley, J. (2007). Emerson's Politics of Uncertainty. *ESQ: A Journal of the American Renaissance* 1(4), p. 327.

[25] Bas & Schub (2017a). Jervis (2017), p. 178. Bas, M.A. (2012). Measuring Uncertainty in International Relations: Heteroskedastic Strategic Models, *Conflict Management and Peace Science*, 29:5. Javorsek II & Schwitz (2014), p. 648. Hopf, T. (2010). The logic of habit in International Relations, *European Journal of International Relations,* 16:4.

[26] Chung, H. (2015). Hobbes' State of Nature: A Modern Bayesian Game-Theoretic Analysis, *Journal of the American Philosophical Association,* 1:3, pp. 488-490. Ramsay, K. (2017). Information, Uncertainty, and War, *Annual Review of Political Science,* 20, p. 506.

[27] Ramsay (2017), pp. 507-511. Bas, M.A., & Schub, R. (2016a). How Uncertainty about War Outcomes Affects War Onset, *Journal of Conflict Resolution,* 60:6.

[28] Reed, W. (2003). Information, Power, and War, *The American Political Science Review,* 97:4. Smith, B., & Spaniel, W. (2019). Militarized Disputes, Uncertainty, and Leader Tenure, *Journal of Conflict Resolution,* 63:5, p. 1225. Fey, M., & Ramsay, K. (2011). Uncertainty and Incentives in Crisis Bargaining: Game-Free Analysis of International Conflict, *American Journal of Political Science*, 55:1. Bas & Schub (2016a), pp. 1100-1101. Bas, M.A., & Schub, R. (2016b). Mutual Optimism as a Cause of Conflict: Secret Alliances and Conflict Onset, *International Studies Quarterly,* 60. Bils, P., & Spaniel, W. (2017). Policy bargaining and militarized conflict, *Journal of Theoretical Politics,* 29:4.

[29] Bas, M.A., & Schub, R. (2017b). Peaceful Uncertainty: When Power Shocks Do Not Create Commitment Problems, *International Studies Quarterly,* 61. Bas & Schub (2016a). Herbst, L., Konrad, K., & Morath, F. (2017). Balance of power and the propensity of conflict. *Games and Economic Behavior,* 103. Reed (2003).

[30] Jervis, R. (1976). *Perception and Misperception in International Politics.* Princeton, NJ: Princeton University Press.

[31] Duelfer, C.A., & Dyson, S.B. (2011). Chronic Misperception and International Conflict: The U.S.-Iraq Experience, *International Security,* 36:1, p. 75.

[32] Kurizaki, S. (2016). Signalling and perception in international crises: Two approaches, *Journal of Theoretical Politics,* 28:4, pp. 625-626.

[33] Jervis (1976), pp. 44-56. Jervis, R. (2017b). *How Statesmen Think: The Psychology of International Politics.* Princeton, NJ: Princeton University Press, pp. 191-192.

[34] Tversky, A., & Kahneman, D. (1982). Judgment under uncertainty: Heuristics and biases. In Kahneman, D., Slovic, P., & Tversky, A. (eds.), *Judgment under Uncertainty: Heuristics and Biases* (pp. 3-20). Cambridge, UK: Cambridge University Press. Slovic, P., Fischhoff, B., & Lichtenstein, S. (1982). Facts versus fears: Understanding perceived risk. In Kahneman, D., Slovic, P., & Tversky, A. (eds.), *Judgment under Uncertainty: Heuristics and Biases* (pp. 463-490). Cambridge, UK: Cambridge University Press. Heuer, R. (1999). *Psychology of Intelligence Analysis*. Center for the Study of Intelligence. Retrieved from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/PsychofIntelNew.pdf.

[35] Jervis (2017b). Herrmann, R. (2013). Perceptions and Image Theory in International Relations. In Huddy, L., Sears, D., & Levy, J. (eds.), *The Oxford Handbook of Political Psychology*. Oxford, UK:

Oxford University Press. Fingar, T. (2011). *Reducing Uncertainty: Intelligence Analysis and National Security.* Stanford, CA: Stanford University Press, pp. 21-24.
[36] Fingar (2011), p. 24.
[37] Milkman, K. (2012). Unsure what the future will bring? You may overindulge: Uncertainty increases the appeal of *wants* over *shoulds, Organizational Behavior and Human Decision Processes,* 119. Jervis (1976).
[38] Fingar (2011), pp. 1-6.
[39] Jervis, R. (2012). U.S. Presidents and Foreign Policy Mistakes by Stephen G. Walker and Akan Malici; Reducing Uncertainty: Intelligence Analysis and National Security by Thomas Fingar, *Political Science Quarterly,* 127:1, pp. 143, 145.
[40] Ben-Haim, Y. (2016) Policy neutrality and uncertainty: An info-gap perspective, *Intelligence and National Security*, 31:7, pp. 978, 979. Jervis (2017a), pp. 176-177. Isaksen, B.G.M., & McNaught, K.R. (2019). Uncertainty handling in estimative intelligence – Challenges and requirements from both analyst and consumer perspectives, *Journal of Risk Research*, p. 2. Jervis (2012).
[41] Weiss, C. (2008). Communicating Uncertainty in Intelligence and Other Professions, *International Journal of Intelligence and CounterIntelligence*, 21:1. Friedman, J.A., & Zeckhauser, R. (2012). Assessing Uncertainty in Intelligence, *Intelligence and National Security,* 27:6, p. 826.
[42] Phythian (2012), p. 196. Pate-Cornell, E. (2015). Uncertainties, Intelligence, and Risk Management: A Few Observations and Recommendations on Measuring and Managing Risk, *Stanford Journal of International Law*, 51:1. Dhami, M.K. (2018) Towards an evidence-based approach to communicating uncertainty in intelligence analysis, *Intelligence and National Security*, 33:2.
[43] Weiss (2008). Javorsek II & Schwitz (2014), p. 653. Conradt, L., List, C., & Roper, T.J. (2013). Swarm Intelligence: When Uncertainty Meets Conflict, *The American Naturalist,* 182:5.
[44] Ben-Haim (2016), pp. 982-984. Isaksen & McNaught (2019).
[45] Haynes, K., & Yoder, B. (2020). Offsetting Uncertainty: Reassurance with Two-Sided Incomplete Information, *American Journal of Political Science*, 64:1.
[46] Przepiorka, W., Rutten, C., Buskens, V., & Szekely, A. (2020). How dominance hierarchies emerge from conflict: A game theoretic model and experimental evidence, *Social Science Research,* 86, 102393. Fey & Ramsay (2011). Shirkey, Z. (2016). Uncertainty and War Duration, *International Studies Review,* 18. Bils & Spaniel (2017). Spaniel, W., & Bils, P. (2018). Slow to Learn: Bargaining, Uncertainty, and the Calculus of Conquest, *Journal of Conflict Resolution,* 62:4.
[47] Debs, A., & Monteiro, N. (2014). Known Unknowns: Power Shifts, Uncertainty, and War, *International Organization,* 68:1.
[48] Jervis (2017b), p. 195. Zagare, F., & Kilgour, D. (2000). *Perfect Deterrence*. Cambridge, UK: Cambridge University Press, pp. 70, 93.
[49] Herman, M. (2011) Intelligence as Threats and Reassurance, *Intelligence and National Security*, 26:6.
[50] Duelfer & Dyson (2011), p. 75. Cioffi-Revilla, C., & Starr, H. (1995). Opportunity, Willingness & Political Uncertainty: Theoretical Foundations of Politics, *Journal of Theoretical Politics,* 7:4, p. 448. Kessler, O., & Daase C. (2008). From Insecurity to Uncertainty: Risk and the Paradox of Security Politics, *Alternatives,* 33, p. 212.
[51] Montgomery, E.B. (2006). Breaking Out of the Security Dilemma: Realism, Reassurance, and the Problem of Uncertainty, *International Security,* 31:2.
[52] Jervis (1976), pp. 409-410. Jervis, R. (1985). Perceiving and Coping with Threat. In R. Jervis, R.N. Lebow, & J.G. Stein (eds.), *Psychology and Deterrence* (pp. 13-33). Baltimore: Johns Hopkins University Press, p. 33.
[53] Immerman (2016).
[54] Fingar (2011), pp. 89, 92. Heazle (2010). Ben-Haim (2016), p. 989.
[55] Fingar (2011), p. 94.
[56] Debs & Monteiro (2014), p. 18.
[57] Ben-Haim (2016), pp. 984-990. Yager, R. (2006). Fuzzy Set Methods for Uncertainty Management in Intelligence Analysis, *International Journal of Intelligent Systems,* 21, p. 523. Debs & Monteiro (2014), pp. 18-19.
[58] Immerman (2016). Javorsek II & Schwitz (2014). Ben-Haim (2016). Fingar (2011).
[59] Woods, K.M., & Stout, M.E. (2010). Saddam's Perceptions and Misperceptions: The Case of "Desert Storm," *The Journal of Strategic Studies*, 33:1. Duelfer & Dyson (2011).
[60] Jervis (2006, 2017a).
[61] Rider, T.J. (2013). Uncertainty, Salient Stakes, and the Causes of Conventional Arms Races, *International Studies Quarterly*, 57.
[62] Javorsek II & Schwitz (2014). Nelson, A. (2018). Arms Control as Uncertainty Management. *Center for International & Security Studies at Maryland.* Retrieved from https://www.cissm.umd.edu/sites/default/files/ArmsControlAsUncertainty_042318.pdf.
[63] Montgomery (2006), pp. 160-167.
[64] Herman (2011).
[65] Zagare & Kilgour (2000), p. 131.
[66] Montgomery (2006), pp. 178-182. Herman (2011).
[67] Floridi, L. (2015). The Politics of Uncertainty, *Philosophy & Technology,* 28:1. Jervis (2017a). Schedler, A. (2013). *The Politics of Uncertainty: Sustaining and Subverting Electoral Authoritarianism.* Oxford, UK: Oxford University Press. Alvarez & Franklin (1994).
[68] Rijsdijk, E. (2011). The politics of hard knowledge: uncertainty, intelligence failures, and the "last minute genocide" of Srebrenica, *Review of International Studies,* 37:5, p. 2223. Schedler (2013).
[69] Yager, R. (2020). Using fuzzy measures for modeling human perception of uncertainty in artificial intelligence, *Engineering Applications of Artificial Intelligence,* 87. Yager (2006). Faunt, R., & Gentile, P. (2019). Artificial Intelligence within the Intelligence Community: The Need to Retain the Human Dimension, *American Intelligence Journal,* 36:2.
70 Floridi (2015).

Javier Martínez Mendoza, who hails from Mexico, is an Erasmus Mundus student in the International Master's in Security, Intelligence, and Strategic Studies Program at Dublin City University, pursuing a concentration in Conflict Studies. Besides his work experience in economic strategy and political communication, he has carried out research and coursework on intrastate conflict, insurgency, terrorism, and radicalization. As a Youth Associate of the Mexican Council on Foreign Affairs (COMEXI), Javier maintains an active social media presence, analyzing topics related to democracy and international politics in various media outlets.

Russian Influence in Austria and Its Impact on the European Union

by Julia Girardi

OVERVIEW

Russia and Austria have strong economic and political ties to one another, which affects how the two countries interact. Russia utilizes energy deals, diplomatic meetings and honors, billions of Euros in Foreign Direct Investment (FDI), and other methods to try to ensure that Austria epitomizes a pro-Kremlin nation within the European Union (EU). Russia's goal to influence Austria is part of a greater objective to weaken the EU, divide Europe and the United States, and create a political and cultural environment more favorable for Moscow's interests.[1]

If a foreign power were able to influence votes in the European Parliament, EU security may be at risk. The aim of this study is to analyze how Russia influences Austria and assess whether such levers of influence impact Austria's voting behaviors on Russia-related resolutions in the European Parliament. This was done by examining the extent of Russia's political and economic influence on Austria in conjunction with votes cast by Austrian Members of the European Parliament over the last 15 years.

Why Austria?

Austria serves both political and economic purposes for Russia. Austria may not be highly influential in EU policymaking, but it is a participant and thus could prove a useful tool for Russia's desires to lift sanctions and influence EU policies. Austria is not the only EU member state targeted by Russian influence campaigns, but it is particularly vulnerable due to a historic public attitude of pervasive euroscepticism[2] and business ties to Central and Eastern Europe. Austria also is skeptical of its Western partners, a perception that Russia may exploit. Economically, Austria serves as a conduit for laundering Russian money into Western Europe.

Recent political and economic events involving Austrian and Russian politicians and businesspeople have brought concerns over Russian influence in Austria to the forefront of the international media. For example, in May 2019, a video surfaced in which the Austrian Vice Chancellor, Heinz-Christian Strache (then-party leader of the Freedom Party of Austria, or FPÖ), discussed trading government contracts in exchange for campaign publicity with an alleged niece of a Russian oligarch while vacationing in Ibiza.[3] The FPÖ's ties to Russia have been a matter of domestic and international scrutiny for several years.

Despite observable characteristics of Russian political and economic influence in Austria, the vast literature regarding Russian influence operations in Europe has a limited focus on Austria. Research has been conducted on Russia's influence in Austrian politics and Russian economic ties with Austria. However, the literature lacks any comprehensive study analyzing both political and economic influence together, and the greater impact it could have on the EU. This research will fill this gap.

RUSSIAN INFLUENCE CAMPAIGN IN AUSTRIA

Russian influence campaigns are tailored to fit the specific societal vulnerabilities of the countries they target. Austria is a wealthy nation with a pragmatic approach to foreign policy that prioritizes economic considerations over political goals. Austria's economic focus on Central and Eastern Europe, strong linkages between business and politics, and lax approach to fighting corruption present economic areas that may be exploited. Politically, Russia is able to capitalize on societal cleavages formed by the economic situation, the refugee crisis, and the subsequent rise of populist ideology in Austria that have defined the last decade of Austrian politics.

In Austria, Russia's goals are to:

- Gain political support and friendly voices in Europe
- Use economic incentives as a tool to minimize the chance of Austria politically challenging Russia
- Exploit the vulnerabilities in Austria's political and economic system and use corruption and loopholes for personal gain and political influence

ECONOMIC INCENTIVES

Russia utilizes energy deals, billions of Euros in foreign direct investment (FDI), and lucrative business ventures to help create a system in which Austria is less inclined to challenge Russia politically, for fear of disrupting the flow of money and resources.

Investment and Business Ties

Russia is the second-largest source of foreign direct investment (FDI) in Austria.[4] Following the 2014 onset of the crisis in Ukraine, Russian investments in EU countries fell due to souring relations.[5] However, Russian FDI in Austria nearly doubled between 2013 and 2014; there was another surge between 2016 and 2017.[6] Conley et al. suggest that this increase could be due to the fact the Viennese branches of the Russian Sberbank and VTB Bank were not included in the EU's sanctions against Russia; therefore, investing in Austria via these banks could allow Russia to avoid sanctions and still maintain investment flows into Europe.[7] Austria is an advantageous destination for Russian investment because of its favorable tax policies and confidentiality. These conditions make it possible to launder money through Austrian banks into Western Europe and/or receive tax benefits.[8] Among the largest Russian investors in Austria are energy corporations such as Gazprom and Lukoil, banks, and businesses in the tourism sector.[9]

Austria's low corporate tax rate makes it one of the most business-friendly EU member states.[10] This, combined with the ease of access to Western European markets and historical, political friendliness between the two countries since 1955, makes Austria a profitable and convenient location for Russian businesses. In Austria there are more than 1,000 businesses with Russian stakeholders.[11] The largest of these companies are the Russian energy giants Gazprom, Rosneft, and Lukoil.[12] In 2016 the Russian ambassador to Austria stated that "while Russia felt they had support from Austrian political leaders, 'even stronger support' was provided by 'Austrian companies, the Austrian Economic Chamber and other associations'."[13]

Austrian business entities are also highly active in Russia. According to the Austrian embassy in Moscow, there are currently around 500 Austrian businesses operating in Russia.[14] In a 2018 speech made at a meeting of the Russian-Austrian Business Council in Vienna, President Vladimir Putin suggested that the number of active Austrian businesses in Russia is much higher, totaling 1,200 with an additional 500 Russian-Austrian joint ventures.[15] The insurance group UNIQA, the construction company Strabag, and the ropeway systems manufacturer Doppelmayr[16] are among Austria's most active companies in Russia outside the energy and banking sectors.[17] These companies have political ties as well. The former Austrian Chancellor and head of the Social Democratic Party of Austria (SPÖ), Alfred Gusenbauer, has served as the chairman of Strabag's supervisory board since 2010.[18] The CEO of Uniqa Insurance Group AG (UNIQA), Andreas Brandstetter, was previously the managing director of the Austrian People's Party (ÖVP) from 1994 to 1995,[19] exemplifying Raiffeisen's ties to Austrian politics.

Many Austrian banks have branches and subsidiaries in Russia and are active in the Russian market.

Since the fall of the Soviet Union, Austrian banks have been heavily focused on Central, Eastern, and Southeastern Europe (CESEE), which exposes them to considerable risk.[20] Many Austrian banks have branches and subsidiaries in Russia and are active in the Russian market. The Austrian-owned UniCredit Bank Austria AG (Bank Austria)[21] is the largest foreign bank in Russia. In 2017 UniCredit had assets in Russia worth over •18 billion.[22] Raiffeisen Bank is Austria's second-largest banking group. Its international entity, Raiffeisen Bank International (RBI), made 78 percent of its corporate profits in Russia in 2014.[23] RBI has been scrutinized for its involvement in a variety of Russia-related scandals over the last two decades.[24] Meinl Bank AG, which has recently been renamed Anglo Austrian AAB Bank AG,[25] focuses its business in Central Europe, including Russia. The bank provides many services to wealthy investors and oligarchs in Russia. "The second-largest holding of this equity fund was in Russia's Sberbank as of June 2018, a bank that has been impacted by U.S. and EU sanctions restricting access to their capital markets after the annexation of Crimea."[26] Since 2009 the bank has also been involved in various fraud scandals and money-laundering schemes involving Russian actors.[27]

Russia's largest foreign lending bank, Sberbank, which is state-controlled, maintains its foreign headquarters in Vienna.[28] In 2011 Sberbank acquired the Austrian bank Volksbanken International, yielding it greater access to the Western, Central, and Eastern European financial markets.[29] Siegfried Wolf, Austrian businessman and Chairman of the Supervisory Board of Sberbank Europe,[30] is a personal friend of Vladimir Putin.[31] VTB Bank AG (Austria), a subsidiary of a leading universal bank in Russia, is very active in Austria[32] and also maintains its Southeastern European branch headquarters in Vienna.[33] The Viennese branches of

Sberbank and VTB were granted exemption from the tougher round of EU sanctions enacted in 2014.[34] This is likely why Russian banking activity in Austria has increased since 2014 despite sanctions, and Russian investments in Austria have surged during the same period.[35]

Energy Relations

Energy is the largest component of Austria's relationship with Russia, both economically and politically. Fossil fuels constitute Austria's main imports from Russia.[36] Moreover, Austria is an important transit hub for Russian gas to Western and Central Europe, and Austria's *Österreichische Mineralölverwaltung* (Austrian Mineral Oil Administration, or OMV) is a longtime European partner of Gazprom. Energy relations between Austria and Russia have not been affected by Russia's intervention in Ukraine or the economic sanctions for which Austria is a signatory through the EU. Natural gas imports to Austria from Russia are at a record high, and OMV and Gazprom are working together on many projects.

Austria is dependent on Russian energy imports, particularly natural gas. Austria's foreign dependence on energy imports is higher than the EU average. In 2017 Austria imported 64.4 percent of its energy, and the EU average was 55.1 percent.[37] Many of these imports come from Russia. At the beginning of 2018, Austria was one of eleven EU member states that imported more than 75 percent of total national imports of natural gas from Russia.[38] Dependence on Russian natural gas imports has created an environment in which Austria is unlikely to challenge Russia politically, because it could disrupt the flow of Russian gas into Austria.

The Vienna-based OMV, an integrated oil and gas company, is a key business partner for Gazprom. OMV and Gazprom have worked together on many pipeline projects and other joint endeavors. The largest project is Nord Stream 2. OMV is one of five financial investors for the Nord Stream 2 pipeline,[39] which together will provide financing for half of the total cost of the project over the long term.[40] U.S. economic sanctions targeting the Russian energy sector have affected Nord Stream 2's construction since they were implemented in 2017.[41] However, a new bill called "Protecting Europe's Energy Security Act" was passed by the U.S. Senate Foreign Relations Committee on July 31, 2019; if made into law, this bill will extend sanctions to cover non-Russian companies helping to construct the Nord Stream 2 pipeline, including Austria's OMV.[42] This could lead to increased frustration over sanctions in Austria, and weaken Austrian resolve to continue being a party to sanctions against Russia, causing more tension in the relationship between the U.S. and the EU.

Gazprom has many assets in Austria and provides Austrian energy companies with lucrative projects and joint ventures.

Nord Stream 2 is not the only controversial project that OMV and Gazprom have worked on together. In 2011 the European Commission blocked a deal between OMV and Gazprom in which Gazprom would have acquired shares in the Central European Gas Hub (CEGH) located in Baumgarten, Lower Austria.[43] The Baumgarten gas hub is "the entry point for nearly one third of Russian gas exports to Western Europe."[44] OMV and Gazprom were also set to collaborate on the now defunct pipeline South Stream,[45] and there have been discussions about extending its replacement TurkStream to terminate in Austria's Baumgarten gas hub, though nothing official has been decided.[46]

Gazprom has many assets in Austria and provides Austrian energy companies with lucrative projects and joint ventures. Vienna has been a base for Gazprom since the early 2000s, from which it could expand into the Western European market; the company has established a variety of private funds and subsidiaries in Vienna.[47] Close ties with Gazprom are economically advantageous because they ensure Austria's access to cheap natural gas and stakes in lucrative projects; however, the economic benefits are contingent on maintaining good relations with Russia.

The energy relationship between Russia and Austria transcends politics as well. OMV is closely connected to the Austrian People's Party (ÖVP). An Austrian business journalist described the OMV supervisory board as "dominated by the ÖVP."[48] For example, Wolfgang Berndt, the Chairman of OMV's Supervisory Board since 2010, donated 65,000 Euros to the ÖVP between 2017 and 2019.[49] Such political connections may lead to influence over government policies related to OMV's interests. The gray intersection between business and politics in Austria creates a vulnerability that can be influenced by external business partners.

Additionally, several former high-level Austrian politicians have taken positions in Russian energy companies. In June 2019 former Austrian Chancellor Wolfgang Schüssel became a member of the board of directors of the Russian energy company Lukoil.[50] Lukoil's international holding Lukoil International GmbH is headquartered in Vienna,[51] and four of its subsidiary companies are registered there.[52] Hans Jörg Schelling, former Austrian Minister of Finance, is a consultant for Gazprom.[53]

EXPLOITING VULNERABILITIES AND LOOPHOLES

Political Vulnerabilities

Austria's legacy of corporatism,[54] lax approach to fighting corruption, and banking secrecy laws have made it a haven for Russian businesses and investment.[55] Austria is an advantageous destination for Russian investment because of its favorable tax policies[56] and confidentiality. These conditions make it possible to launder money through Austrian banks into Western Europe, or receive tax benefits.[57]

Since 1945 the Austrian political and corporate landscape has been defined by an informal power-sharing system between the two major political parties (SPÖ and ÖVP) called *Proporz*[58] and a system of corporatism known as the *social partnership*. These phenomena have created a system in which business, industry, and finance are closely tied to politics. Through the Proporz system, many top private and public sector positions are split between persons affiliated with one of the two parties. Such appointments may include non-political positions in government ministries, board-level positions in state-owned or partially state-owned enterprises, and even senior positions in state-run schools.[59] The system is susceptible to corruption and cronyism, and during the last 20 years Austrian political life has been marred by corruption scandals involving bribes for government contracts and favorable legislation.[60] The Proporz system is not as pronounced in Austrian public life as it once was, though it is still present.[61] The corruption scandals of the past few decades illuminate areas that may be exploited by Russia.

Legislation and government policies in Austria are heavily influenced by corporate interest groups representing industry, agriculture, and labor through a corporatist framework known in Austria as the *social partnership*, mentioned earlier. These political interest groups, known as social partners, are historically affiliated with political parties.[62] In turn, members of these interest groups have populated high government posts representing those parties, thereby shaping policies that are heavily influenced by said interest groups.[63] On the supranational front, the social partner interest groups are also able to impact EU policies relating to their interests by influencing Austria's positions in proposals for EU legislation.[64] Austria's constitution protects official secrecy in government, and the Austrian government has often been criticized for a lack of transparency.[65] It is possible to exploit this intersection between business and politics by forging ties with corporations and thus potentially influencing policies.

Austria has deep banking networks across Europe and banking secrecy provisions that make it a popular destination for Russian funds, both licit and illicit.

The Council of Europe's Group of States against Corruption (GRECO) has criticized Austria for its weak legislation on political party financing.[66] Austrian law sets a limit of •2,500 for election donations from foreign individuals, but loopholes exist.[67] On May 24, 2019, a video surfaced in which then-Austrian Vice Chancellor Heinz-Christian Strache (also Chairman of the FPÖ) and Johann Gudenus (then-Managing Club Chairman of the FPÖ and former vice mayor of Vienna) discussed trading government contracts in exchange for campaign publicity with an alleged niece of a Russian oligarch. In the video, Strache detailed ways by which legal loopholes could be exploited to deliver money to political parties without being detected. He also inferred that this is not an uncommon practice in Austrian politics.[68] Although the situation was a set-up and Strache did not actually take money from an oligarch's niece, it exposes the Freedom Party's willingness to engage in such behavior, and the ease through which money (from reportedly illicit origins) could be used to purchase influence in Austrian politics.[69]

Financial Vulnerabilities

Austria has deep banking networks across Europe and banking secrecy provisions that make it a popular destination for Russian funds, both licit and illicit. Major Austrian banks and their international branches and subsidiaries have been implicated in a variety of money-laundering schemes over the past decade that have been traced back to Russian sources. Strong financial involvement in the emerging markets of Central, Eastern, and Southeastern Europe (CESEE) has yielded significant financial gains for Austria but has also left Austrian banks exposed to significant risk. Austrian banks lack a compliance function to require the same standardized practices for its branches and subsidiaries in higher-risk areas such as the CESEE region as it does domestically, thus increasing their susceptibility for illicit financial activity.[70] In 2017 the Organized Crime and Corruption Reporting Project (OOCRP) uncovered an illicit network that has come to be known as the "Russian Laundromat." In connection with this scheme, •1,589,546.9 of Russian funds originating in dubious transactions with Moldovan banks was distributed in more than 25 transactions to Austrian businesses and individuals, including a prominent Viennese international high school and a bank account supposedly belonging to the commercial court of

Vienna (*Handelsgericht Wien*).[71] Seventeen Austrian banks were involved in the Russian Laundromat, including Raiffeisen and Meinl Bank AG.

In March 2019 Hermitage Capital Management filed a complaint with the Vienna Economic and Corruption Prosecutor's Office connecting Raiffeisen Bank International (RBI) to the multibillion-dollar Russian money-laundering scandal known as the Troika Laundromat. Research conducted by the OCCRP shows that this scheme ran between 2004 and 2014; during this time, a total of •169,884,718 flowed through Austria, and •734,333,256 was laundered through RBI banks and branches. Of the many banks used in the illicit network, RBI saw the second-largest amount of funds.[72] It also had strong ties with AB Ukio Bankas,[73] the Lithuanian private bank through which the vast majority of the illicit funds was laundered.[74]

Gain Political Support and Friendly Voices in Europe

Russia has forged ties with influential business leaders and politicians in Austria to influence policies conducive to Russia's interests, such as opposing sanctions. Russia's most explicit political ties are with Austria's Freedom Party (FPÖ), but it also maintains important political and business contacts with members of the mainstream Social Democratic Party (SPÖ) and conservative People's Party (ÖVP).

Russia's soft power in Austria is amplified by political connections among Austrian high-level politicians and businesspeople with Russian politicians and oligarchs, within a corporatist political system characterized by the mixture of political interests and business.[75] The lack of transparency in the Austrian lobbying sphere also raises concerns for corruption.[76]

Relationships with Political Parties

Russia's strongest political ties in Austria are with the FPÖ, a far-right conservative party that holds nationalistic, anti-EU, and anti-American views.[77] Long an underdog in Austrian politics, support for the FPÖ has increased markedly in the last two decades. Its greatest success was in the National Council election of 2017 in which the ÖVP won the largest percentage of the vote and chose the FPÖ as its coalition partner, FPÖ party leader Heinz-Christian Strache became Vice Chancellor, and the FPÖ was awarded six cabinet posts.[78] The FPÖ took a pro-Russian turn beginning in 2007 that became more entrenched after Russia's intervention in Ukraine in 2014.[79] The FPÖ ideologically identifies with Russia's foreign policy representation of themselves as a worldwide defender of traditional values and counterbalance to the U.S. and the liberal world order. The FPÖ, partly because of its pro-Russian stance, is staunchly anti-sanctions. The FPÖ does not try to hide its affinity for Russia; since 2016 it has had a partnership agreement with United Russia (Putin's political party), and in August 2018 Putin was invited to the wedding of Austria's FPÖ-appointed foreign minister, Karin Kneissl, where the two were photographed dancing together.[80]

Since 2008, high-ranking members of the FPÖ have traveled to Russia on multiple occasions to meet with Russian diplomats and politicians. The most notable of these trips took place in December 2016 when the FPÖ became the first far-right European party to enact an association agreement with United Russia. The five-year agreement focuses on making a commitment to meeting and discussing experiences and information on domestic politics; it will automatically renew for another five years, and was sharply criticized by the other political parties in Austria.[81] Members of the FPÖ also have been invited to serve as election observers in Russian and Ukrainian elections. Three members of the FPÖ observed the March 16, 2014, Crimean referendum: Johannes Hübner (then-FPÖ spokesman for foreign affairs), Johann Gudenus, and Ewald Stadler. The FPÖ delegation described the referendum as fair and even "exemplary."[82] Gudenus also observed the gubernatorial elections in Saint Petersburg in September 2014, which he praised as more legitimate and transparent than elections for the European Parliament.[83]

Many European intelligence agencies halted or reduced sharing intelligence with the Austrian domestic intelligence agency...

The FPÖ has worked with Russian political organizations and NGOs to organize and host events including balls, political congresses and conferences, and business events.[84] Between 2008 and 2010, the partially state-funded company Austrian Technologies GmbH that had strong ties to the FPÖ co-organized a variety of Russia-related conferences, one of which was co-organized by the Russian agency Rossotrudnichestvo.

Many European intelligence agencies halted or reduced sharing intelligence with the Austrian domestic intelligence agency (Bundesamt für Verfassungsschutz und Terrorismusbekämpfung, or BVT) following a February 2018 police raid of the agency due to concerns about sensitive data leaks.[85] At the time of the incident the FPÖ was in the coalition government and controlled both the Department of the Interior and the Ministry of Defense, the ministries that control domestic and foreign

intelligence organizations, respectively. Some had expressed concerns over the FPÖ's leadership of the intelligence service, considering its close ties to the Russia.[86]

The FPÖ and Russia both benefit from their relations. They use one another to validate their world view based on anti-EU, anti-U.S., and ultra-conservative values.[87] For Russia, the FPÖ legitimizes its foreign policy by speaking positively of it. Russia is able to present members of the FPÖ in its domestic media as experts from Europe, giving the appearance of vast networks of support for Russian foreign policy. Furthermore, election observations by European politicians legitimize Russian elections, particularly for the purpose of Russia's domestic media. The FPÖ, long an underdog in Austrian politics, gains validation from Russia that it is not alone in its beliefs. As the FPÖ has grown in popularity, Russia has grown in its ability to influence Austrian politics.

Russia also has connections with the mainstream political parties in Austria (SPÖ and ÖVP) and the business community, though their relationship is based on purely economic rather than ideological considerations. Russia did not fully embrace its relationship with the FPÖ until 2016 when the presidential election showed that it would likely be politically successful in the future, because it did not want to spoil its existing relationships with mainstream parties.[88] Sebastian Kurz (ÖVP) visited Russia many times during his time as Foreign Minister and Chancellor to discuss strengthening ties between Russia and the EU. He made Austria's main goal of its 2017 Organization for Security and Cooperation in Europe (OSCE) presidency speeding along the implementation of the Minsk II Agreement to end the conflict in Ukraine.[89]

Russia has many connections with former and current Austrian political and business figures who are trusted people in the political sphere. Heather Conley describes this practice as having the appearance of "influence for sale."[90] For example, former Chancellor Wolfgang Schüssel is on the board of MTS, a Russian telecommunications company,[91] and the Russian energy company Lukoil.[92] Former Chancellor Alfred Gusenbauer is on the board of the Russian Dialogue of Civilization Research Institute. The SPÖ party academy, Doktor-Karl-Renner-Institut, which Gusenbauer formerly directed, works in cooperation with the Dialogue of Civilizations (DOC).[93] Some news outlets have accused the DOC's annual Rhodes Forum for having pro-Kremlin leanings.[94]

Former Chancellor Christian Kern is an independent director on the board of Russian Railways (RZD).[95] Former Finance Minister Hans Jörg Schelling is a consultant for Gazprom and its Nord Stream 2 pipeline.[96] Additionally, many of Austria's large, state-owned or partially state-owned companies that are closely connected to political parties through the social partnership and Proporz systems also have "long-standing ties with Russian companies and oligarchs."[97] The existence of these business connections with Russian entities may lead these politically influential individuals and companies to promote political objectives that are within Russia's interests, or act as advocates for said interests both domestically and internationally. The pervasive anti-sanctions attitude in Austria may be a by-product of this.

Analysis

Austria's strong economic ties with Russia and its dependence on Russian energy imports make it economically beneficial to maintain good relations with Moscow. Austria is unlikely to take a stand against Russia and jeopardize losing these benefits. For example, after the Skripal poisoning in March 2018, nineteen EU member states expelled Russian diplomats from embassies in their countries because they suspected them of being Russian intelligence agents. However, Austria did not.[98] Austrians urged the necessity of keeping open the avenues of communication with Russia, an argument they use often. Austria has had its own issues with Russian intelligence agents active on its soil.[99] In the last 12 years there have been a number of Russian spies uncovered and arrested in Austria, but in each instance the subject was quickly released and relations between the two countries were returned to normal as soon as possible.[100] These instances have shown that Austria is willing to prioritize economic considerations above challenging Russia, and is susceptible to pressure from Russia.[101] This is exactly what Moscow wants.

The number of influential Austrians from the political and business spheres serving on the boards of directors of Russian businesses raises concerns about the ability to buy influence in Austria.

Economic ties with Russia have also impacted Austrian politicians' perceptions of sanctions against Russia. In principle, Austria officially supports EU sanctions against Russia, and votes with the EU to continue them every time they are up for renewal. However, it has also been among the harshest critics of the sanctions since first enacted. Prominent members of the ÖVP, FPÖ, and SPÖ have all repeatedly expressed their desire to see the sanctions against Russia lifted.[102] Christoph Leitl, member of the ÖVP and president of the Austrian Federal

Economic Chamber (Wirtschaftskammer Österreich, or WKO) from 2000 until 2018, is among the most outspoken on the issue, calling EU sanctions against Russia "nonsensical."[103] Despite friendly attitudes toward Russia by the Austrian elite, "the overwhelming majority of Austrians (70 percent) hold a 'negative' or 'rather negative' geopolitical view of Russia."[104]

The number of influential Austrians from the political and business spheres serving on the boards of directors of Russian businesses raises concerns about the ability to buy influence in Austria.[105] By choosing to overlook Russia's corrupt domestic practices and either ignore or assist Russian money laundering into Europe, Western rulers and business elites have given the Russian elites the perception they are equally as corrupt as they are. This encourages more of the same behavior and plays into the Kremlin's foreign policy ideology of a morally depraved West driven only by money.[106] Despite evidence of Russian aggression in the West including election meddling and espionage activity, Austria ignores or denies the existence of Russian influence operations in Austria.[107] Twelve EU member states have updated their policies on Russian interference, but Austria is not among them.[108] Austria's foreign and security policy barely mentions Russia at all,[109] though since 2014 Russian influence campaigns and cyber attacks against EU member states have been matters of great importance across the EU.

Austria's persistence in remaining a neutral intermediary between Russia and the West is not new; since the Kreisky era of the 1970s Austria has stressed the importance of multilateral talks to facilitate solutions to international disputes.[110] It is also not nefarious in itself to seek to keep the channel of communication with Moscow open, but it does place Austria in a precarious position because it, on occasion, contradicts its duties as an EU member state. Austria could weaken EU foreign policy toward Russia with its lenient approach to Russian relations. It is also not possible to gauge how much of Austria's position is due to the desire to safeguard economic benefits and how much is related to the neutrality and risk aversion that is integral to Austrian identity. Both factors certainly play into Austria's behavior toward Russia. Regardless of intent, diplomatic silence surrounding Russian coercive acts in the West, and the deepening of economic and political ties to Russia, may encourage more of the same behavior.[111] A 2007 article written in the Russian newspaper *Kommersant* stated that Austria is "'viewed [by] the Kremlin as a potential lobbyist of its interests in Europe'."[112] Austria's behavior does not necessarily disprove this statement.

QUANTITATIVE ANALYSIS

A quantitative analysis was conducted to determine if there is a relationship between the observed increase in Russian economic and political ties with Austria and Austrian voting patterns in the European Parliament. Data was collected on individual votes cast by Austrian Members of the European Parliament (MEPs) on EU resolutions and relevant amendments to resolutions pertaining to Russia or Russian interests voted on in the European Parliament between 2004 and 2018.[113] A table including the resolutions, amendments, and votes is available upon request.

A quantitative analysis was conducted to determine if there is a relationship between the observed increase in Russian economic and political ties with Austria and Austrian voting patterns in the European Parliament.

Descriptive statistics, more specifically the calculation of the mean of the data points, were utilized to calculate the frequency that pro-Russian options and non-pro-Russian options were voted on, or the frequency at which the MEPs abstained per year. Since the analysis in the previous sections indicates that the Freedom Party of Austria (FPÖ) has become increasingly pro-Russian in its rhetoric and actions since 2007, two analyses were conducted: one with all of the Austrian MEPs, and the other with MEPs from all of the parties except for the FPÖ. The intent was to measure if Austrian MEPs as a whole have shifted their voting habits on Russia-related matters in the European Parliament. If a pattern were to be evident, it would be possible also to gauge if pro-Russian voting behaviors affect parliamentarians outside of the visibly pro-Russian party in Austria (FPÖ). The results from this analysis are displayed in the table below. Furthermore, the resolutions were separated into three categories: association agreements with countries within Russia's perceived sphere of influence, conflicts involving Russia, and human rights matters involving Russia. These categories were chosen because almost every resolution was associated with one of these themes. *The descriptive statistics found that the most Austrian pro-Russian votes or abstentions on Russia-related resolutions in the European Parliament were cast by members of the outspokenly pro-Russian FPÖ. However, Austrian MEPs from other parties have also voted for pro-Russian options or abstained from voting on resolutions related to conflicts involving Russia*.

Table. Votes by Austrian MEPs in the European Parliament, on all Russia-Related Resolutions

		PERCENT (%) OF VOTES FROM MEPS FROM ALL PARTIES			PERCENT (%) OF VOTES FROM MEPS FROM ALL PARTIES EXCEPT THE FPÖ		
Year	# of Items Voted On	**Pro-Russian Option**	**Non-Pro-Russian Option**	**Abstain**	**Pro-Russian Option**	**Non-Pro-Russian Option**	**Abstain**
2004	1	0	92	8	0	100	0
2005	1	0	86	14	0	92	3
2006	0	NA	NA	NA	NA	NA	NA
2007	1	0	100	0	0	100	0
2008	4	31.75	64.5	3.75	26.5	69.75	3.75
2009	0	NA	NA	NA	NA	NA	NA
2010	3	0	91.3	8.7	0	100	0
2011	1	0	82	18	0	100	0
2012	0	NA	NA	NA	NA	NA	NA
2013	1	19	81	0	0	100	0
2014	8	21.5	69.4	9.1	0	87	13
2015	14	15	75	10	4.1	90.5	5.2
2016	3	15.3	60.7	24	0	79	21
2017	5	9.2	82.6	8.2	0	100	0
2018	3	21	62	17	5	85	10

Sources: Mepvote.eu, votewatch.eu, and European Parliament Plenary Session Minutes

*NA denotes areas for which no data was available

Once the descriptive statistics were completed, chi-square tests of independence were performed to examine the relation between voting habits among Austrian MEPs and the following economic and political indicators detailing the relationship between Russia and Austria—frequency of political meetings and visits at three levels: heads of state, other politicians, and leader of the Austrian Chamber of Commerce (WKO); amount of foreign direct investment (FDI) invested in Austria by Russia, and in Russia by Austria (in EUR million); the amount of natural gas imported to Austria from Russia measured in billions of cubic meters (BCM); trade exports from Austria to Russia, and imports from Russia (in EUR 1000); number of treaties signed with Russia; and number of Russian tourist arrivals in Austria. Tables detailing the political and economic indicators and the votes on each selected resolution are available upon request. Not all observed political and economic variables were significant, but some were. *The chi-square tests found that there are statistically significant relationships between Russian FDI in Austria and Russian natural gas imports to Austria, and number of pro-Russian votes or abstentions made my Austrian MEPs.* All chi-square tables, frequency tables, and descriptive statistics related to these categories are available upon request.

CONCLUSION

The line that Austria walks between East and West, epitomized by its deep financial ties with Central, Eastern, and Southeastern Europe, and its persistence in remaining a neutral intermediary between Russia and the West, is dangerous. It is not nefarious in itself to seek to keep the channel of communication with Moscow open, but it places Austria in a precarious position because it, on occasion, contradicts its duties as an EU member state. Austria could weaken EU foreign policy toward Russia with its lenient approach to Russian relations. It is also not possible to gauge how much of Austria's position is due to the desire to safeguard economic benefits and how much is related to the neutrality and risk aversion that is integral with Austrian identity. Both factors certainly play into Austria's behavior toward Russia. Regardless of intent, diplomatic silence surrounding Russian coercive acts in the West, and the deepening of economic and political ties to Russia, may encourage more of the same behavior, particularly because Austria ignores or denies the existence of Russian influence operations in Austria.

The statistical analyses in this research show that there are statistically significant relationships between Russian FDI in Austria and Russian natural gas imports to Austria, and the number of pro-Russian votes or abstentions made my Austrian MEPs. Additionally, the most Austrian pro-Russian votes or abstentions on Russia-related resolutions in the European Parliament were cast by members of the outspokenly pro-Russian FPÖ, but Austrian MEPs from other parties have also voted for pro-Russian options or abstained from voting on resolutions related to conflicts involving Russia. Abstentions are not as strong as pro-Russian votes, but are still noteworthy, because if votes are close on a resolution, abstentions can keep the resolution from passing. Abstentions can also make a point for MEPs who do not feel strongly enough to vote against a resolution but want to make it known that they do not support it.

Although Russia's influence campaign in Austria has yielded some observable successes, it is unlikely that Austria is, or will become, an agent of Russian influence in the EU. The FPÖ will likely maintain its pro-Russian positions, which will be reflected in future votes on Russia-related resolutions in the European Parliament by MEPs belonging to the FPÖ. However, the European Parliamentary elections in May 2019 resulted in a decrease in the number of FPÖ MEPs from four MEPs in the 8th term (2014-2019) to three in the new, 9th term (2019-2023).[114] Therefore, the FPÖ's impact in the European Parliament will be slightly smaller in the current term than the last. Additionally, the FPÖ's involvement in the Ibiza Scandal and subsequent party in-fighting make it unlikely that the party will be elected or chosen as a coalition partner to lead the government anytime soon.

Austria is pragmatic, and its behaviors outside of its borders are largely focused on attaining economic benefits, averting becoming entangled in international conflicts, and using its neutral platform to mediate conflicts between nations. On the one hand, Austria's behavior toward Russia falls within this pattern of behavior that Austria has exhibited since 1955. On the other hand, Austria uses these traits to toe the line of what is acceptable behavior as an EU member state. Austria will continue to balance between East and West, because that allows it to obtain maximum benefits from both sides. However, Austrian politicians and business leaders must be careful not to veer too far to the East, because it could lead to Austria losing credibility in the EU, or these leaders could inadvertently become useful mouthpieces for the Kremlin.

NOTES

[1] Mark Galeotti, "Controlling Chaos: How Russia Manages Its Political War in Europe," European Council on Foreign Relations, September 1, 2017, 2, accessed February 16, 2019, https://www.ecfr.eu/publications/summary/controlling_chaos_how_russia_manages_its_political_war_in_europe.

[2] Christian Karner, "Europe and the Nation: Austrian EU-Scepticism and Its Contestation," *Journal of Contemporary European Studies* 21, no. 2 (2013).

[3] Der Spiegel Staff, "The Strache Recordings – The Whole Story," *Der Spiegel*, May 17, 2019, accessed May 28, 2019, https://www.spiegel.de/international/europe/strache-caught-on-camera-in-ibiza-secret-recordings-a-1267959.html.

[4] Oestereichische Nationalbank (OeNB), "Inward Direct Investment Positions Broken Down by Region: Region by Ultimate Beneficial Owner," March 29, 2019.

[5] Igor Makarov and Alexandra Morozkina, "Regional Dimension of Foreign Direct Investment in Russia," in *Drivers of Regional Integration: Value Chains, Investment and New Forms of Co-Operation* (Economic Policy Forum (EPF) and South African Institute of International Affairs (SAIIA), 2015), pp. 45-71.

[6] Oestereichische Nationalbank (OeNB), *Inward Direct Investment Positions Broken Down by Region*.

[7] Heather A. Conley et al., *The Kremlin Playbook 2: The Enablers*, (Washington, D.C.,, CSIS, March 2019), 4, accessed April 1, 2019, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/190326_KPII_WEB FINAL.pdf.

[8] Makarov and Morozkina, *Regional Dimension of Foreign Direct Investment in Russia*, 9.

[9] Austria invests much less in Russia than Russia invests in Austria; it is not among Russia's top ten investors, but Austrian FDI in Russia increased in 2018. Austrian investment in Russia is largely focused on goods and services, industry, and manufacturing sectors; Kari Liuhto, "The Economic Relations between Austria and Russia," ResearchGate, February 2018, 9, accessed March 22, 2019, https://www.researchgate.net/publication/323007037_The_economic_relations_between_Austria_and_Russia; Makarov and Morozkina, *Regional Dimension of Foreign Direct Investment in Russia*, 11; "Russia: Foreign Investment," Santander Trade Portal (Banco Santander, S.A., September 2019), https://en.portal.santandertrade.com/establish-overseas/russia/foreign-investment; "Wirtschaftsbericht Russische Föderation," Wirtschaftsbericht Russische Föderation § (2019), 10, https://www.wko.at/service/aussenwirtschaft/russische-foederation-wirtschaftsbericht.pdf.

[10] "Taxes in Austria: Corporate Taxation of Companies," Invest in Austria (ABA), accessed September 27, 2019, https://investinaustria.at/en/business-location-austria/taxes.php.

[11] Andrei Zolotov, Jr., "Russisch-Österreichisches Wirtschaftsforum: Es Geht Wieder Aufwärts," Ostexperte.de, November 25, 2016, accessed March 25, 2019, https://ostexperte.de/russisch-oesterreichisches-wirtschaftsforum/.

[12] Zolotov, Jr., *Russisch-Österreichisches Wirtschaftsforum*.

[13] Bernhard Weidinger, Fabian Schmid, and Péter Krekó, *Russian Connections of the Austrian Far-Right* (Budapest: Political Capital, April 2017), 10, http://www.politicalcapital.hu/pc-admin/source/documents/PC_NED_country_study_AT_20170428.pdf.

[14] "Wirtschaftsbeziehungen Zwischen Österreich Und Russland," Österreichische Botschaft Moskau, accessed October 23, 2019, https://www.bmeia.gv.at/oeb-moskau/bilaterale-beziehungen/russische-foederation/wirtschaft/.

[15] "Meeting with Russian and Austrian Business Leaders," President of Russia (Presidential Executive Office, June 5, 2018), http://en.kremlin.ru/events/president/news/57682.

[16] The Austrian company Doppelmayr/Garaventa is the world market leader in ropeway systems and manufactures chairlifts, cable cars, gondolas, and surface tows for ski and amusement parks. Doppelmayr was also contracted to construct facilities for the Sochi Olympics as well as the 2018 World Cup in Russia. Some of this work included a cable liner at Sheremetyevo International Airport in Moscow; Weidinger et al., *Russian Connections of the Austrian Far-Right*, 18; "Doppelmayr/Garaventa Group: Revenue Growth of 5.7%," November 21, 2018, accessed March 25, 2019, http://newsroom.doppelmayr.com/en/doppelmayr/press/doppelmayr-garaventa-group-revenue-growth-of-57/.

[17] Additional Austrian companies that are heavily engaged in Russia include the *Österreichische Mineralölverwaltung* (Austrian Mineral Oil Administration, OMV), discussed earlier in this chapter; the real estate companies Immofinanz and CA Immo; Schoeller-Bleckmann, a producer of drills for oil exploration activities; and the packaging company Mayr-Melnhof. "Österreicher Stark in Russland Engagiert," *Der Standard*, March 24, 2014, https://www.derstandard.at/story/1395363068222/oesterreicher-stark-in-russland-engagiert.

[18] "Dr. Alfred Gusenbauer," STRABAG SE, April 30, 2014, https://www.strabag.com/databases/internet/_public/content.nsf/web/DE-STRABAG.COM-gusenbauer.html#?men1=1&men2=1&sid=142&h=undefined.

[19] UNIQA Group, "Holding Management Board: Andreas Brandstetter," UNIQA Grou, accessed October 23, 2019, https://www.uniqagroup.com/gruppe/versicherung/uniqa-group/management/vorstand-holding/andreas-brandstetter/Andreas_Brandstetter.en.html.

[20] According to the International Monetary Fund (IMF), the CESEE is comprised of the following countries: Albania, Belarus, Bosnia and Herzegovina, Bulgaria, Croatia, Czech Republic, Estonia, Hungary, Kosovo, Latvia, Lithuania, Macedonia, Moldova, Montenegro, Poland, Romania, Russia, Serbia, Slovak Republic, Slovenia, Turkey, and Ukraine; "Safeguarding the Recovery as the Global Liquidity Tide Recedes: Central, Eastern and Southeastern Europe," International Monetary Fund, April 2014, https://www.imf.org/en/Publications/REO/EU/Issues/2017/01/25/SAFEGUARDING-THE-RECOVERY-AS-THE-GLOBAL-LIQUIDITY-TIDE-RECEDES; Wolfgang Sützl, "Austria's Banking Sector: Facts & Figures," European Banking Federation, September 2019, https://www.ebf.eu/austria/.

[21] Some authors refer to UniCredit Bank Austria AG as UniCredit rather than Bank Austria.

[22] Conley et al., *The Kremlin Playbook 2*, 52.

[23] Heather A. Conley et al., "The Kremlin Playbook II: Interactive Abridged Report," Center for Strategic and International Studies, accessed March 21, 2019, https://www.csis.org/features/kremlin-playbook-2?fbclid=IwAR0-k8ymA1Po4fFSmifsPL7Z1WjB6HSrLQ-rB9vF4fZjOd_UbWosNhvoVes.

[24] The bank received criticism for its connection with RosUkrEnergo, a company that was the subject of significant media scrutiny. It is owned by the Ukrainian oligarch Dmytro Firtash, who was the exclusive importer of gas to Ukraine between 2006 and 2008; Raiffeisen (on behalf of unnamed clients who turned out to be Firtash and the Ukrainian politician Ivan Fursin) helped to manage the company in conjunction with Gazprom. Dmytro Firtash was arrested by Austrian authorities at the behest of U.S. law enforcement in 2014 and has been under house arrest in Austria since then, as he awaits a final sentencing to see if he will be extradited to the United States; Taras Kuzio, "Dmytro Firtash Launches New Opaque Gas Intermediary," *Eurasia Daily Monitor*, March 25, 2013, http://www.taraskuzio.com/media11_files/10.pdf; Mark Rachkevych, "U.S. Official: Austrian Bank's Ties to RosUkrEnergo Suspicious," *Kyiv Post*, December 3, 2010, https://www.kyivpost.com/article/content/ukraine-politics/us-official-austrian-banks-ties-to-rosukrenergo-su-91986.html?cn-reloaded=1; Mark Leonard and Nicu Popescu, *A Power Audit of EU-Russia Relations* (ECFR, November 2007), 37, accessed May 8, 2019, https://www.ecfr.eu/publications/summary/a_power_audit_of_eu_russia_relations; Todd Prince, "Dmytro Firtash: Who Is the Ukrainian Tycoon Wanted by the U.S. on Bribery Charges?" RadioFreeEurope/RadioLiberty (Radio Free Europe/Radio Liberty, June 25, 2019), https://www.rferl.org/a/dmytro-firtash-who-is-the-ukrainian-tycoon-wanted-by-the-u-s-on-bribery-charges-/30020239.html.

[25] "Anglo Austrian AAB Bank AG," Anglo Austrian Bank, accessed October 23, 2019, https://www.aab-bank.com/en/home.

[26] Heather A. Conley and Donatienne Ruy, "Kremlin Playbook Spotlight: Austria's Meinl Bank Affairs," Center for Strategic and International Studies, December 14, 2018, accessed March 21, 2019, https://www.csis.org/blogs/kremlin-playbook-spotlight/kremlin-playbook-spotlight-austrias-meinl-bank-affairs.

[27] Conley and Ruy, *Kremlin Playbook Spotlight: Austria's Meinl Bank Affairs*.

[28] "In Austria, Russia Hopes to Exploit Europe's Divisions," *Stratfor,* June 23, 2014, 1, accessed February 15, 2019, https://worldview.stratfor.com/article/austria-russia-hopes-exploit-europes-divisions.

[29] Conley et al., *The Kremlin Playbook 2: The Enablers*, 52.

[30] "Changes in the Management Board of Sberbank Europe Group," Sberbank Europe AG, May 23, 2018, https://www.sberbank.at/press-releases/changes-management-board-sberbank-europe-group.

[31] Wolf concurrently chairs the board of directors at Russian Machines Corporation, a Russian industrial and engineering conglomerate owned by the Russian oligarch Oleg Deripaska. Wolf's business ventures have garnered him political connections in Austria; from 2014 to 2015 he served as the chairman of the supervisory board of the Austrian industry-holding stock corporation (Österreichische Industrieholding AG [ÖIAG], now known as Austrian Investment AG, *Österreichische Beteiligungs AG* [ÖBAG]), which owns 31.5 percent of OMV; Weidinger et al., *Russian Connections of the Austrian Far-Right*, 24; Miriam Widman, "Austria Shields Russian Banks from E.U. Sanctions," *Handelsblatt Today* (Handelsblatt Media Group GmbH & Co. KG, July 31, 2014), https://www.handelsblatt.com/today/companies/alpine-exemptions-austria-shields-russian-banks-from-e-u-sanctions/23612486.html?ticket=ST-21165017-5Br16PT464DAINz1LHqi-ap5; "Shareholder Structure," OMV Group (OMV Aktiengesellschaft), accessed October 23, 2019, https://www.omv.com/en/shareholder-structure.

[32] Zolotov, *Russisch-Österreichisches Wirtschaftsforum: Es Geht Wieder Aufwärts*.

[33] "Austrian Branch," VTB Bank, December 22, 2017, accessed March 25, 2019, https://www.vtb.eu/en/about/page/austrian-branch.

[34] Widman, *Austria Shields Russian Banks from E.U. Sanctions*.

[35] Conley et al., *The Kremlin Playbook 2*, 4.

[36] Conley et al., *The Kremlin Playbook 2*, 51.

[37] Austria, Bundesministerium für Nachhaltigkeit und Tourismus, *Energie in Österreich 2018: Zahlen, Daten, Fakten,* 2018, 34, accessed May 8, 2019, file:///home/chronos/u-697eb88a146fa1a7bbc1f30950a9dd48ef3eaa5a/Downloads/Energie_in_OE2018_Barrierefrei.pdf.
[38] The other ten member states were Bulgaria, Czech Republic, Estonia, Latvia, Hungary, Poland, Romania, Slovenia, Slovakia, and Finland; "EU Imports of Energy Products: Recent Developments," Eurostat: Statistics Explained, November 19, 2018, 8, accessed February 15, 2019, https://ec.europa.eu/eurostat/statistics-explained/pdfscache/46126.pdf.
[39] The others are ENGIE (France), Royal Dutch Shell (Netherlands and United Kingdom), Uniper (Germany), and Wintershall Dea (Germany); "Shareholder and Financial Investors," Nord Stream 2: Committed, Reliable, Safe, https://www.nord-stream2.com/company/shareholder-and-financial-investors/.
[40] "Nord Stream 2: A New Export Gas Pipeline Running From Russia to Europe Across the Baltic Sea," Gazprom, accessed March 18, 2019, http://www.gazprom.com/projects/nord-stream2/

[41] Agata £oskot-Strachota, Rafa³ Bajczuk, and Szymon Kardaœ, *Nord Stream 2 Divides the West* (Centre for Eastern Studies [OSW], June 18, 2018), https://www.osw.waw.pl/en/publikacje/osw-commentary/2018-06-18/nord-stream-2-divides-west.
[42] Timothy Gardner and Patricia Zengerle, "Senate Panel Backs Nord Stream 2 Pipeline Sanctions Bill," *Reuters*, July 31, 2019, https://www.reuters.com/article/us-usa-senate-nord-stream-2/senate-panel-backs-nord-stream-2-pipeline-sanctions-bill-idUSKCN1UQ22D.
[43] Malek and Luif, *Austria*, 10.
[44] "Austria," European Values Center for Security Policy, https://www.europeanvalues.net/austria/.
[45] "Putin's Move: South Stream to Austria," *Institute of Energy for South-East Europe (IENE)*, May 2, 2014, https://www.iene.eu/putins-move-south-stream-to-austria-p597.html.
[46] Conley et al., *The Kremlin Playbook 2*, 51.
[47] Conley et al., *The Kremlin Playbook 2*, 51.
[48] Andrea Hodoschek. "Excitement About Fifth Board at OMV," *Kurier*, September 4, 2019, https://kurier.at/wirtschaft/aufregung-um-fuenften-vorstand-bei-der-omv/400596578.
[49] Hodoschek, *Excitement About Fifth Board at OMV*.
[50] Lukoil is Russia's second-largest company; the largest is Gazprom; "Lukoil Wins Russian Corporate Social Responsibility Award," *Russia Business Today*, May 13, 2019, https://russiabusinesstoday.com/economy/lukoil-wins-russian-corporate-social-responsibility-award/.
[51] "Wolfgang Schüssel Soll Im Juni Lukoil-Aufsichtsrat Werden," *Der Standard*, March 7, 2019, https://www.derstandard.at/story/2000099126750/wolfgang-schuessel-soll-im-juni-lukoil-aufsichtsrat-werden.
[52] "Lukoil Invests in Its Vienna Hub for Foreign Business," January 24, 2018, https://investinaustria.at/en/news/2018/01/lukoil.php.
[53] Conley et al., *The Kremlin Playbook 2*, 21.
[54] Corporatism is defined by *Merriam-Webster Dictionary* as "the organization of a society into industrial and professional corporations serving as organs of political representation and exercising control over persons and activities within their jurisdiction," *Merriam-Webster Dictionary* (Springfield, MA: G&C Merriam), "Corporatism," accessed May 6, 2019, https://www.merriam-webster.com/dictionary/corporatism.
[55] Conley et al., *The Kremlin Playbook 2*, 48-49.
[56] Invest in Austria (ABA), *Taxes in Austria: Corporate Taxation of Companies*.
[57] Makarov and Morozkina, *Regional Dimension of Foreign Direct Investment in Russia*, 9.
[58] Since 1945 there has been a balancing in Austrian politics between the two major political parties, the center-left Social Democratic Party (SPÖ) and the Austrian People's Party (ÖVP). Apart from the periods of 1966-1986, 2000-2006, and 2017 to present, the SPÖ and ÖVP have governed Austria as coalition partners, also known as the "Grand Coalition"; Anton Pelinka, "How Austrian Politics Went From Over-Stability to Unpredictability," *World Politics Review*, July 13, 2017, 1-3, accessed May 15, 2019, https://www.worldpoliticsreview.com/articles/22697/how-austrian-politics-went-from-over-stability-to-unpredictability.
[59] Franz-Stefan Gady, "Corruption and Collusion Can't Stop Austria's Far-Right," *Foreign Policy*, May 23, 2019, https://foreignpolicy.com/2019/05/23/corruption-and-collusion-cant-stop-austrias-far-right/; "Freedom in the World 2001: Austria," Freedom House, accessed October 9, 2019, https://freedomhouse.org/report/freedom-world/2001/austria.
[60] Notable examples include the Buwog Affair, in which former Austrian Minister of Finance Karl-Heinz Grasser reportedly embezzled over 1.5 million Euros from the Austrian tax system while in office; the Telekom Affair, in which bribes were paid to two FPÖ politicians to provide benefits to the company Telekom Austria (among other things); and the "Cash for Laws" Scandal in which former Austrian Minister of the Interior, and then-member of the European Parliament, Ernst Strasser was one of three European Parliamentarians who were caught offering to urge the passage of legal amendments in exchange for large sums of money by (what turned out to be fake) lobbyists; Markus Salzmann, "Corruption Scandals Rock Austrian Politics," World Socialist Web Site (International Committee of the Fourth International (ICFI), August 17, 2012), https://www.wsws.org/en/articles/2012/08/aust-a17.html.
[61] Over the last two decades the two parties of the Grand Coalition have been steadily losing popularity at the polls and their relationship with one another has become increasingly tense. Thus, the Proporz system, which was also weakening because it was considered outdated, has gradually subsided; Kurt Richard Luther, "The Revival of the Radical Right: The Austrian Parliamentary Election of 2008," *West European Politics* 32, no. 5 (August 12, 2009): 1050, accessed May 15, 2019.
[62] Since the Grand Coalition was in power for the majority of the years since 1945, the social partner interest groups and chambers have historically been dominated by these two political parties. When the FPÖ came to power, it tried to oust members of the SPÖ from some positions, to replace them with its own party members; Pelinka, *How Austrian Politics Went from Over-Stability to Unpredictability*, 1-3.
[63] Historically, trade unions are largely connected to the SPÖ, and employers' associations, agriculture, and commerce are dominated by the ÖVP; other political groups are largely excluded from decision-making in these fields. Education, foreign policy, and civil law fall outside of the social partnership.; Ewald Nowotny, *The Austrian Social Partnership and Democracy* (Minneapolis:

University of Minnesota, Center for Austrian Studies, 1993), 13-16.
[64] "The Social Partnership," Austrian Embassy, Washington, DC, Austrian Ministry of Foreign Affairs (BMEIA), accessed September 1, 2019, https://www.austria.org/the-social-partnership.
[65] "Freedom in the World 2019: Austria," Freedom House, accessed October 9, 2019, https://freedomhouse.org/report/freedom-world/2001/austria.
[66] "Freedom in the World 2019: Austria," Freedom House.
[67] Kristine Berzina, "Foreign Funding Threats to the EU's 2019 Elections," The German Marshall Fund of the United States: Alliance for Securing Democracy, October 9, 2018, http://www.gmfus.org/blog/2018/10/09/foreign-funding-threats-eus-2019-elections.
[68] Following the incident (now referred to as the Ibiza Scandal), all FPÖ ministers resigned from the federal government, and Chancellor Sebastian Kurz was ousted with a vote of no-confidence from the Austrian Parliament. Kurz was reelected in the September 2019 election, and chose the Green Party as his coalition partner; *Der Spiegel* Staff, *The Strache Recordings*; Hasnain Kazim, "Kurz Ist Am Ende – Und Steht Schon Vorm Comeback," *Der Spiegel*, May 27, 2019, accessed May 28, 2019, https://www.spiegel.de/politik/ausland/oesterreich-sebastian-kurz-ist-am-ende-und-steht-vor-dem-comeback-a-1269607.html.
[69] The person or organization behind the set-up is not known for certain. On May 22, 2019, a Viennese lawyer named Ramin Mirfakhrai admitted to having commissioned the video, but would not reveal any others involved. There remains public skepticism surrounding the true organizer of the video; Paul Ronzheimer, "Wiener Anwalt Gesteht: Ich Stecke Hinter Dem Strache-Video Sein Angebliches Motiv: 'Zivilgesellschaftlich Motiviertes Projekt'," *Bild*, May 24, 2019, https://www.bild.de/politik/ausland/politik-ausland/oesterreich-nach-video-mit-strache-fpoe-gestaendnis-eines-beteiligten-anwalts-62164764.bild.html.
[70] FATF (2016), *Anti-money laundering and counter-terrorist financing measures – Austria*, Fourth Round Mutual Evaluation Report (Paris, FATF, 2016), 8, www.fatf-gafi.org/publications/mutualevaluations/documents/mer-austria-2016.html.
[71] Organized Crime and Corruption Reporting Project, "Laundromat. Where Did the Money Go? Handelsgericht Wien," OCCRP, accessed October 23, 2019, https://www.occrp.org/en/laundromat/profiles/handelsgericht-wien.
[72] "Troika Laundromat," Organized Crime and Corruption Reporting Project (OCCRP), accessed October 11, 2019, https://cdn.occrp.org/projects/kremlins-laundromat/#/overview/companies.
[73] Ukios Bankas went bankrupt and was closed in 2013; Michael Nikbakhsh and Christoph Zotter, "[Exklusiv] Die Akte Erich Rebasso: Protokoll Einer Unglaublichen Affäre," *Profil*, March 4, 2019, https://www.profil.at/wirtschaft/akte-rebasso-10671153.
[74] Michael Nikbakhsh and Christoph Zotter, "Die Ukio-Spuren Nach Wien: 'Wir Nehmen Ihre Anfrage Ernst'," *Profil*, March 4, 2019, https://www.profil.at/wirtschaft/ukio-spuren-wien-wir-ihre-anfrage-10671613.
[75] Conley et al., *The Kremlin Playbook 2*, 20.
[76] Magdalena Reinberg-Leibel, *Lobbying in Austria: In Whose Interest? What Are We Allowed to Know?* (Transparency International: Austrian Chapter, and the Prevention of and Fight against Crime Programme of the European Union, December 2014), 2.
[77] Gustav Gressel, "Austria: Russia's Trojan Horse?" European Council on Foreign Relations, December 21, 2017, accessed February 15, 2019, https://www.ecfr.eu/article/commentary_austria_russias_trojan_horse.
[78] The FPÖ controlled the following ministries and positions during this time: Defense, Foreign Affairs, Interior, Labor and Health, Sport, Transport, State Secretary and Federal Minister for Finance, and the Vice Chancellorship; Anita Bodlos and Carolina Plescia, "The 2017 Austrian Snap Election: A Shift Rightward," *West European Politics* 41, no. 6 (February 7, 2018): 1360, accessed May 15, 2019.
[79] Prior to this, Austria's far right (including the FPÖ) was staunchly anti-Russian, due to Russia's treatment of the Nazis during and after the Second World War. The FPÖ was initially founded by former national socialists; Péter Krekó, Lóránt Gyõri, and Edit Zgut, *From Russia with Hate: The Activity of Pro-Russian Extremist Groups in Central-Eastern Europe* (Budapest: Political Capital Policy Research and Consulting Institute, 2017), 36, accessed October 10, 2019, https://www.politicalcapital.hu/pc-admin/source/documents/PC_NED_summary_analysis_EN_20170428.pdf.
[80] Kneissl has since left politics. However, in May 2020 she published a guest commentary on the Russian news outlet RT, a news station sharply criticized by the international media for being a pro-Kremlin propaganda network. Kneissl has indicated she does not intend to write a regular column for RT, but will continue to publish pieces for it on varying topics in the future. Joshua Posaner, "Austrian Foreign Minister under Fire for Putin Wedding Invite," *Politico*, August 18, 2018, accessed March 23, 2019, https://www.politico.eu/article/karin-kneissl-wedding-vladimir-putin-invite-controversy/; "Russischer Sender: Kneissl nun RT-Kolumnisten," *ORF*, May 9, 2020, accessed May 14, 2020, https://orf.at/stories/3165029/.
[81] Weidinger et al., *Russian Connections of the Austrian Far Right*, 5 and 30.
[82] Weidinger et al., *Russian Connections of the Austrian Far Right*, 5 and 60.
[83] Weidinger et al., *Russian Connections of the Austrian Far Right*, 61.
[84] Gressel, *Austria: Russia's Trojan Horse?*
[85] *2018 Ranking of Countermeasures by the EU28 to the Kremlin's Subversion Operations: Kremlin Watch Report* (Prague: European Values Think Tank, 2018), 12, https://www.europeanvalues.net/vyzkum/2018-ranking-countermeasures-eu28-kremlins-subversion-operations/.
[86] Ralph Atkins and Guy Chazan, "Germany Voices Concern Over Sharing Intelligence with Austria," *Financial Times*, March 23, 2018, https://www.ft.com/content/fa60aa00-2e64-11e8-9b4b-bc4b9f08f381.
[87] Krekó et al., *From Russia with Hate*, 36-37.
[88] Anton Shekhovtsov, *Russia and the Western Far Right: Tango Noir* (Abingdon, Oxon, UK, and New York: Routledge, 2018), 173-175.
[89] Weidinger et al., *Russian Connections of the Austrian Far Right*, 14-15.
[90] Conley et al., *The Kremlin Playbook 2*, 28.
[91] Conley et al., *The Kremlin Playbook 2*, 54.
[92] *Wolfgang Schüssel Soll Im Juni Lukoil-Aufsichtsrat Werden*.
[93] European Values Think Tank, *2018 Ranking of Countermeasures by the EU28 to the Kremlin's Subversion Operations*, 17.

[94] Conley et al., *The Kremlin Playbook 2*, 5.
[95] "Structure," Russian Railways, accessed October 19, 2019, http://eng.rzd.ru/statice/public/en/5?STRUCTURE_ID=174.
[96] "Ex-Finanzminister Schelling Berät Gazprom: Beratervertrag für Gaspipeline-Projekt Nord Stream 2," *Der Standard*, March 26, 2018, https://www.derstandard.at/story/2000076853235/ex-finanzminister-schelling-beraet-russischen-energieriesen-gazprom.
[97] Conley et al., *The Kremlin Playbook 2*, 48-49.
[98] Angela Dewan, "These Are All the Countries that Are Expelling Russian Diplomats" (CNN, March 28, 2018), https://www.cnn.com/2018/03/26/europe/full-list-of-russian-diplomats-expelled-over-s-intl/index.html.
[99] During the Cold War, Vienna was a hub for spies, and the city continues to be a popular location for Russian agents. It is estimated there are currently between 2,000 and 3,000 Russian agents and informants operating in Vienna, and experts suggest that at least half of the diplomats working in the capital are spies. Vienna is an attractive location for espionage activities because it houses a variety of international bodies such as the United Nations (UN) and the Organization for Security and Cooperation in Europe (OSCE), and Austria has loose laws governing activities related to espionage. According to Austrian law, "Spying is only a crime if it is directed against the Austrian state"; Sigrun Rottmann, "Vienna Is Still a Favourite Playground for Spies," BBC, July 8, 2010, https://www.bbc.com/news/10553310); European Values Think Tank, *2018 Ranking of Countermeasures by the EU28 to the Kremlin's Subversion Operations*, 16; Conley et al., *The Kremlin Playbook 2*, 50.
[100] In June 2007 Russian national Vladimir Vozhzhov was apprehended for offering an Austrian official and member of the armed forces 20,000 Euros in exchange for classified information but was released 16 days later. In 2011 former KGB official Mikhail Golovatov was detained in Vienna in connection to 14 civilians he shot and killed in Lithuania in 1991. Despite the existence of a European arrest warrant for Golovatov issued in Lithuania, he was released after 22 hours. In November 2018 the Austrian government began to investigate an Austrian army colonel suspected of spying for Russia from the 1990s to 2018. Although Chancellor Kurz expressed concern about the situation, at the time of writing no further information was available regarding this case; Malek and Luif, *Austria*, 16; Francois Murphy, "Austrian Colonel Spied for Russia for Decades, Vienna Says," *Reuters*, November 9, 2018, https://www.reuters.com/article/us-austria-russia-spy/austrian-colonel-spied-for-russia-for-decades-vienna-says-idUSKCN1NE0SH.
[101] Malek and Luif, *Austria*, 19.
[102] Franz-Stefan Gady, "Not All Russia-Friendly Policies Are Nefarious," *Foreign Policy*, March 30, 2018, accessed March 25, 2019, https://foreignpolicy.com/2018/03/30/not-all-russia-friendly-policies-are-nefarious/.
[103] "Leitl: Sanktionen Gegen Russland Sind 'Unsinnig'," *Kleine Zeitung*, April 3, 2016, https://www.kleinezeitung.at/wirtschaft/4958981/WKPraesident_Leitl_Sanktionen-gegen-Russland-sind-unsinnig; Weidinger et al., *Russian Connections of the Austrian Far Right*, 22-23.
[104] Lóránt Gyõri, Péter Krekó, Jakub Janda, and Bernhard Weidinger, *Does Russia Interfere in Czech, Austrian and Hungarian Elections?* (Budapest: Political Capital, European Values think tank in cooperation with Dokumentationsarchiv des Österreichischen Widerstandes, 2017), 11.
[105] Conley et al., *The Kremlin Playbook 2*, 20.
[106] Shekhovtsov, *Russia and the Western Far Right*, 75.
[107] European Values, *2018 Ranking of Countermeasures by the EU28 to the Kremlin's Subversion Operations*, 9.
[108] European Values, *2018 Ranking of Countermeasures by the EU28 to the Kremlin's Subversion Operations*, 9.
[109] Malek and Luif, *Austria*, 18.
[110] Malek and Luif, *Austria*, 13.
[111] Krekó et al., *From Russia with Hate*, 16.
[112] Malek and Luif, *Austria*, 18.
[113] There were many limitations to the collection of voting records of individual MEPs on Russia-related resolutions in the European Parliament. The majority of the resolutions in the European Parliament are decided on by a show of hands. If there is a clear majority, the item either passes or fails. If the number of votes for each option appears close, a roll-call vote or electronic vote is used. Votes of individual MEPs are only recorded if a roll-call vote or electronic vote is utilized. Therefore, data was not available on all Russia-related resolutions voted on in the European Parliament, just those that utilized roll-call or electronic votes. This limited the information available to make a full assessment of MEP's voting patterns to best conduct the statistical analyses in this research; "How Do MEPs Vote? Parliament's Rules of Procedure," European Parliament (August 24, 2009), https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT IM-PRESS 20060628STO09319 0 DOC XML V0//EN).
[114] "MEPs European Parliament," European Parliament, accessed November 29, 2019, http://www.europarl.europa.eu/meps/en/search/advanced).

Julia Girardi is a recent graduate of the Daniel Morgan Graduate School of National Security with an MA in National Security. Her main research interests include European security issues and Russian foreign policy. She has a particular interest in Austrian culture and politics stemming from the three years she lived there, which inspired this research topic. This article is an abbreviated version of her master's thesis titled "Russian Influence in Austria and Its Impact on the EU: An Analysis." Julia lives and works in Washington, DC, as an analyst at a management consulting firm.

Non-Democracies Prone to All Forms of Terrorism

by Sara Harmouch

INTRODUCTION

Suicide terrorism destroys the safety of civilian spaces, in addition to the terrorist and his/her victims. This tool is a strategy of coercion, a method to compel a target government to alter its policy. It is a virulent weapon that can throw thousands of people into a panic. The increase in the use of suicide terrorism by terrorist groups is due, at least in part, to the perception that it is an effective way to achieve goals at a low cost.[1] Terrorist organizations use violence as a mean to an end. Such groups are unable to attain, or do not believe they can attain, their goals through peaceful means, and thus must resort to more violent tactics.[2] When facing a choice between giving up and shifting to a more extreme tactic, they choose the latter. Any group's level of political power defines and may limit the number of potential options it may use, and groups with little political power may be reduced to extreme tactics. The use of violent tactics to achieve their goals may find it most pragmatic to strike a blow where it can cause disproportionately high levels of damage. According to Robert Pape, suicide terrorism is one of the most belligerent forms of terrorism; the attacker uses this method to cause mass casualties beyond the main target, and at the expense of not surviving.[3]

Suicide terrorism is an offensive tactic in which success depends upon the death of the perpetrator and the number of people killed. Suicide terrorism, similar to other tactics used in terrorism, has strategic, tactical, and operational objectives. According to Mia Bloom, suicide terrorism is used to achieve and further the agenda of terrorist groups through the heavy-handed counter-terror strategies.[4] It fosters a sense of powerlessness within the targeted society. Suicide terrorism gains popularity when nation-states deploy harsh military tactics, in part because of the high casualty rate associated with such attacks. Pape comments that "violent organizations chose suicide attacks from among a variety of tactical options in order to achieve certain strategic, tactical, and operational goals."[5] In addition, suicide terrorism is intended to cause more anxiety, fear, and a sense of helplessness with its high lethality.

Suicide terrorism is used in order to gain public support for the terrorist cause and sometimes is conducted to create chaos in a specific area, so that the larger group may gain an advantage in other areas. Suicide terrorism is used to get a quicker, harsher, and more aggressive response from the government being targeted. Terrorists use suicide terrorism as a tactic to fulfill their short-term and long-term goals. They aim at getting nation-states to initiate quick responses, or to retaliate aggressively and harshly with a high level of audience cost which guarantees a larger number of civilian deaths (and may cause public empathy with their cause). "Suicide terrorism is also, or even more, attractive because it enhances an organization's prestige and gives it an advantage in intra-movement competition by attracting recruits, publicity, and money."[6] The goals of terrorist groups who use suicide terrorism tactically may be best achieved in non-democracies.

Suicide terrorism is often used to remove foreign occupation, obtain national independence, destabilize or replace a political regime, intensify violence in a conflict already occurring, or interrupt a peace process.[7] Suicide terrorists often want to achieve larger strategic goals that are not limited to removal of foreign occupation. The use of coercion through suicide terrorism is as effective in non-democracies as in democracies.

The conventional wisdom argues that suicide terrorism is a phenomenon that targets democracies because they are willing to alter policies due to democratic values such as the preservation of human rights or the popular vote. Hence, they are compelled to give in to the demands of terrorists.[8] Although a consensus in terrorism literature[9] has developed that democracies are primarily targeted because they are easily coerced, I challenge this argument. I argue that non-democracies may be more prone to suicide terrorism due to many reasons, such as they respond to terrorists in the exact way terrorists want them to respond, leading terrorists to achieve their short-term and long-term goals. Due to the characteristics of non-democracies, it makes it easier for terrorists to target them.

This study is a qualitative comparative case study that analyzes regime types and their impact on terrorism. I argue that suicide terrorism is more likely to occur and coerce non-democracies. This study proceeds as follows: (1) It discusses the definition of coercion; (2) it highlights the response of regime types to suicide terrorism; and (3) it examines two cases of non-democracies that were coerced by suicide attacks: Russia and the Chechens, and Turkey and the Kurdish Workers Party. I conclude with a statement that confirms my argument that non- democracies may be prone to terrorism, specifically suicide terrorism.

DEFINITION OF COERCION

Suicide terrorism is likely to coerce non-democratic regimes; however, this requires a more nuanced definition of coercion.[10] Coercion is used for much more than forcing compliance with the short-term demands or goals of the terrorist groups; rather, it is done in pursuit of their longer-term and much larger strategic goals, such as aiming to kill the maximum number of civilians. As noted by former Director of Central Intelligence James Woolsey, "Today's terrorists don't want a seat at the table; they want to destroy the table and everyone sitting at it."[11] Terrorists seek more violence, damage, and a high number of civilian casualties in order to spread fear and provoke any government to retaliate with violence. Other larger strategic goals can include getting nation-states embroiled in long costly wars that drain the state's financial and military resources, or heavy-handed retaliation by the nation-states in order to evoke public support for, and perhaps recruitment to, the terrorists' cause. "If the government responds to terrorist activity by imposing repressive measures not only affecting the terrorist organization but also the general population, proactive measures may increase popular sympathy for the grievances expressed by terrorist groups and could even further terrorist recruitment."[12]

Coercion can be used as a tool in getting an adversary to change its behavior; we can define coercion in many ways. For example, terrorist groups have immediate goals such as being granted autonomy, compelling the departure of foreign occupation and spreading fear, but terrorists can also have other goals that are not immediate, such as engaging an adversary in a costly, drawn-out war. In the case of 9/11, Osama bin Laden said that he wanted to get the U.S. embroiled in a war. Terrorist goals can include adopting costly counterterrorism measures that lead to high civilian casualties and the violation of human rights, as well as potentially gaining legitimacy and recognition.

The conventional wisdom argues that democracies are the targets of suicide terrorism because they can be coerced.[13] I challenge this. Instead, I argue that non-democracies can be coerced by suicide terrorism. In certain cases, a terrorist group wants its adversaries to retaliate harshly, to start costly wars, to respond quickly to its acts, and to negotiate with it. Non-democratic countries are in some cases more likely to engage in such behavior. In contrast, democracies are constrained, there are limits to their retaliation, willingness to go to war, longer time to respond and to negotiate. Non-democracies are more likely to engage in a way that furthers terrorists' agendas.[14]

RESPONSES TO SUICIDE ATTACKS

Democratic Responses to Terrorism

Terrorist groups aim at getting nation-states embroiled in costly and bloody wars. Democracies are less likely to get involved in costly wars. As Reiter and Stam put it, "Because democratic executives know they risk ouster if they lead their state to defeat, they will be especially unwilling to launch risky military ventures. In contrast, autocratic leaders know that defeat in war is unlikely to threaten their hold on power. As a result, they will be more willing to initiate risky wars that democracies avoid."[15] Democracies require the consent of their citizens to pass policies and their domestic populace will usually constrain their leaders from entering a war because it is costly in human terms. Domestic politics play a major role in which democracies are beholden to their public. "This combination of ease of removal in democracies and the likelihood that policy failure in the form of losing the war will turn the public against the leader and increase the likelihood that he or she will suffer defeat in the next election induces a healthy dose of caution in democratic elites."[16] As a result, democracies are not likely to get involved in costly wars.

Democracies cannot respond harshly, and they typically cannot afford to be seen violating human rights. They promote civil liberties and have high audience costs which limit them from overreacting to a terrorist's provocation.[17] They are beholden to their populace because they want to be re-elected and they will not risk a heavy-handed retaliation. Accountability to voters limits democracies on how to respond to attacks. Responding to attacks harshly costs the lives of many people and is a financial burden. The removal of leaders in democracies in case of policy failure and public backlash against the leader make it possible that he or she will not be re-elected. This usually keeps the leader in check and requires extensive cost-benefit analysis in democracies.[18] The aim of terrorist groups is to provoke the state, to urge a response from democracies.

Most democracies have a long decision-making process to respond to these attacks, which is slower and much more difficult than that in non-democracies. In democracies, the process of decision-making is typically conducted with fairness and equitability. There are often pre-existing rules

and procedures to follow that allow the policies to be formed. There is no one individual person responsible for the decision-making; rather, the decision is made by a representative of the public. Getting a group together and hoping the majority agrees on an issue cannot only be challenging but is a slow and lengthy process requiring consensus and majority vote. Democracies have more than one body to consult on a way to respond; for example, in the United States, the Congress must approve bills and pass legislation, which takes time. It may be a lengthy process to pass new legislation and require even more time for decisions to be put in place. Thus, in general, democracies have more limitations on their counterterrorism options than non-democratic countries, which are not bound by such concerns.[19]

Negotiating with terrorist groups is not usually an option that democracies exercise. Negotiating with a terrorist group allows the terrorists to gain recognition and legitimize their cause. In 2003, for example, U.S. President George W. Bush declared: "You've got to be strong, not weak. The only way to deal with these people is to bring them to justice. You can't talk to them. You can't negotiate with them."[20] Democracies usually are not willing to negotiate with terrorists, and thus legitimize them, making them a harder target for coercion, but some democracies do and that can be a problem. For democracies to agree to negotiate with terrorists is to give them legitimacy and a place at the table. "Talking to them would serve only to incite more violence and weaken the fabric of democratic states, they argue."[21] Many terrorist groups want legitimacy, especially if their strategic long-term goal is to be recognized by the state or achieve some type of representation. Walter Laqueur claims compromising with terrorists gives "full recognition to terrorist groups" that leads to increased attacks.[22] The argument against negotiating with terrorists is simple. Neumann argues that negotiations give legitimacy to terrorists.[23] Negotiating with terrorists is often seen as legitimizing the terrorists, their goals, and their means. Democracies will not undermine themselves and their domestic populace and agree to negotiate with terrorists nor give them legitimacy, which makes democracies less vulnerable to coercion.[24] Many democratic countries refuse to talk to terrorists, making it difficult for these groups to accomplish their purpose. "Similarly, Kenneth Hicks (1991) argued that U.S. designation of terrorist groups under the Reagan and first Bush administration placed severe limitations on the range of U.S. response to such attacks, encouraging the use of military force while imposing strong disincentives on negotiation."[25]

Democratic countries are often unwilling to make any changes in their policies to accommodate terrorist groups, unlike non-democratic countries which are willing to concede and make policy concessions.[26] "Although suicide terrorism occasionally compels democratic countries to prematurely end their foreign occupations, which holds true in the case of al-Qaeda, the terrorist group's efforts to kill many Americans was to drive the United States and its allies from the Arabian Peninsula and other Muslim countries. It has been powerless to change democratic countries' ideology or borders.[27] Targeting democracies does not work in achieving long-term strategic goals of terrorist groups such as coercing the country into policy change, or territorial inquiry, or even negotiating with them; however, non-democracies fit all the criteria that would further terrorists' agendas. Non-democracies are more vulnerable to coercion than democracies.

Non-Democratic Response to Terrorism

"In fact, terrorists were more than five times as likely to achieve their policy objectives against non-democratic countries. The number (percent) of countries successfully coerced was 11 (55 percent) versus 2 (10 percent) for the non-democratic and democratic regime types respectively (P = 0.006)."[28] Terrorist groups using suicide terrorism as a tactic aim at killing as many people as possible, and that is a strategic goal of terrorist groups, yet it is best achieved in a regime type where there is a fast decision-making process. In a non-democracy, decisions are typically made solely by one individual, the dictator, or within a small tightly-linked group, and the government can respond to terrorist with attacks and bombings harshly without considering the death of its own civilians or the violation of human rights as it is seen in Assad's Syria. Additionally, the government has no problem with negotiating with terrorist groups as it lacks any democratic value (thereby giving them power and legitimacy).

"Non-democratic" had on average more than twice as many incidents and six times as many fatalities as "democratic countries as categorized by Freedom House metrics.[29] Most non-democratic countries do not have a legislative body to consult and therefore can respond quickly. They do not have a long decision-making process, nor do they have to wait for Congress' approval to move forward. Dictators act directly, quickly, and belligerently. Non-democracies do not need to seek approval or oversight from a large governing body, but rather only from a dictator and can respond to terrorist attacks more quickly and harshly.[30]

Terrorists are more likely to expect a response from non-democracies that generate domestic audience costs. Non-democratic countries have no commitment to civil liberties, allowing a greater opportunity for suicide terrorists to achieve their goals, whether those goals are killing civilians or getting state support for their group. Non-democracies are not as responsible as democratic countries to their populace, and they are willing to go far and beyond to achieve their

goals and portray themselves as strong. Thus they are ready to get involved in costly wars and even initiate them to project their authority and oppression. "The WITS [World Integrated Trade Solution] data suggest that the world's most non-democratic countries are the victims of a disproportionate number of terrorist incidents and fatalities."[31]

Moreover, non-democratic countries can be voted out of office or overthrown. Thus, dictators make sure to play within the dynamics that advances terrorist groups' aims in retaliating harshly in a way that ensures the death of many civilians. Non-democracies tend to respond harshly to ensure they are the strongest and cannot be defeated or replaced by other groups. In that way, they eliminate any competition within their own political realm, and they accomplish what terrorists want: the death of many people.

Non-democratic countries have more leeway to increase the level of violence, thus making them an easy target for coercion. For example, the Russian public was in favor of appeasing the Chechens and granting them an independent Chechen state. However, when terrorism erupted in the 1990s and the acts of the Chechens were apparently bent on harming it, shifting popular support away from concessions, Putin instead bombed Grozny.[32] This amply reflects that Russia, being a non-democratic country, was willing to use violence and retaliate harshly because it was not beholden to its domestic populace. "The cases suggest that heavy-handed counter-terror strategies might appear effective in the short term; however over time, such strategies will inculcate a greater sense of outrage and anger, making a formerly inhospitable environment accepting and approving of mounting violence against civilians. This appears to be the trend in Israel and in Chechnya."[33] Non-democratic countries are vulnerable to coercion more than democracies. "Examples of partial success include al-Qaeda's attacks on Poland and Bulgaria since these two countries in 2004 announced their intent to significantly reduce their troop presence in Iraq."[34]

Leaders of non-democratic states are typically not beholden to public opinion and they have no problem negotiating with terrorists, which serves the larger strategic goals of terrorist groups in wanting a seat at the negotiating table. For example, Turkey has not conceded to the Kurdish Workers Party, but it sat with its representatives around the same table to negotiate, which suggests that it conceded at a certain level. Non-democratic countries can be coerced into changing their ideological position or conceding some territorial areas for some minority groups residing in the country due to their non-democratic nature. For example, Iraqi Kurds were able to hold an independence referendum in Iraq. Iraq is not a strong democracy. "Even during the height of Saddam Hussein's dictatorship in the 1980s, the Kurdish Iraqi Democratic Front managed to carry out dozens of attacks inside Iraq. Indeed, high-value targets exist even in the most illiberal countries."[35] All these aspects and features of non-democracies make them engage in a way that serves terrorist groups' larger strategic goals.

NON-DEMOCRACIES IN RUSSIA AND TURKEY

The strategic long-term objectives of many terrorist groups are forcing countries to concede some of their policies, killing as many civilians as possible, acquiring territorial areas, and having a seat at the negotiating table. In "Deterring Terrorism: A New Strategy," Max Abrahms points out that "in the rare cases where targets are effectively hard to coerce or will not fit the criteria they want, terrorists simply move on to softer targets which means non-democracies."[36] The characteristics of non-democracies make them vulnerable to effectively playing into terrorist groups' overall goals, which is a contrast with the argument pervading the terrorism literature regarding the coercion of democracies, as defined by Pape. Russia and Turkey are defined by Freedom House as "partially free," which means they are only partially democracies and do not qualify fully as democracies. The appearance of a democracy does not actually create one. I challenge this designation in two ways. First, Russia and Turkey are non-democracies. Second, non-democratic characteristics have enabled both countries to respond in such ways that advanced terrorist groups' agendas. In this section, I argue that Russia and Turkey are non-democracies and the way they have responded to suicide terrorism fulfills terrorists' goals in various ways.

Methodology and Indicators of Democracy

Democracy exists as a civil structure that permits individual freedom of expression as well as self-determination, granting to its citizens an equal platform, regardless of identity. Democracies encourage the people and government to participate and cooperate, in order to continue free expression and self-determination. A democracy is a state in which citizens vote to choose the best candidate. It is a political system for choosing a government through free and fair elections; it is the active participation of the people, as citizens, in politics and civic life.[37]

Moreover, democracy focuses on the protection of human rights of all citizens and laws that are equally applied to all citizens.[38] To prove that Russia and Turkey are non-democracies I will be using a definition of democracy from a combination of the World Bank's government index by Kaufmann-Kraay and the CIRI Human Rights Data Project that records each country's commitment to human rights, such as women's rights, civil liberties, and state oppression.

Democracy will be measured as follows: voice and accountability, the extent to which a country's citizens are able to participate in selecting their government (free and fair elections), as well as freedom of expression, freedom of association, and free media.[39] Political stability and absence of violence reflect perceptions of the likelihood that the government will not be destabilized or overthrown by unconstitutional or violent means, including political violence and terrorism, rule of law and corruption.[40] The definition adds human rights violations that measures the extent a government violates or respects the rights of its citizens and the level of audience cost each government possesses.[41]

Using the aforementioned definitions for democracy, I use the indicators of democracy in a comparative qualitative analysis of government types to prove the case of Russia as a non-democracy with the Chechens and Turkey as a non-democracy with the Kurdish Workers Party. I refrain from using three measures: Freedom House's index of liberal democracy, the Polity IV project's assessment of constitutional democracy, and Przeworski et al.'s classification. These measures ignore some classifications of democracies and hence are contested. Freedom House ignores the classifications of human rights, which are essential components to measure democracy. Polity IV highlights the presence of limitations upon the chief executive as a central element of its measures and, although it underlines the importance of civil liberties, it does not actually venture to measure this aspect. Finally, Przeworski defines democratic states in terms of the populace having the power to replace its government through elections. Countries are considered autocracies if they fill the seat of the chief executive through inheritance or patronage rather than by popular elections, such as in Syria. It focuses on competitiveness of parties, yet there is no best way to calculate that. Moreover, while this assessment is parsimonious, it overlooks many other elements of paramount significance. Therefore, these three measures represent bleak definitions for democracy indicators and also, by themselves, they lack some aspects. Hence, I refrain from using them.

Russia and Its Non-Democratic Actions with the Chechens

Russia was classified as a democracy by Freedom House, but according to the definition provided above Russia is considered as a non-democracy and definitely acts like one. Russia's many undemocratic practices render its classification as a democracy problematic. "If both Chechen suicide attacks and Russia's non-democratic trend continue, Russia may well become the first clearly non-democratic state to face suicide terrorism."[42] Russia is a non-democracy based on the definition provided. Pape uses Freedom House as his one indicator of democracy, which stands mostly on free and fair elections. Free and fair elections do not make a country democratic or non-democratic; there are other aspects of democracy that need to be fulfilled. Freedom House ranked Russia as "partly free," which does not qualify it to be a democracy or deserve that label. An almost-democracy is not a democracy. According to the World Bank index, Russia had scored 44 percent in 1996 but decreased to 15 percent in 2016 on voice and accountability, which means it does not provide its citizens with all of their freedom of speech rights. In addition, it scored low on political stability, absence of violence, and rule of law. On the latter, it scored 25 percent in 1996, which decreased to 21 percent in 2016. Russia has not acted like a democracy, and it also scores high on corruption. Moreover, in the CIRI Human Rights Data, Russia scores a 0 out of 2, demonstrating that the government has complete control over the media and freedom of expression is limited. There are also many human rights violations. These indicators all reflect that Russia is not a democracy and instead is a non-democratic country. Now, having established Russia's government type, we can discuss the Chechen case and suicide terrorism.

Russia has long been in a conflict with its Chechen minority group that has been seeking an independent Chechnya. This conflict has lasted three centuries and has led Chechens to resort to suicide terrorism as a tactic to achieve their short-term and long-term strategic goals. This struggle began in 1785 and continues with a theme of harsh measures, marked by inhumane policies and acts that have fomented extreme resistance. Chechnya was incorporated into Russia after the 1991 dissolution of the Soviet Union, but Russia was working on its own government and left the Chechens to oversee themselves. Chechnya insisted on independence when the Soviet Union fell in 1991.

Russia, a non-democratic regime, has violated human rights, killed many civilians, and responded harshly to the Chechens despite many international treaties that it had signed and ratified. Russia's actions portray a non-democratic regime that acted alone and responded exactly how the Chechens wanted in order to get international sympathy for their cause and to recruit. The second Chechen war was also accompanied by similar brutal atrocities and responses by the Russians. The harsh methods used by Russia had an inverse effect on Russians and solidified the resistance movement by the Chechens (a strategic goal of the Chechens). Its heavy-handedness motivated Chechen resistance. Chechnya struggled in its fight against Russia and was compelled to ally with Islamist foreign fighter terrorist groups that could bolster its tactics and help its cause. This collaboration led to the use of suicide terrorism as a tactic. Chechens used female suicide terrorists as their ultimate tool. This tool helped the spread of trepidation, disruption, and public outcry. "In Chechnya,

suicide bombings have become increasingly frequent since 2000, and their perpetrators are more motivated by revenge, despair, and their drive for an independent state than by religious fundamentalism or individual honor."[43]

Chechen suicide tactics started in 2000 and then increased in frequency. The most destructive attack was in 2003 after a constitutional referendum and the second largest one was in 2000. Many suicide bombers were victims of Russia's counterterrorism strategy. More repression led to more resistance. Russia responded to Chechens with vicious tactics, quick and violently disproportionate violations of human rights, and negotiated with the Chechens giving them legitimacy and equal power (even though these negotiations failed). "Horrendous cruelties were routine: 700 persons were immolated in a locked barn, thousands were shot and dumped in a lake, and the elderly and sick were executed to save the trouble of moving them."[44] These are longtime strategic goals of the Chechens and Russia fell into the trap, responding exactly how the Chechens wanted. "Bloom describes the conditions under which groups chose suicide terrorism as a 'complexity of motivations,' defining it as 'contingent violence,' in which the next act is shaped by the reactions of the target audience. Major factors in the use of ST [suicide terrorism] are foundational decision-making, conducive circumstances, and intended outcomes."[45]

The Chechens stooped to suicide terrorism as a tactic to achieve their strategic goals. During the second Chechen war, on October 23, 2002, about 40 terrorists, including 19 women, stormed into a theater and took 1,000 hostages. These terrorists all wore suicide belts. Chechen demands were for Russia to vacate Chechnya; however, Russia responded by releasing unidentified gas that killed over one hundred hostages. Chechnya's long-term strategic goals were to get support for its cause. The Chechnyans wanted a quick, heavy-handed retaliation to which Russia gave in easily. This resulted in the death of many civilians and the violations of human rights; Chechnya demanded recognition and legitimacy, which it technically received when Russia agreed to negotiate with the Chechens. Russia was coerced by suicide terrorism and helped the Chechens achieve their long-term strategic goals. The Chechen question is still a contentious one and a third war between the two is very plausible. A Russian-installed government that acts as a dictatorship will not be tolerated for long, and Chechnya will not settle into its rejected status and live under the shadow of Russia, similarly to the Kurdish Workers Party (PKK) in Turkey.

Turkey and the Kurdish Workers Party

Robert Pape labeled Turkey as a democracy while making his argument about suicide terrorism using Freedom House databases. Turkey does not behave as a democracy, especially when it violates human rights, kills civilians, undermines the Turkish rule of law, and spreads corruption. The Turkish military undermined the rule of law and committed illegal acts in order to serve its goals. "Highlighting the Turkish military's impunity and its role in undermining the rule of law, the Semdinli prosecutor was removed from his post and his license to practice law was revoked."[46] Under the indicators established in this study using the World Bank's governance index by Kaufmann-Kraay and the CIRI Human Rights Data and in terms of the level of audience cost, Turkey ranks as non-democratic due to its behavior. According to the World Bank Governance Index, on voice and accountability, from 1996 Turkey scored 46 percent, which dropped to 30 percent by 2016. In measurements of political stability and absence of violence and terrorism, Turkey scored 11 percent in 1996, which dropped down to 6 percent in 2016; on rule of law Turkey score 47 percent in 1996 and 49 percent in 2016; and on corruption, Turkey scored 52 percent in 1996 which decreased to 50 percent in 2016.

Thus, Turkey scored low on aspects of democracy and high on non-democratic behavior. Turkey controls many aspects of the media as well as abolishing its people's freedom of speech. Additionally, in the CIRI Human Rights Data, Turkey on a scale of 0-2 scores an average of 0.5 in respecting human rights from free speech and women's rights to civil liberties.[47] Turkey also failed to reform laws stifling free speech. In 2005, the Turkish novelist Orhan Pamuk stated that "30,000 Kurds and a million Armenians were killed in these lands, but nobody dares to talk about it." He was charged with "insulting Turkishness" under Article 301 of the Penal Code.[48] These numbers, compared to those of actual democratic nations, prove that Turkey is a non-democracy.

Therefore, Turkey is a non-democratic country; it has been repressing the Kurds for as long as the Kurds have existed. It is quite possible that if the country had been a democracy, the PKK may not have found it necessary to resort to such tactics. "Turkey's electoral law prohibits parties from being seated in parliament unless they receive more than 10 percent of the national vote. As a result of this undemocratic and counterproductive requirement, no exclusively Kurdish party was ever able to pass the threshold for participation in parliament."[49] The PKK is regarded as a terrorist organization by Turkey, Europe, and the United States. The Kurdish movement organized an insurgency to establish an independent state. "The rebellion was brutally put down and its ringleaders hanged in the central square of Diyarbakir. After a series of uprisings that culminated in another rebellion in 1937, Turkey adopted draconian measures such as denying the very existence of Kurds in Turkey, referring to them only as "Mountain Turks."[50]

Kurdish language, culture and geographical place names were banned."[51] Turkey's strategy was harsh; it only caused the conflict to intensify and galvanize the Kurds.

Turkey has long suppressed the Kurdish identity, language, traditions, and practices. The fight between the PKK and Turkey resulted in around 30,000 casualties by late 1990.[52] The PKK succeeded in gaining substantial public support for its cause, although it has not yet established an independent state. The PKK aimed at spreading fear and causing destructive damage in order to become more powerful, to recruit more supporters, and to prove itself to the Turkish government. "In June 1987, the PKK slaughtered residents in the village of Pinarcik because they were unsympathetic to its cause. Two months later, it killed 24 residents of Kilickaya including 14 children."[53]

The PKK started using suicide terrorism tactics in 1996, and it was responsible for 21 suicide attacks.[54] "The PKK's decision to adopt suicide terrorism came during 1996, as the Turkish government bolstered its possession of conventional armaments and significantly weakened the organization" (Center for Contemporary Conflicts). Turkey responded to the PKK with an iron fist. "These efforts also included political assassination; government-backed death squads killed hundreds of suspected PKK sympathizers. Close to 500 disappeared between 1991 and 1997, and between 1983 and 1994, 230 people—many of them Kurds—died from torture while in police custody."[55] Turkey implemented many strategies that intended to defend the Turkish people, but it had the opposite effect and became a magnet for PKK operations.

Kurds protested peacefully, yet the police dispersed the protests with violence, killing civilians. Turkey responded to the PKK with bombings, airstrikes, and various heavy-handed measures, which led to the PKK gaining substantial international support for its cause. Human Rights Watch and other groups decried Turkey's heavy-handed response, accusing it of excessive use of force. Turkey killed many civilians and violated many human rights leading to a high level of audience costs and a high number of casualties. Moreover, the PKK managed to get Turkey's recognition by negotiating and that gave the PKK legitimacy and equal power. "The PKK wants to gain legitimacy in the eyes of the Turkish State; that is why they are willing to negotiate."[56] Turkey responded quickly, acting by itself, and thus the decision-making process was instant. Turkey, as a non-democracy, was not beholden to its domestic populace, and Turks were scared to show empathy toward the Kurds because police and security forces were killing and condemning Kurdish supporters. "Between 1989 and 1996, more than 1,500 persons affiliated with the Kurdish opposition were victims of unidentified murderers."[57] Turkey was coerced by suicide terrorism and helped the Kurdish people achieve their long-term strategic goals whether it was by gaining legitimacy, escalating the level of violence, the high number of casualties, human rights violations, or gaining support. The Kurdish question remains an issue and the only solution foreseen after this study is the actual process of democratization.

CONCLUSION

Suicide terrorism coerces non-democracies because they can be easier to coerce due to some constraining features of democracy. In some cases, democracies can act similarly to non-democracies if they are led by the wrong people. Democracies typically cannot act in a belligerent way because they are held accountable to their populace; thus, they cannot always respond in a way that can lead to terrorists achieving their goals. They are limited by civic values of civil liberties, preservation of human rights, and their long decision-making process. In democracies, heavy-handed responses to suicide terrorism decrease the legitimacy of the government and may, therefore, contribute to popular support of the terrorist organization. In contrast, non-democracies have features that allow terrorist groups to further their agendas and achieve their long-term objectives, such as they have no problem violating human rights, acting harshly, and retaliating in very heavy-handed ways, because it is part of their political culture and they do not risk losing legitimacy. However, democracies can act like non-democracies when responding to suicide terrorism.

NOTES

[1] Pape, Robert A. *Dying to Win: The Strategic Logic of Suicide Terror.* New York: Columbia University Press, 2005.
[2] Abrahams, Max. "What Terrorists Really Want: Terrorist Motives and Counterterrorism Strategy." *International Security* 32, no. 4. (2008): 78-105.
[3] Pape, Robert A. *Dying to Win: The Strategic Logic of Suicide Terror.* New York: Columbia University Press, 2005.
[4] Bloom, Mia M. *Bombshell*. Philadelphia: University of Pennsylvania Press, 2011. "Death Becomes Her: Women, Occupation, and Terrorist Mobilization."
[5] "Suicide Terrorism and Democracy." *Suicide*, no. 582 (2006): 1-18.
[6] Crenshaw, Martha. "The Logic of Terrorism." *Terrorism in Perspective* 24 (2007): 24-33. *Terrorism in Context*. University Park: The Pennsylvania State University.
[7] De la Corte, Luis, and Andrea Giménez-Salinas. "Suicide terrorism as a tool of insurgency campaigns: Functions, risk factors, and countermeasures." *Perspectives on Terrorism* 3, no. 1 (2009): 11-19.
[8] Pape, Robert A. *Dying to Win: The Strategic Logic of Suicide Terror.* New York: Columbia University Press, 2005.
[9] Pape, Chenoweth, and Bloom, 2005.
[10] Conrad, Courtenay R., Conrad, Justin, and Young, Joseph K. "Tyrants and Terrorism: Why Some Autocrats are Terrorized

While Others are Not." *International Studies Quarterly*. Vol 58, Issue 3, pp 539-549.
[11] Abrahams, Max. "What Terrorists Really Want: Terrorist Motives and Counterterrorism Strategy." *International Security* 32, no. 4. (2008): 78-105.
[12] Daxecker, Ursula, and Hess, Michael (2013). "Repression Hurts: Coercive Government Responses and the Demise of Terrorist Campaigns." *British Journal of Political Science.*
[13] Pape, 2005, Bloom, 2005, Crenshaw, 2007, & Abrahams, 2008.
[14] Chenoweth, Erica. "Democratic competition and terrorist activity." *The Journal of Politics* 72, no. 1 (2010): 16-30.
[15] Downes, Alexander B. "How Smart and Tough Are Democracies? Reassessing Theories of Democratic Victory in War." *Inter*[16] Crenshaw, Martha. "The Logic of Terrorism." *Terrorism in Perspective* 24 (2007): 24-33. *Terrorism in Context*. University Park: The Pennsylvania State University.
[17] De la Corte, Luis, and Andrea Giménez-Salinas. "Suicide terrorism as a tool of insurgency campaigns: Functions, risk factors, and countermeasures." *Perspectives on Terrorism* 3, no. 1 (2009): 11-19.
[18] Pape, Robert A. *Dying to Win: The Strategic Logic of Suicide Terror.* New York: Columbia University Press, 2005.
[19] Pape, Chenoweth, and Bloom, 2005.
[20] Conrad, Courtenay R., Conrad, Justin, and Young, Joseph K. "Tyrants and Terrorism: Why Some Autocrats are Terrorized While Others are Not." *International Studies Quarterly*. Vol 58, Issue 3, pp 539-549.
[21] Abrahams *national Security* 33, no. 4 (2009): 9-51.
[22] Ibid.
[23] Abrahams, Max. "Why democracies make superior counterterrorists." *Security Studies* 16, no. 2 (2007): 223-253.
[24] Aksoy, Deniz, Carter, D.B., and Wright, J. (2015). "Terrorism and the Fate of Dictators." *World Politics*, 67930, 423-468.
[25] Li, Quan. "Does Democracy Promote or Reduce Transnational Terrorist Incidents?" *The Journal of Conflict Resolution*, vol. 49, no. 2, 2005, pp. 278-297.
[26] Bush, George W., 2003. "President Bush, President Arroyo Hold Joint Press Conference," White House press release.
[27] Toros, Harmonie. "We Don't Negotiate with Terrorists! Legitimacy and Complexity in Terrorist Conflicts." *Security Dialogue*. Vol. 39, Issue 4, pp, 407-426.
[28] Laqueur, Walter. *The Age of Terrorism*. Boston, MA: Little, Brown, 1987.
[29] Neumann, Peter R., 2007. "Negotiating with Terrorists," *Foreign Affairs* 86(1): 128.
[30] Sandler, Todd. "On the relationship between democracy and terrorism." *Terrorism and Political Violence* 7, no. 4 (1995): 1-9.
[31] Ibid., 19.
[32] Findley, Michael G., and Joseph K. Young. "Terrorism, democracy, and credible commitments." *International Studies Quarterly* 55, no. 2 (2011): 357-378.
[33] Ibid., 16.
[34] Ibid.
[35] Ibid.
[36] Hoffman, Bruce. *Inside Terrorism*. New York: Columbia University Press, 2006.
[37] Ibid., 16.
[38] Cornell, Svante E. "International Reactions to Massive Human Rights Violations: The Case of Chechnya." *Europe-Asia Studies* 51, no. 1 (1999): 85-100.
[39] Bloom, Mia M. *Bombshell*. Philadelphia: University of Pennsylvania Press, 2011. "Death Becomes Her: Women, Occupation, and Terrorist Mobilization."
[40] Ibid., 16.
[41] Ibid., 16.
[42] Abrahms, Max. "Deterring Terrorism: A New Strategy." *Perspectives on Terrorism* 8, no. 3 (2014): 2-15.
[43] Freedom House.
[44]Dalton, R.J., Sin, T.C., & Jou, W. "Understanding Democracy: Data from Unlikely Places." *Journal of Democracy*, 18(4), 142-156 (2007).
[45] Cingranelli-Richards.
[46] World Bank Kaufmann-Kraay.
[47] CIRI Human Rights Data Project.
[48] Ibid., 8.
[49] Kurz, Robert W., and Charles K. Bartles. "Chechen suicide bombers." *Journal of Slavic Military Studies* 20, no. 4 (2007): 529-547.
[50] Calhoun: The NPS Institutional Archive DSpace Repository. Chechen female suicide terrorism, Crawford, Zane K. Monterey, California: Naval Postgraduate School, 2017: 1-61.
[51] *Dying to Kill: The Allure of Suicide Terror*. New York: Columbia University Press.
[52] Phillips, David L. "Disarming, Demobilizing, and Reintegrating the Kurdistan Workers Party." *American Foreign Policy Interests* 30, no. 2 (2008): 70-87.
[53] CIRI Data.
[54] Ibid., 38.
[55] Ibid., 38.
[56] Eyrice, Idris U. "Roots and causes that created the PKK terrorist organization." PhD diss., Monterey, CA: Naval Postgraduate School, 2013.
[57] Ibid., 38.
[58] Tezcür, Güneº Murat. "When democratization radicalizes: The Kurdish nationalist movement in Turkey." *Journal of Peace Research* 47, no. 6 (2010): 775-789.
[59] Ibid., 38.
[60] Chicago Project on Security and Terrorism Suicide Attack Database.
[61] Turkish Human Rights Association, 2004.
[62] Barkey, Henri J., and Graham E. Fuller. "Turkey's Kurdish Question: Critical Turning Points and Missed Opportunities." *The Middle East Journal* (1997): 59-79.
[63] Ibid., 16.

Sara Harmouch was born in Tripoli, Lebanon, and is now a PhD candidate at American University studying Justice, Law, and Criminology. Sara holds a master's degree in International Relations, Science, and Technology from the Georgia Institute of Technology and a master's degree in Intelligence from the Daniel Morgan Graduate School of National Security. She specializes in terrorism studies with a focus on the Middle East and North Africa regions. She currently focuses on terrorist alliances and the reasons behind their perpetuation.

Is the Coronavirus an Intelligence Failure? Lessons for Intelligence Analysts in Pandemic

by Olivia M. Shumaker

OVERVIEW

The coronavirus pandemic will undoubtedly define a generation—including a generation of intelligence analysts. This is in part because, according to some estimates, the coronavirus pandemic is a massive intelligence failure, with far greater casualties than the 9/11 attacks and with consequences that will likely alter the American psyche. This article argues that the pandemic is an intelligence failure, and that both the nature of the failure and the current face of the coronavirus response hold valuable lessons for future analysts.

INTRODUCTION

In the span of just three months, the coronavirus went from an unknown virus to a pandemic infecting every country in the world, crashing the global economy, decimating healthcare systems, and reshaping the fabric of day-to-day life. By the time the pandemic is over, the United States may end up with the largest COVID-19 outbreak in the industrialized world.[1] Yet the pandemic was not unexpected. Worldwide threat assessments dating back to 2018[2] named a cousin of the current coronavirus strain (Middle East Respiratory Syndrome Coronavirus) as a major threat with pandemic potential if the virus acquired sufficient human-to-human transmissibility. Intelligence reports going back to January and February 2020 warned of the global danger of the coronavirus threat in China.[3]

However, policymakers did not act on the warnings, and Americans are now paying the price. Coronavirus deaths in New York alone are already more than double the fatalities seen in the September 11, 2001, attack,[4] and projections of the pandemic's total fatalities in the United States could be two to four times the U.S. casualty rate during the entire 20-year Vietnam War.[5]

The pandemic is a reckoning, and few will be spared—including the Intelligence Community. In fact, some have already dubbed the coronavirus the worst intelligence failure in U.S. history.[6] Nevertheless, is the coronavirus pandemic an intelligence failure? This article will argue that, in some sense it is—and that it holds important lessons for intelligence analysts in dealing with policymakers who are reluctant to listen.

RESPONSIBILITIES OF 21ST CENTURY INTELLIGENCE

Is the coronavirus an intelligence failure? To answer that question, we must first consider whether the virus is, in fact, the responsibility of the intelligence workforce. In other words, are the coronavirus and other public health threats within the domain of intelligence?

The Cold War understanding of intelligence consists of tracking the movement of concrete existential threats to the United States. By this logic, the coronavirus is not an intelligence failure because it is not the IC's responsibility. In the post-Cold War intelligence world, however, which has evolved to analyze any potential existential threat to any American in the world at any given time, coronavirus is certainly within the realm of intelligence.

THE ROLE OF INTELLIGENCE

As noted by Mark Lowenthal, the former Vice Chairman of the National Intelligence Council, one of the foremost responsibilities of intelligence is to prevent strategic surprise: "The foremost goal of any intelligence community must be to keep track of threats, forces, events, and developments that are capable of endangering the nation's existence."[7] The problem is balancing current intelligence—short-term assessments usually extending no more than a week or two—with long-term or strategic intelligence, which uses longer horizons to look at trends over time. Put another way, it is the conflict between tactical intelligence and strategic intelligence, each focused on threats in a different light. "Tactical intelligence is considered more pressing, dealing with 'straightforward information,' while strategic intelligence encompasses more long term issues, including political and economic factors and trends over time."[8]

The Cold War context posits tactical and strategic threat-focused thinking as a question of ascertaining an adversary's intent and capability. The capabilities of a conventional enemy (such as a foreign military) are well understood, but its intent is in question. With terrorism, the intent to commit harm is clear, and the intelligence challenge is to ascertain the enemy's capability to inflict harm.[9] Yet, the novel coronavirus is not a conventional threat, and intelligence no longer operates under Cold War expectations.

In 1994, during the Rwandan genocide, hundreds of thousands of people fled westward, many of them setting up camp at the foot of an active volcano. At the time, the U.S. State Department's Deputy Assistant Secretary for Analysis, Thomas Fingar, was asked: If the volcano did erupt, which way would it erupt, and which way would the poisonous gas blow? Fingar's flippant response was that they had failed to spy on Mother Nature,[10] but the question was a serious one, with a potentially disastrous threat if realized. It also reflects a dramatically altered understanding of what constitutes a threat—and as a consequence, the dramatically altered responsibilities of modern intelligence analysts.

The novel coronavirus is not a conventional threat, and intelligence no longer operates under Cold War expectations.

Today, intelligence has the daunting responsibility for protecting all Americans in the world and at all times. This has a great deal to do with policymakers, who believe intelligence to be omniscient and capable of managing the Soviet Union threat times six billion. On the other hand, policymakers, like the rest of the public, obtain the majority of their knowledge about intelligence from a combination of Hollywood spy movies and the community's greatest failures. They believe it to be both possible and obvious for the IC to track down a single person in the world who intends to cause harm to Americans (thanks to Hollywood), yet they also garner most of their knowledge about the real IC as a consequence of its worst-hair days on record (such as Pearl Harbor or the 9/11 attacks) and derive their opinion of intelligence from its most public embarrassments (the Edward Snowden leak, for example).

Worse, intelligence analysts now operate at a critical disadvantage compared to their Cold War predecessors: their consumers view them as optional equipment. In the Cold War era, policymakers had very few resources to turn to outside of intelligence reports when they wanted to know what was happening in the world. We now live in a world where anyone, policymakers included, can open a search bar and pull up thousands of results on any conceivable topic in seconds. Policymakers now believe themselves to be their own analysts and, driven by their own strong worldview and political agenda, turn to analysts to confirm what they already believe to be true, treating the intelligence apparatus as comparable to the only analogous resource for the average person: Google.

Policymakers now believe themselves to be their own analysts and, driven by their own strong worldview and political agenda, turn to analysts to confirm what they already believe to be true...

What does this mean for the COVID-19 pandemic? For one thing, when major threats to the American people—as the pandemic surely is—occur, policymakers and the public will wonder why the IC, believed to be omniscient, did not predict them. It is not the responsibility of the IC to predict the future, but that matters little to the public and the policymakers subject to their whims. Furthermore, the response is obvious. The IC *did* offer repeated warnings about the coming threat of a pandemic like COVID-19. "[For] years, American intelligence agencies have been warning about the increasing risks of a global pandemic that could strain resources and damage the global economy, while observing that the frequency and diversity of global disease outbreaks have been rising," even going so far as to mention a close cousin of the current COVID-19 strain by name in 2017 and 2018 global threat assessments.[11]

Yet this response is also insufficient. The IC's success or failure is not based purely on the fact of offering warning. If that were enough to negate failure, then 9/11 would not be viewed as a catastrophic disaster for U.S. intelligence agencies.

WHAT IS AN INTELLIGENCE FAILURE?

Erik Dahl, an associate professor at the Naval Postgraduate School, in his assessment of intelligence failure vis-a-vis intelligence success, defines intelligence success as a two-step process: "First, intelligence agencies and officials must correctly assess the situation… In the second step, intelligence officials must convey their assessments to decision makers and convince them of the importance of the issue."[12] It is the second half of the process which is essential in the case

of several historic intelligence failures, and it is an issue present in the early coronavirus warnings.

The coronavirus pandemic is a difficult issue for intelligence because it is so complex. It is not a terrorist group or foreign adversary. It follows no timeline, has no loyalties or motivations, and knows no borders or strategic targets. A virus has neither intent nor conventional attack capabilities.

The second stage of the process can be understood as the need for tactical warning—not just the fact of a threat existing but what, in specific terms, a policymaker can do about it. While the exact nature of the warnings provided on coronavirus remain unknown to the general public, the available portrait is one of strategic warning, "The intelligence reports didn't predict when the virus might land on U.S. shores or recommend particular steps that public health officials should take… But they did track the spread of the virus in China, and later in other countries, and warned that Chinese officials appeared to be minimizing the severity of the outbreak."[13] This falls into the category of what Dahl calls the paradox of strategic warning: strategic warnings are surprisingly easy to acquire, but they are also less likely to be acted upon by policymakers, because strategic surprises are still fundamentally tactical events requiring tactical response.[14]

[Editor's Note: Dr. Dahl currently serves as the chair of the Intelligence Studies Section of the International Studies Association, the principal professional organization for those involved in the field of international relations.]

INTELLIGENCE, STRATEGIC SURPRISE, AND PANDEMIC

The coronavirus pandemic is a difficult issue for intelligence because it is so complex. It is not a terrorist group or foreign adversary. It follows no timeline, has no loyalties or motivations, and knows no borders or strategic targets. A virus has neither intent nor conventional attack capabilities. It simply does what a virus does best: opportunistic infection. Because the virus does not discriminate, intelligence cannot extrapolate its next steps based on previous patterns of behavior and, because it does not discriminate between one person and the next, anyone is a fair target.

Furthermore, the involvement of the larger public automatically complicates any response taken. Fighting a virus is a medical concern, but closing a border is a political one. Any risk-based horizon scanning by decision-makers must account for the social and political fallout of their actions, especially if those actions are taken before the public perceives any real threat. The public, unlike the military, cannot be mobilized quickly or consistently, nor can Americans be easily convinced to do something that thoroughly inconveniences them to avoid a threat that many do not believe will reach the United States.

A virus is also a less concrete threat than, say, a bombing. Bombings must involve an explosive in a specific location at a specific time and place. If one happens not to be in or near the place the bomb will go off, at the time it goes off, one does not face any real danger from the bombing. A viral epidemic, on the other hand, can spread from patient zero and impact an entire country by jumping from one person to the next, so long as the people in contact with it are not taking appropriate precautions. This particular virus also has less of a visceral impact than a bombing or even a different virus such as Ebola—the symptoms resemble the common cold, and under normal conditions with readily available medical care its fatality rate is relatively low.

In translation, the IC was fighting an uphill battle. How could the IC convince policymakers to take preventive action when the threat seemed too distant and minor to justify harsh tactical steps?

WAS THIS A FAILURE?

According to Dahl's first criteria, involving a correct assessment, the coronavirus pandemic was not an intelligence failure. However, by Dahl's second criteria, convincing policymakers of the importance of the issue such that they take action against it, the pandemic is an intelligence failure.

Inform vs. Convince: The Thin Line of Politicization

Former national security advisor Henry Kissinger once observed, "Well, you've informed me, but you haven't convinced me."[15] This is the root of the failure in the coronavirus pandemic, yet the gap between informing and convincing is a sticky point for intelligence analysis, straddling the thin line of politicization.

At this point, it is important to delineate acceptable versus unacceptable practice. "One must differentiate between attempting to influence (that is, inform) the process by providing intelligence, which is acceptable,

and trying to manipulate intelligence so that policy makers make a certain choice, which is not acceptable. . .senior policy makers can and do ask senior intelligence officials for their opinions, which are given."[16] It is acceptable to influence the process by providing sound intelligence analysis. Convincing, in this context, is acceptable because it is part of an analyst's job—providing the right analysis to the right decision-makers at the right time to allow those decision-makers to make informed decisions in order to counter those threats.

It is not acceptable for an analyst to provide his or her own opinion as fact or analysis.

It is not acceptable for an analyst to provide his or her own opinion as fact or analysis. Nor is it acceptable to mold analysis to meet the analyst's perspective, or the policymaker's, for that matter. Fitting the analysis to the policymaker (i.e., telling the policymaker what he/she wants to hear, as opposed to tailoring reporting to suit the practical needs of the consumer) is upward politicization; similarly, a policymaker strong-arming an analyst into providing intelligence based on what he/she wants to see (as opposed to communicating the need that must be met through the intelligence) is downward politicization, and it harms both sides by washing away the most important elements of an intelligence report.

In the case of coronavirus, intelligence agencies *informed*—the threat was recognized accurately, as were the scope and consequences, and it was communicated successfully. They did not *convince*, in that they did not provide the information that policymakers would have needed to act on the intelligence in a realistic way.

This is not to argue that intelligence agencies could or should have offered tactical intelligence for a non-tactical threat or that agencies should have reached beyond the scope of their expertise to offer recommendations. Nor is it arguing that intelligence agencies are inherently responsible for the decisions that policymakers take of their own accord, or that they are responsible for examining the interaction of every relevant factor. This is rarely, if ever, possible based on the timelines of real-world decisions.

That said, "Prompting decision makers to rethink their own assumptions and preliminary judgments may be more beneficial to the national security enterprise than providing definitive answers to specific questions. . . Getting it completely right is often less important than providing useful information and insights to the right people at the right time."[17] It is more useful to convince policymakers to shift their perspective at the right moment than it is to collect all available information. The key, then, is striking a balance: providing the right strategic and tactical intelligence at the right moment to enable tactical response.

Could intelligence have prevented the pandemic? The rapid spread of infection and the difficulty of placing roadblocks in the global economy suggest not, and blaming the IC is an easy out to a difficult problem. Could timely, effective intelligence have mitigated the effects of the pandemic? Possibly, and the possibility could have saved lives. Regardless, there is room for improvement in the coronavirus warning that may help future analysts better mitigate the consequences of a similar disaster in the future.

Lessons for the Analysts of Tomorrow

Intelligence has never been a business of easy answers, and the coronavirus pandemic is no simple threat. Yet there is a lesson to be found here for the intelligence analysts of tomorrow, and it is best exemplified in a familiar face of the American coronavirus response: Anthony Fauci. Dr. Fauci is not, and has never been, an intelligence professional, at least not in the conventional sense of the word. He is the nation's leading expert on infectious diseases; he has served as Director of the National Institute of Allergy and Infectious Diseases for 36 years, advising six presidential administrations from both political parties on a long list of viral epidemics, some of which defined generations: HIV, SARS, Ebola, Zika, swine flu, and avian influenza among them.[18] He is also everything that the current U.S. President disdains in an advisor: educated, competent, pragmatic, disciplined and, above all, candid.

Intelligence has never been a business of easy answers, and the coronavirus pandemic is no simple threat.

Yet while the President has grown impatient with Fauci's unwillingness to parrot his proclamations or say what he wants to hear, to the point of leaking threats of imminent firing,[19] Fauci has still retained the right to disagree publicly with the administration while keeping both his position and the President's ear. Dr. Fauci has managed this feat by being apolitical, non-ideological, and so good at his job as to be indispensable, even when his meetings with the President consist of nothing but bad news. This

is embodied in a dictum shared with Fauci by someone who used to work for the Nixon administration: "When you go into the White House, you should be prepared that that is the last time you will ever go in. Because if you go in saying, I'm going to tell somebody something they want to hear, then you've shot yourself in the foot."[20]

Balancing Candor, Access, and Professional Good Graces

This is not to argue that giving this type of plain talk is easy or straightforward. It requires a steady commitment to prioritize doing one's job above currying favor, a high degree of nerve to face the consequences without flinching, and a stubborn refusal to intermingle the personal and the professional.

The COVID-19 pandemic is not the last wildly unconventional threat the IC will face...

To be clear, this is not without professional complications. As Martin Petersen, former Deputy Executive Director at the CIA, noted in reflecting on 40 years of experience in intelligence analysis, speaking truth to power first requires access to power.[21] The IC must sell the need for its services to policymakers who view those services as nonessential. There is also incredible professional pressure on analysts from within their own agencies. The power of an analyst's manager, balancing the force of mission trajectory against the whims of decision-makers who will decide the unit's budget in the next fiscal year, cannot be overstated.

It is to say that a high degree of candor requires a constant awareness that written products are the record, that going on the record is to stay on the record forever, and that the record must be beyond reproach. A party guest may win the right to deliver bad news to the host, but only if that bad news is supported with strong evidence, reasoned soundly, and offered without any traces of arrogance.

It is also to say that, if an analyst is to deliver bad news, he/she must be so thoroughly good at his/her job that a policymaker cannot discard the news out of hand based on the analyst's qualifications to deliver it. However, delivering bad news is not synonymous with sharp elbows—quite the opposite. The combination of bad news and persistent sharp elbows will eventually be perceived as stubbornness or arrogance, even if it is not delivered that way.

An answer, again, may be found in Dr. Fauci. He is apparently direct to the point of bluntness but, while he has corrected erroneous statements and publicly disagreed with the administration, he has managed to do so without saying that the President is wrong or chiding him for his messaging. This is born of pragmatism, not arrogance, and it is the reason why Fauci has kept his position through six administrations and multiple viral epidemics. He corrects and publicly disagrees not because he is right, but because his job is saving lives, and correcting inaccuracies is a necessary part of doing his job well.

WHY IT ALL MATTERS

The COVID-19 pandemic is not the last wildly unconventional threat the IC will face, and President Trump is far from the last resistant politician whom analysts will brief. Yet, crises like this are times that reveal both our weaknesses and the strength of our resolve to fix them. The way forward for intelligence professionals is hard. So, too, is the nature of intelligence analysis, which lacks the glamor of an overseas assignment or covert operations. If anything, it is one of the least revered and unromanticized elements of intelligence. However, the minds that make up the analytical workforce are the ones that drive the entire community forward, and it is the work of analysts that will change the minds of people who matter.

It is the responsibility of intelligence analysts to be ethically humble and intellectually thorough enough to prioritize the mission and to prioritize the security of the public above easy answers or professional gain.

Failure to learn is a form of arrogance in its own right and, in our times of greatest crisis, the American public deserves better of the men and women who have sworn to protect it. It is the responsibility of intelligence analysts to be ethically humble and intellectually thorough enough to prioritize the mission and to prioritize the security of the public above easy answers or professional gain.

In the darkest hour of the American Civil War, another of America's deadliest crises, President Abraham Lincoln attended Sunday service at a small church across from the White House, led by a young pastor. On his way back, when a parishioner asked Lincoln what he thought of the

individual, Lincoln gave a simple reply: The reverend had a strong voice and a clear message, but still, Lincoln said, the young reverend failed. This was, Lincoln said, for one simple reason: he failed to ask us to do something great. Do the mission. Do something great.

NOTES

[1] Ed Yong, "How the Pandemic Will End," *The Atlantic*, March 25, 2020, https://www.theatlantic.com/health/archive/2020/03/how-will-coronavirus-end/608719/.
[2] Daniel R. Coats, "Worldwide Threat Assessment of the U.S. Intelligence Community," Director of National Intelligence, https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA—Unclassified-SSCI.pdf.
[3] Shane Harris, Greg Miller, Josh Dawsey, and Ellen Nakashima, "U.S. intelligence reports from January and February warned about a likely pandemic," *The Washington Post*, March 20, 2020. https://www.washingtonpost.com/national-security/us-intelligence-reports-from-january-and-february-warned-about-a-likely-pandemic/2020/03/20/299d8cda-6ad5-11ea-b5f1-a5a804158597_story.html?utm_campaign.
[4] Michael Finnegan, "New York state's coronavirus deaths now more than double 9/11 fatalities," *The Los Angeles Times*, April 8, 2020, https://www.latimes.com/world-nation/story/2020-04-08/coronavirus-national-states-pandemic.
[5] Olivia B. Waxman and Chris Wilson, "How the Coronavirus Death Toll Compares to Other Deadly Events from American History," *TIME*, April 12, 2020, https://time.com/5815367/coronavirus-deaths-comparison/.
[6] Micah Zenko, "The Coronavirus Is the Worst Intelligence Failure in U.S. History," *Foreign Policy*, March 25, 2020, https://foreignpolicy.com/2020/03/25/coronavirus-worst-intelligence-failure-us-history-covid-19/.
[7] Mark Lowenthal, *Intelligence: From Secrets to Policy* (Washington, DC: CQ Press, 2006), 2.
[8] Amanda Gookins, "The Role of Intelligence in Policy Making," *SAIS Review* 28, no. 1 (2008): 66.
[9] Erik J. Dahl, "Why Does Intelligence Fail, and How Can It Succeed?" in *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond* (Washington, DC: Georgetown University Press, 2013), 16-17.
[10] Thomas Fingar, "Reducing Uncertainty: Intelligence Analysis and National Security," November 28, 2011, The Mission Inn, Riverside, California, 59:50, https://www.youtube.com/watch?v=CkQvRKRRcLY&feature=emb_title.
[11] Ken Dilanian, "U.S. intel agencies warned of rising risk of outbreak like coronavirus," *NBC News*, February 28, 2020, https://www.nbcnews.com/politics/national-security/u-s-intel-agencies-warned-rising-risk-outbreak-coronavirus-n1144891.
[12] Erik J. Dahl, "Why Does Intelligence Fail, and How Can It Succeed?" in *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond* (Washington, DC: Georgetown University Press, 2013), 22.
[13] Shane Harris, Greg Miller, Josh Dawsey, and Ellen Nakashima, "U.S. intelligence reports from January and February warned about a likely pandemic," *The Washington Post*, March 20, 2020, https://www.washingtonpost.com/national-security/us-intelligence-reports-from-january-and-february-warned-about-a-likely-pandemic/2020/03/20/299d8cda-6ad5-11ea-b5f1-a5a804158597_story.html?utm_campaign.
[14] Erik J. Dahl, "Why Does Intelligence Fail, and How Can It Succeed?" in *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond* (Washington, DC: Georgetown University Press, 2013), 22.
[15] Roger Z. George and James B. Bruce, *Analyzing Intelligence: National Security Practitioners' Perspective* (Washington, DC: Georgetown University Press, 2014), 188.
[16] Mark Lowenthal, *Intelligence: From Secrets to Policy* (Washington, DC: CQ Press, 2006), 4.
[17] Thomas Fingar, "Analysis in the U.S. Intelligence Community: Missions, Masters, and Methods," in *Intelligence Analysis: Behavioral and Social Scientific Foundations*, eds. Baruch Fischhoff and Cherie Chevin (Washington, DC: The National Academies Press, 2011), 4.
[18] "Anthony S. Fauci, M.D., NIAID Director," National Institute of Allergy and Infectious Diseases, accessed April 11, 2020, https://www.niaid.nih.gov/about/director.
[19] Maggie Haberman, "Trump Has Given Unusual Leeway to Fauci, but Aides Say He's Losing His Patience," *The New York Times*, March 22, 2020, https://www.nytimes.com/2020/03/23/us/politics/coronavirus-trump-fauci.html.
[20] Michael Specter, "How Anthony Fauci Became America's Doctor," *The New Yorker*, April 10, 2020, https://www.newyorker.com/magazine/2020/04/20/how-anthony-fauci-became-americas-doctor.
[21] Martin Petersen, "What I Learned in 40 Years of Doing Intelligence Analysis for US Foreign Policymakers," Center for the Study of Intelligence, *Studies in Intelligence* 55, no. 1 (2011), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-55-no.-1/what-i-learned-in-40-years-of-doing-intelligence-analysis-for-us-foreign-policymakers.html.

Olivia M. Shumaker is a current master's student in the Applied Intelligence program at Georgetown University. Previously, she was a Woodrow Wilson Research Fellow and Bloomberg Scholar at Johns Hopkins University. Her work was selected for the 2020 Intelligence Studies Consortium at Georgetown University as part of a panel on Ethics/Moral Issues in the Intelligence Profession, presenting on ethics as a training tool in technology-based intelligence. However, due to the pandemic that event was indefinitely postponed.

From CIA to C(AI):
Using Artificial Intelligence as a Shield and Sword in Cyberespionage

by Roman Kolodii

OVERVIEW

To succeed in an age of machine learning one must be a learning "machine." This article offers a broad look at how much we can learn as scholars and practitioners of intelligence from a rapid unraveling of machine learning (ML) techniques to be protected online. Cyberespionage and cyberattacks remain a cause of severe material and reputational damage for the state and thus are a frontline national security concern, especially for intelligence institutions in charge of keeping information secure. This study aims to address the challenge of a threat-ridden cyberspace through a close examination of the nexus between cybersecurity and ML-driven artificial intelligence (AI), serving the practical needs of the Intelligence Community dealing with cyberespionage. The article suggests a number of ways how AI could benefit cyber-protection strategies of government and intelligence institutions profoundly, giving cyber-defense an edge over cyber-offense. However, the analysis also reveals that the upper hand of AI-assisted cyber-defenses might have diminishing returns in case an AI-powered malware is designed and deployed to enhance cyberattacks by adversaries. Hence, governments, and especially their intelligence components, can largely benefit from implementing AI in cyber-defense, but they should pursue this goal with much caution, given AI's inherent vulnerabilities and its potential for ill.

INTRODUCTION

The concept of cybersecurity conjures up a myriad of names of prominent scientists who have made enduring contributions to the functioning of computing machines and digital networks. However, it might never occur to the reader that the Spartan king Leonidas could fit well with the cybersecurity narratives of our age. As a famous legend has it, while facing an imminent threat of Persian invasion and ensuing devastation, Leonidas deemed the real-world military intelligence he possessed insufficient for taking an ultimate decision to resist foreign incursion and so resorted to a counsel of a quasi-human entity—the Oracle at Delphi, widely believed to voice credible prophesies on the matters of war. The Oracle's prediction proved accurate; despite their committed resistance, the Spartans lost to Xerxes I and turmoil reigned. Being the celebration of Spartan courage ever since, this timeless story, however, can have a different interpretation if revisited today. In modern times, military and political leaders, just like Leonidas, can also gain the assistance of quasi-human forces, this time those "summoned" from the digital realm, when contemplating actions to safeguard their nations. What is implied here is a ground-breaking technology of artificial intelligence (AI) with its powerful machine learning (ML) algorithms that, just like the Oracle at Delphi, can offer predictions. What differs, though, is that the predictions of AI are mathematically structured models based on incremental plentitudes of digital data, which makes their prognosis much more reliable. Moreover, as this study argues, cybersecurity can be a realm in which the use of this new-age oracle—AI—can accrue some practical purchase in policy planning and mitigation of threats.

Overall, this article reflects on ways and strategies to integrate artificial intelligence tools within cybersecurity mechanisms that underpin all modern societal systems. These systems have grown increasingly reliant on sound, smooth, and uninterrupted workings of critical information infrastructure, while suffering from resultant vulnerabilities and security loopholes that constitute modern cyberspace. Over the years, cyberspace has gone through a drastic evolution from a no man's land to a balkanized virtual territory with countries fencing themselves off with great firewalls, proclaiming exclusive Internet sovereignty, instigating security breaches, and ultimately failing to reach any consensus on how to regulate this borderless reality. While cyberspace buttresses the functioning of industrial infrastructure through information and communications technologies, fosters international commerce through cross-border data flaws, and indulges our daily needs through broadband connection, it opens up a great many avenues for compromising the security of our governments, companies, and households. The destructive effects of cyberattacks were visible with the cases of the Maroochy Shire sewage spill in Australia in 2000, the denial-of-service attacks shutting down critical infrastructure facilities in Estonia in

2007 and Georgia in 2008, Stuxnet's destruction of nuclear centrifuges in Iran in 2010, and Industroyer and NotPetya cyberattacks shutting down Ukrainian power grids and its banking system in 2016 and 2017, respectively.[1] Nevertheless, the majority of cyberattacks are deployed not for destructive but disruptive purposes and focus on data exfiltration and cyberespionage, which are at times equally disastrous. The cost of economic cyberespionage, for instance, has risen to billions of dollars over recent years, bleeding the affected economies and disrupting financial markets. According to the U.S. Commission on the Theft of American Intellectual Property, the country loses more than $300 billion annually from the cyber-enabled theft of intellectual property.[2]

As a result of many threats emanating from it, cyberspace has become increasingly militarized, with NATO proclaiming it a domain of operations, just like air, sea, and land.[3] In the same spirit, as an acknowledgment of a growing importance of cyber-protection, the United States has officially set the goal of "manag[ing] cybersecurity risks to increase the security and resilience of the Nation's information and information systems."[4] Many other countries followed suit. Cybersecurity, therefore, has emerged as a frontline national interest that requires proactive and innovative support from all institutions in charge of homeland security. Yet, the continuous damage caused by cyberattacks in the form of spying malware remains on the rise and keeps causing substantial losses due to lost business revenues, stolen trade secrets, leaked sensitive data, and compromised critical computer networks. Tackling these risks is of particular importance for intelligence institutions, which are entrusted with keeping sensitive information confidential and undisclosed, especially in light of constant foreign cyber-intrusions.

This study aims to address these concerns through a close examination of the nexus between cybersecurity and artificial intelligence, specifically to the benefit of the Intelligence Community (IC) dealing with cyberespionage and specialized institutions, such as U.S. Cyber Command which coordinates both defensive and offensive operations in cyberspace.[5] This research asks two inextricably linked questions: to what extent can AI transform cybersecurity practices and what implications can it incur for offense-defense dynamics among its key stakeholders in cyberspace? Its core argument reveals that AI can tangibly and extensively transform cyber-defense mechanisms and practices when compared to their conventional forms, mostly by improving cyber-threat detection and prediction, increasing time- and cost-efficiency of cybersecurity management, and raising the threshold for an effective cyberattack to succeed. Ultimately, this transformation, in turn, can shift the defense-offense dialectics in cyberspace in favor of cyber-defense, but this asymmetry might level out if AI becomes more democratized and proliferated, resulting in the creation of a superior AI-driven malware.

The discussion of this topic will unfold as follows. The next section will present methodology and research objectives, clarifying the principal scientific interest of the article. The subsequent three paragraphs on cyber-defense will investigate various ways AI can enhance cyber-protection mechanisms as compared to their conventional premises. The fourth paragraph, in turn, will critically engage with preceding sections and scrutinize the weaknesses and limitations of AI as a tool of cyber-defense, as well as demonstrate how it can be used for offensive purposes based on some nascent instances of an AI-assisted malware already prototyped. Finally, the article will conclude that AI can significantly enhance organizations' defensive capacity in cyberspace, giving them an edge over offensive actions of cyber-perpetrators. However, inherent vulnerabilities of machine learning algorithms and further proliferation of AI on commercial markets can result in cybercriminals with the ways and means to exploit AI for cyberattacks, which might cause severe disruptions that should be carefully considered.

THE DESIGN AND SCOPE OF THE STUDY

The research design has been determined by the complexity of the task at hand. To understand the measure of transformation possible due to the adoption of AI for cyber-preparedness and resilience, a comparative framework was set juxtaposing traditional methods of cyber-protection with the most recent cutting-edge research into artificial intelligence-based network security techniques. To this end, a considerable body of technical literature on modern advancements in machine learning has been selected and carefully surveyed using the comparative method. However, the research goes further beyond the focus solely on cyber-protection. More specifically, to understand properly the real impact of AI on the cybersecurity landscape, the essay examines its potential use not only as a means of empowering cyber-defensive protocols, but also as a tool for upgrading cyber-offensive methods, mostly through malware sophistication. This Hegelian approach, which invites one to look for the conflict and unity of the opposites in the object under scrutiny, has been indispensable, as any analysis of how AI could help counter cyberattacks would not be complete without disclosing the potential of AI to encourage such attacks and render them more hazardous. But why do we seek a philosophical angle for *this particular research question*? As was noted by proponents of social epistemology of intelligence, establishing intersections between philosophy and intelligence is "very useful to clarify many problems"[6]—in this article's case, AI's impact on the cybersecurity praxis of the Intelligence Community. Hegel's philosophy, which inspired the dialectical approach to warfare employed by Clausewitz and through him informed the very canon of Western military thought, has been noted for its usefulness in the analysis of intelligence services. Specifically, Hegel's

emphasis on the interplay of the opposites—of thesis and antithesis—has lent itself well to explaining the importance of compromise or, in Hegel's terms, synthesis, between the IC and state control mechanisms, including the judiciary.[7] Applying the Hegelian approach even further, inside the depth of national cybersecurity, has allowed for a more nuanced appreciation of long-haul effects of AI on offense-defense dialectics within cyberspace and uncovered its ambiguous potential to challenge the cybersecurity climate to an unprecedented degree.

As for the key categories and scope of this research, cyber-defense implies strategies, tools, and methods deployed by individual, corporate, and government entities to safeguard security of their data, digital assets, and information infrastructure. Accordingly, cyber-offense denotes a wide array of actions undertaken to compromise such systems by inflicting physical damage or stealing sensitive data. Cyberespionage in this research stands for "cyber operations to copy confidential data that is resident in or transiting through cyberspace, even if it is not read or analyzed."[8] Although other types of cyber-intrusions will be mentioned as well, including impersonation attacks and distributed-denial-of-service attacks, we will focus predominantly on cyberespionage. Then, importantly, artificial intelligence refers to "a means of describing computer programs capable of simulating human cognition," while machine learning—so far the key integral and driving force behind AI—is a "set of techniques and tools that allow computers to think by creating mathematical algorithms based on accumulated data."[9] For the sake of this study we will sometimes use artificial intelligence and machine learning interchangeably, keeping in mind that in practice they relate to each other functionally and normally would be differentiated: ML as an activity or technique, and AI roughly as its final desirable outcome.

With the key notions now clarified, the argument begins to unfold with the following section that explores key trajectories of how artificial intelligence can improve cybersecurity measures compared to most traditional practices and outlines its potential impact on organizations' approach toward cyber-threat anticipation and response.

AI AND CYBER-DEFENSE: BRINGING CYBERSECURITY ON A NEW LEVEL

AI and Cyber-Threat Intelligence

When exercised to strengthen counter-cyberespionage efforts, AI-based cybersecurity solutions can substantially benefit defensive strategies of government organizations by augmenting their capacity for proactive and preemptive agency in cyberspace.

Before the rise of AI, the most broadly utilized protection methods, such as host or network firewalls, intrusion prevention systems, and antiviruses, had all been designed to counter a specific class of cyberattacks.[10] In the wake of malware deployment and its subsequent infliction of damage upon an organization, security vendors would normally examine the malware and issue proper patches for their platforms or products that were compromised. These measures have long allowed organizations to resist recurring cyberattacks by a malware belonging to the same or similar class. However, the speed and versatility of approaches to cyberattacking constantly surpass the increase in preparedness to repel them effectively. Quite often the task for cyber-adversaries consists simply in constructing "a new piece of malware" or using "a method like packing or obfuscation to make the malware appear unique"[11] for derailing the functioning of systems under siege. As a result, "*most*[12] [advanced persistent threats] in cyberspace are able to successfully evade current anti-virus technology."[13]

Other defensive techniques like firewalls that scan network traffic—a path for cybercriminals to the sought-after data—searching for unusual items and suspicious behaviors are also susceptible to considerable risks. Both traditional and next-generation network firewalls, as well as intrusion prevention systems that trace irregular items and behaviors in traffic, are rigidly adjusted to combat assaults that match only a predefined signature.[14] These signatures reflect essential technical characteristics behind an established malware whose configurations have been captured and fed into anti-virus scanning matrices. However, such a heavy reliance on specific signatures restricts many conventional cyber-defenses in countering yet unknown threats that circumvent their patterns owing to a rapid growth of malware variations in the wild.

There are methods seeking to compensate deficiencies of signature-based malware detection, such as heuristic engines that evaluate suspicious source code against malicious datasets to capture novel threats. However, even these methods demonstrate poor performance due to an increasingly larger volume of malicious programs being deployed daily, as they ensure very low precision in code detection[15] and work effectively only within "a limited number of training datasets."[16] Yet another non-signature method—anomaly-based detection that locates deviations of suspicious items from legitimate patterns to determine their degree of danger—suffers from the same problem due to "the rapid increase in the network traffic behavior and very limited availability of computational resources (computation time and memory)."[17] As new classes and generations of malware emerge, the amount of data to be analyzed grows exponentially. Consequently, traditional cyber-defensive methods falter, and organizations procured with seemingly up-to-date solutions fall victim to upgraded and modified cyberattacks.

In this regard, the application of artificial intelligence can drastically reduce the asymmetry between cybercriminals and their targets in cyberattack anticipation. Specifically, AI can effectively lower dependency on malicious signatures during threat detection, as it is able to "automatically scan for unknown malware or zero-day exploitation, based on certain features and behavior, rather than specific signatures."[18] Machine learning algorithms dealing with harmful code retrieved from knowledge bases can identify sustainable or altering patterns behind a particular malware. With these patterns, AI-powered solutions can determine existing modifications of a malware in the wild and even predict its new forms in the future. In a sense, they replace conventional fixed algorithms used in cyber-threat detection with flexible algorithms able to de-compile and recompose malicious source code in many forms to anticipate its variations. Hence, equipped with AI, organizations are not only capable of cyberattack detection in a nascent stage but also of cyberattack prevention, as they have foreknowledge of possible varieties of malware potentially deployed against them. To illustrate empirically, ML has reached a detection rate above 96% in ransomware analysis, 99.97% in botnet detection,[19] 99.56% in web shell (remote access Trojans accessing data on websites) recognition,[20] and beyond 99% in network traffic analysis of Android malware, which is considered "very successful."[21]

Machine learning can also reinforce system robustness against botnets—networks of hosts used for data espionage, click-frauds, and distributed-denial-of-service attacks. Non-AI-based intrusion detection systems frequently fall short of isolating more recent botnets because those use encrypted payload that requires extensive big data analysis to be deciphered and tracked effectively. Also, traditional botnet traffic detection systems work within a single botnet topology or, in other words, are able to identify botnet traffic only of a specific kind—a centralized or decentralized one, making them clumsy in tackling botnet varieties.[22] Due to this limitation, organizations risk omitting malicious traffic and forcibly joining botnets exploited for nefarious purposes. However, deep learning algorithms, which unlike many other ML methods can classify unlabeled data without human assistance, remedy these flaws of traditional detection methods, as they filter traffic independently of botnet topology.[23] This is primarily due to their ability to "envision" botnet varieties based on massive amounts of available unlabeled samples, which makes their detection approach universal. This can help organizations to preserve the integrity of their systems, save resources on malware removal, and keep their assets uncompromised.

In summary, AI can extensively impact cybersecurity practices by strengthening the robustness of cyber-intrusion detection practices. AI-enabled cyber-defenses can be more accurate and effective (although still not perfect) in identifying intrusions, quarantining various types of malware like ransomware or botnets. Importantly, AI can also increase a preventive capacity of cyber-defense substantially, allowing organizations not only to catch up with the pace of malware innovation but also at times to foresee it due to AI's ability to predict variations of malware used in cyberattacks. Along with the deployment of AI-based "honeypots" to lure attackers and learn their methods and habits well before the assault,[24] these advancements can make organizations' strategy of cyber-defense more evidently proactive and preemptive. Proceeding with organizational dimensions of cybersecurity, the next paragraph will explore how AI can shape the administrative handling of cyber-risks and what implications it can yield for human resource management and the costs associated with it.

AI and Cybersecurity Management

Shielding information infrastructure from hostile intrusions requires not only increased alertness and cyber-threat mitigation via technical toolkits, but also an advanced organizational prowess and coordination. In this regard, artificial intelligence can step up efficacy of counter-cyberespionage and cybersecurity management by reducing time, cost, and human error-related risks during cyberattack detection.

Traditionally, organizations have had to handle the menace of cyberattacks manually, i.e., relying on direct human involvement to reverse-engineer malicious software in order to design appropriate patches or issue proper certificates to mend vulnerabilities. Normally, as a result of manually delivered inspections, security providers locate the signature of a malware and then design countermeasures to prevent similar cyberattacks in the future. These routines come as costs and labor-intensive processes that are prone to errors[25] and non-objective judgment,[26] and require "a large amount of time and effort alongside expertise and experience"[27] to examine malicious code carefully, track its logic, establish its triggering mechanism, and propose solutions. To illustrate, one of the most popular methods to locate unknown threats—specification-based detection—requires a manual development of detailed specifications on what constitutes a benign behavior in cyberspace. Although this method performs less poorly than other detection techniques, it is rather time-consuming,[28] which gives the edge to cyber adversaries in launching new attacks in the meantime. This tangibly obstructs the efforts of organizations to keep abreast with the high speed of malware development. As time is an utmost strategic resource in cyberspace, a heavy reliance on human manipulations in analyzing malware and locating it within a broader class of malign intrusions devours much time, while the patches issued for a particular malware become increasingly outdated

and obsolete. Importantly, due to repetitiveness and attention-oriented direction of work assignments, the personnel in cyber-defense units face a constant risk of fatigue and vigilance failures, resulting in accidents of varied magnitude.[29] All these factors result in organizations spending resources on cyberattack prevention without achieving an enduring, stable, and reliable mechanism able to withstand newer cyber-intrusions.

Artificial intelligence, in this regard, can reinstate organizations' capacity to tackle a continuous innovation of malware deployed against them in a time- and cost-efficient manner, as it can assume much of the work carried out by human agents, particularly in handling large datasets to classify a malware. This can lower the probability of human error, as AI-powered automated mechanisms can "generate non-trivial statements about correlations even experienced analysts would overlook, and automatically identify misconfigurations that could potentially lead to vulnerabilities."[30] One of the examples is an active cyber-defense using honeypots, which are a computer security measure that detects and derails attempts at unauthorized access to internal cyber-networks. Specifically, honeypots are implemented to lure attackers with the purpose of learning their methods and designing countermeasures. "Since the data in the honeypot is huge and without the function of status monitoring, the management error rate will be very high if it is manually monitored."[31] In this regard, AI-based solutions can run the code under scrutiny through multiple layers of algorithms making it possible to analyze malware on a self-sustainable *autonomous* basis. Another example is cross-site scripting attacks (XSS attacks) that allow cyber criminals to steal cookies and different types of sensitive information from web pages. Traditional methods against XSS attacks have seen a decline in efficacy, as it is "extremely time-consuming and error-prone to manually discover the keyword combination rules for new XSS attack statements."[32] The use of AI, however, proved to improve the robustness of XSS detection models credibly by relying on finely tailored algorithms, including Apriori algorithms classically used to establish association rules within databases with a great number of transactions.[33] Similarly to XSS attacks, deep learning algorithms can battle another nuisance known as web shells—a class of remote access Trojans—precisely by eliminating the need for "manual extraction of features," which was a source, along with low automation, of unsatisfactory performance of previous web shell detection methods.[34]

As AI solutions continue to learn on exponentially expanding datasets, their speed of analysis grows faster, and cyber-threat identification becomes ever more time-efficient. Besides, AI lowers the risk of human error substantially because it is able to sift through heaps of code to derive important security insights without historically contingent, and therefore increasingly outdated, expert knowledge which underlies knowledge bases of traditional intrusion detection systems.[35] As an example, in previously mentioned botnet detection procedures, deep learning solutions can verify the legitimacy of all features of incoming traffic without the need for experts' knowledge during feature selection,[36]
thus increasing the volume of features under inspection and covering a larger threat landscape in contrast to the analogous human-assisted procedure. As a result, the ability of increasingly autonomous AI-driven cyber-defenses to mitigate cyber threats swiftly, without as much human involvement as sometime ago, through identification and further patching wins time for those who defend over those who attack.

Furthermore, AI-based solutions proved instrumental in calibrating cybersecurity-related decision-making, especially when it comes to expert systems. Expert systems are tools that "assist intelligence analysts in conducting quality intelligence analysis to provide timely and accurate intelligence relevant to commanders and warfighters," for instance, by reducing redundant reporting and assisting political forecasting.[37] In this regard, ML-powered expert systems can fuse intelligence data in an increasingly broad and fast manner, which facilitates adoption of security measures and helps to optimize the use of limited resources for their execution.[38] Another forceful example is Bayesian attack graphs that help to determine the probability of cyberattacks and choose respective security measures thus contributing to "efficient security management and threat mitigation plans."[39] Some algorithms along with identification of vulnerabilities can "also recommend (sometimes perform) corrective actions."[40] Overall, optimized time resources allowed by AI coupled with neural nets that assist security planning "guarantee rapid situation assessment that gives a decision superiority to leaders and decision makers on any C2 level"[41]—a significant step forward when compared to traditional cyber-defense strategies.

All in all, artificial intelligence can introduce palpable improvements into the administration of cybersecurity mechanisms. AI can tangibly boost automation of cyber-threat intelligence, making it less vulnerable to human error and history-bound human expertise and thus faster and more cost-efficient in terms of cyber-detection. By reducing the presence of human operators, although not replacing them entirely, it can free up human resources previously allocated to execute mundane and tedious tasks to focus instead on other important areas of cybersecurity management. Finally, with such tools as ML-powered expert systems, AI can benefit decision-making and security planning by providing recommendations and evaluating options for response. The next section will examine how this and other previously outlined factors can enable AI to shape the structure of defense-offense dialectics and what implications it might have for the development of cyber-weapons.

AI and the Development of Cyber-Weapons

It is not only that security vendors and their client organizations monitor constantly emerging novelties in malware design and deployment. Similarly, cyber-perpetrators keep a careful watch on security providers and target organizations in a bid to understand institutional responses to their malicious products and introduce more effective upgrades. This forms a complex structure of interactions between both sides of cyber transactions, which has long been favoring imaginative powers and "market position" of cyber-intruders. Applied to cyber-defense, however, AI can help reshuffle defense-offense dialectics in cyberspace by raising the standards and requirements for effective and successful cyberattacks, thus forging favorable structural conditions for actionable cyber-protection.

Traditionally, the protection of computer systems that underpin the workings of many organizations has been developing along a bumpy pathway fraught with uncertainties, constant threats, and exposed vulnerabilities. This was caused largely by steady progress in the design of offensive cyber capabilities and their subsequent real-world application. The rise in cybercrime and hacking due to proliferation of cyber-technologies did generate demand for effective cyber-defense, but protection mechanisms have lagged behind innovation in cyber-weapons. The democratization of cyber-technologies made creation and deployment of malware an easily achievable task for those with sufficient technical expertise and, over time, even for those who lack it. These circumstances saw a rise of the entire industry of cyber-weapon production, which proposed constant innovation and multiple methodologies for cybercrime. Exposed to delinquent actions from anonymous entities, many organizations started to make generous investments in cyber-protection, but being proactive in this respect was obstructed by a rapid pace of cyber-weapon development and its deployment. Since cyber-perpetrators quite often have enough access to resources needed to construct a malware, organizations struggle to catch up with the tendencies in cyber-offense, and thus their protection measures are mostly motivated and informed by bitter experiences of past cyberattacks. To illustrate, zero-day attacks are still crippling many businesses, as "it is difficult to realize risk assessment of single zero-day vulnerability by existing methods,"[42] which are mostly narrowed to existing knowledge bases. Conventional cyber protection, therefore, has been largely backward-looking.

This can be palpably changed due to the adoption of AI-driven solutions that can make cyber-threat mitigation more productive than before. "In contrast to traditional signature-based systems, ML has generalization capabilities; i.e., learning algorithms can produce predictions for samples they have not seen before."[43] Overall, this predictive potential of AI makes cyber adversaries struggle to exceed the pace at which AI foresees new types of cyberattacks. Perpetrators would be pressed constantly to design new types of malware to bypass strong AI-powered cyber-defenses and obfuscate cyberattacks effectively in a new cybersecurity setting. To illustrate, since fairly early on, cyber-criminals have exploited zero-day vulnerabilities of complex systems before the release of proper patches by cybersecurity vendors. However, the present-day AI can conduct proper zero-day vulnerability assessment for organizations by relying on a "zero-day attack graph generation algorithm" that matches "preconditions and post-conditions of known vulnerabilities in network."[44] These techniques ensure "security hardening of target network when zero-day attack has not occurred, increase attack cost, and reduce the probability of attack success,"[45] thus making once the most hazardous type of cyberattacks—zero-days—much more restricted in their disruptive capacity.

Naturally, cyber criminals could try to use AI-driven malware for nefarious purposes to compromise AI-powered protection systems. However, not only is AI in itself a costly technology which requires substantial computational capacity and expertise,[46] but it is also rather difficult to harness AI without ample organizational resources. So far, creating a potent AI-based malware is much more demanding in technical and financial terms than adopting AI for malware detection. In the meantime, however, regular cyberattacks may end up in need of sophistication parallel to AI cyber-defense to prove successful. For instance, AI-assisted simulation of cyberattacks already empowers cyber-defensive strategies in the face of creative and innovative approaches to cyberattacking that are constantly deployed to serve malign causes. AI-supported attack planning and execution programs, in this regard, can "discover more plans than human experts due to intelligent algorithms and fast processing power" and "help non-experts to avoid the complexity of learning new knowledge, whilst save time, effort and resources."[47] In this way, more complete knowledge of possible attack plans lays an additional burden on cyber-perpetrators who have to innovate against powerful AI-enabled cyberattack simulation. "This may have a snowball effect and, for example, reduce the value of exploits and zero-days, slowing down the race to acquire vulnerabilities"[48] and considerably shrinking opportunities for those engaged in cybercrime.

In summary, artificial intelligence can raise the requirements for an effective, unexpected, and virulent cyberattack. AI's ability to predict modifications of malware and its behavior due to strong computational resources available to organizations seeking protection can place AI-powered

cyber-defense ahead of some of the trends in the construction of cyber-weapons. Although in this way AI can shift defense-offense dialectics in favor of the former, its application largely depends on sufficient organizational resources, which makes its use not as widespread as it could be otherwise, especially for individual users. The final section of this article will critically assess this impact of AI by unearthing weaknesses of AI defenses in spite of their valuable contributions and will establish how it might affect defense-offense dichotomy in the future if a fully operational AI-based malware becomes a normal practice for cyberattacks.

AI AND CYBERSECURITY: EMPOWERING CYBER-OFFENSE

As an emerging technology, artificial intelligence can exert an ambivalent impact on the state of cybersecurity. While offering seemingly productive insights into ways of enhancing risk-assessment and cyber-preparedness, AI can be equally disruptive for the cause of shielding cyber-infrastructures due to its technical limitations and its potential for ill.

Perils of AI as a Tool for Cyber-Defense

Although AI can largely strengthen cyber-defensive practices, it nonetheless has the potential to jeopardize cybersecurity of essential computer systems due to its intrinsic vulnerabilities toward adversarial examples. These are deliberate interferences or distortions within a data flow fed through ML algorithms that alter data fabric and derail cyber-threat detection processes. As a consequence, AI-driven solutions might provide erroneous results and mislead cybersecurity strategies. During exploratory adversarial attacks, for instance, perpetrators can train a deep neural network to infer input data from a functioning classifier which underpins a certain intrusion detection system and labels items as malicious or legitimate.[49] During an evasive adversarial attack, on the other hand, perpetrators trick machine learning algorithms into misclassifying input data and causing misdetection of intrusions. Some of these attacks, such as data injection attacks, can effectively change probability distribution in the workings of machine learning algorithms without being detected.[50]

Data poisoning—another malicious AI-driven technique—can feed in misleading data in machine learning algorithms, which can multiply opportunities for spamming, smart phishing, and data exfiltration. Poisoning attacks might be launched not only against AI-powered cyber defenses, but also against AI-based tools and applications by infecting them with untrusted data. This makes adversarial attacks a prominent threat against machine learning algorithms in charge of cyber-protection, as they can cripple defenses of unmanned aerial vehicles, self-driving cars, and IoT devices, thus causing immediate real-world damage—injuries and even deaths. In order to mitigate this threat, researchers apply adversarial ML techniques, including generative adversarial networks[51] and adversarial retraining (when adversarial examples are deployed against training datasets)[52] to simulate adversarial attacks and better prepare for proper response, but results are not yet universally actionable. To make matters worse, given the increasing availability of AI kits in dark markets and open sources, the ability of cyber-perpetrators to hijack these AI supply chains and examine AI-assisted or -powered defenses in order to spot exploitable loopholes in their algorithms increases substantially. That being said, devising adversarial attacks is still very difficult due to intricacies and complexities of neural networks,[53] which are still impossible to reverse-engineer.[54] Overall, this helps to preserve the advantage of AI cyber-defense in most cases.

To recapitulate, the key weakness of AI-powered cyber-defenses is their vulnerability to adversarial attacks against machine learning algorithms and data poisoning that might compromise the accuracy of cyber-threat detection. Although attacking algorithms effectively is still problematic due to the lack of proper resources at cybercriminals' disposal, a further proliferation of AI already makes available open-source AI toolkits that can be used in staging adversarial attacks.

AI as a Building Block for New-Generation Cyber-Intrusions

Another risk stemming from AI is its prospective contribution to the development of cyber-weapons of unprecedented sophistication and technical intricacy, which would augment dramatically the ability to harm and exploit. Most primitive uses of machine learning for malevolent purposes, such as those to undo CAPTCHAs or test user passwords across multiple websites,[55] have long been recorded. More nuanced, thus more hazardous, applications of AI, however, can exceed in an unprecedented fashion what has yet been known as severe consequences for cyber-protection. In this regard, all the benefits surrounding the adoption of AI-based solutions for cybersecurity mentioned above nonetheless can have flipside representations in cyber-offensive strategies. For instance, similarly to how AI can enhance precision of malware detection and prediction of its possible variations, it can use the same technique to obfuscate the malware effectively during a cyberattack. Specifically, when a malicious program nests itself inside the targeted environment, AI can enable the malware to learn key features of that environment and camouflage itself accordingly to act undetected. This is possible due to the AI-based malware's

capacity to analyze past events of the infected system and effectively adjust its malign behavior to the surrounding dynamics, delete itself automatically, update its own versions, and trick the detection systems.[56] Furthermore, just like reducing the role of humans in cyber-threat intelligence, AI can limit the involvement of a perpetrator throughout the cyberattack, as the AI-powered malware is expected to act mostly autonomously. This might lead to an increased difficulty in tracing the source of cyberattack and conduct attribution.

Although a malware entirely propelled by artificial intelligence has not yet been reported as deployed for nefarious purposes, it has already been prototyped. IBM's DeepLocker, for instance, has been a groundbreaking advancement in the black-hat culture, as this malware is capable of self-obfuscation and can use face and voice recognition, as well as geolocation, to identify and infect its targets.[57] The key takeaway from DeepLocker's deployment, which was conducted in a controlled and safe testing-ground setting, is that its composition built of deep neural networks (DNNs)—the most advanced machine-learning technique so far—proved itself a decisive factor in making the malware so delicate and effective in cyberattack execution. The key problem with DNNs is that it is not yet possible to reverse-engineer them at the moment due to their superior complexity, which makes a code obfuscated with the help of such networks an extremely dangerous tool in the hands of criminals.[58]

While all these potential dangers of AI deployed in cyber-offense appear severe and even gruesome, one may ask a reasonable question regarding the probability of such developments. After all, what determines the imminence of AI-powered cyberattacks at present? The technology of AI, as many other cyber-technologies, requires openness and availability of its constituent parts out on the market. The more data and tools are shared online, the faster and more reliable the outcomes of machine learning applications are. However, because of broader availability of open-source research on AI and further proliferation of technological components needed for machine learning, cybercriminals can become increasingly capable of upgrading their weapons using machine learning. Some known viruses such as Swizzor Trojan, WannaCry, or Emotet, as well as such technologies as DeepFake, are all already equipped with some features of artificial intelligence, offering some shortcuts to the design of a fully AI-driven malware. This malware will be able to mimic private communications credibly, unleash its poisonous payload through face or voice recognition, and conduct effective impersonation attacks. The latter has already become a tangible problem: in 2018 two-thirds of businesses suffered deep learning-based impersonation attacks, with 73% of them being damaged financially as a result.[59]

The arrival of AI-based cyber-weapons, therefore, may empower cyber-perpetrators enormously, reinstating their advantageous position as malware innovators. What hampers the possibility of cyber-offense to regain its dominance in cyber-threat innovation is the fact that leveraging AI for cyberattacks effectively and successfully requires many more resources and expertise than is currently available to cyber-perpetrators. The distance, however, between AI-powered cyber-offense and AI-driven cyber-defense seems to shorten as the progress of machine learning methods expands. Moreover, with more AI components available online, however simple they may still be, on the dark market or even in open-sources (such as Kali Linux depository, Google's TensorFlow dataflow repository, or GitHub), the ability of cyber-criminals to build AI-assisted or -powered weapons might increase substantially, with some security vendors professing its first manifestations to surface 1-3 years from now.[60]

CONCLUSION

The analysis of the ways and means of empowering cybersecurity strategies of government and private organizations through artificial intelligence predicts major changes to commonly accepted standards of both cyber-defense and cyberattacks. As cyberespionage remains a cause of severe material and reputational damage, especially for intelligence institutions in charge of keeping information secure, this research suggests a number of ways that a ground-breaking technology like AI can benefit cyber-protection strategies of these organizations. First, AI can strengthen resilience and robustness of cyber-threat detection systems, making them more accurate and effective in countering intrusions and detecting malware. This can step up preventive and proactive capacity of cyber-defenses significantly, as now they can predict modifications of malware and use more effective deception techniques such as honeypots to preempt cyberattacks. Also, AI can make cyber-threat management faster, more automated, more cost-efficient, and less prone to human error. It can also free up some human resources dealing with mundane and tedious tasks and facilitate decision-making and security planning by providing recommendations for action. Finally, AI can raise the threshold for an effective, unexpected, and virulent cyberattack, as AI's ability to predict modifications of malware renders cyber-weapon innovation more problematic than before, reshuffling defense-offense dynamics profoundly by giving cyber-defense an edge over cyber-offense.

Nonetheless, AI-powered cyber-defense does suffer from weaknesses, such as its vulnerability to adversarial examples launched against machine learning algorithms that can diminish the reliability of cyber-threat detection. Also, AI can be used in the development of malware which can have

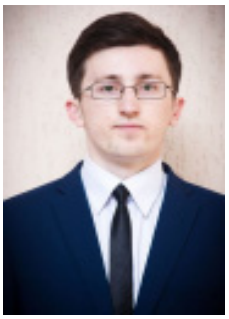
more devastating capabilities than its present-day analogues. As AI is further democratized, its availability in open-source markets can compensate for the lack of computational resources available to cyber-criminals, which otherwise constrains them, and enable them to create an AI-driven malware. Consequently, the upper hand of AI-powered cyber-defenses might pose diminishing returns if concerns about AI-powered malware materialize. The juxtaposition of these trajectories is a convincing testimony that the impact of AI on cybersecurity and cyberespionage will be strictly dialectical in a traditional Hegelian sense: while empowering cyber-defense, it will also shape the practice of cyber-offense, incarnating the unity and struggle of the opposites. On one hand, they both will be mutually reinforcing—evolution in cyber-defense will propel innovation in cyber-weapons, while upgrades of cyberattacks will push the progress in cyber-protection. On the other hand, they will remain reciprocally disruptive, as the consequences of their contention could be dramatic for the causes guided by intelligence institutions around the world, including international peace and security. Therefore, in their effort to preserve the integrity of cyberspace from cyberattacks and cyberespionage, governments—and especially their intelligence components—can largely benefit from implementing AI in cyber-defense, but they should pursue this goal with much caution, given AI's intrinsic vulnerabilities and its potential for ill. Only in that way can it be possible for the Intelligence Community to perpetuate the advantage of cyber-defense over cyber-intrusions to the benefit of security interests shared by all.

[Author's Note: I would like to thank Dr. Giangiuseppe Pili for his helpful comments on this research and valuable insights on many scholarly topics, which he kindly shared with his former student, and also the editor of *AIJ*, Dr. William Spracher, for his warm welcome and active support of this publication.]

NOTES

[1] Nicole Perlroth, Mark Scott, and Sheera Frenkel, "Cyberattack Hits Ukraine Then Spreads Internationally," *The New York Times*, accessed May 5, 2020, https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html.
[2] Russell Buchan, *Cyber Espionage and International Law* (Oxford, UK: Hart Publishing, 2018), 46.
[3] Elspeth D. Bryan and Anthony H. Smith, "North Atlantic Treaty Organization: Challenges to Collective Defense in Cyberspace," *American Intelligence Journal* 35, no. 2 (2018): 42.
[4] "National Cyber Strategy of the United States of America," The White House, last modified 2018, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
[5] CDR (USNR) Catherine S. Deppa, "U.S. Cyber Command: An Overview," *American Intelligence Journal* 34, no. 1 (2017): 13.
[6] Giangiuseppe Pili, "Epistemology and Intelligence – Some Philosophical Problems to Be Solved," *The International Journal of Intelligence, Security, and Public Affairs* 20, no. 3 (2018): 265.
[7] Pelle de Meij, "Hegelian Dialectics as a Source of Inspiration for the Intelligence Community," *American Intelligence Journal* 33, no. 1 (2016): 69.
[8] Buchan, *Cyber Espionage*, 18.
[9] J. Rocco Blais and Adam M. Jungdahl, "Artificial Intelligence in a Human Intelligence World," *American Intelligence Journal* 36, no. 1 (2019): 109.
[10] I. Ahl, "The Relevance of Endpoint Security in Enterprise Networks," in *Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities and Implications for Theory, Policy and Practice,* eds. E.G. Carayannis et al. (New York: Springer, 2014), 346.
[11] Ahl, "The Relevance of Endpoint Security," 346.
[12] Italics are the author's.
[13] J. Papalitsas, S. Rauti, J. Tammi, and V. Leppänen, "Honeypot Proxy Framework for Deceiving Attackers with Fabricated Content," in *Cyber Threat Intelligence*, eds. A. Dehghantanha et al. (Cham, Switzerland: Springer International Publishing, 2018), 242.
[14] Ahl, "The Relevance of Endpoint Security," 348.
[15] F. Pecorelli, F. Palomba, D. Di Nucci, and A. De Lucia, "Comparing Heuristic and Machine Learning Approaches for Metric-Based Code Smell Detection," IEEE/ACM 27th International Conference on Program Comprehension (ICPC) (Montreal, 2019), 93.
[16] A. Amini, K. Banitsas, and J. Cosmas, "A Comparison between Heuristic and Machine Learning Techniques in Fall Detection Using Kinect v2," IEEE International Symposium on Medical Measurements and Applications (MeMeA) (Benevento, 2016), 1.
[17] V. Kanimozhi and T. Jacob, "AI-Based Network Intrusion Detection with Hyper-Parameter Optimization Tuning on the Realistic Cyber Dataset CSE-CIC-IDS2018 Using Cloud Computing," *ICT Express* 5, no. 3 (2019): 211.
[18] L. Sikos, *AI in Cybersecurity* (Cham, Switzerland: Springer International Publishing, 2019): v.
[19] Kanimozhi, "AI-Based Network Intrusion Detection," 211.
[20] F. Tao, Ch. Cao, and Zh. Liu, "Webshell Detection Model Based on Deep Learning," in *AI and Security: 5th International Conference, ICAIS Proceedings* 1, no. 4, eds. X. Sun et al. (Cham, Switzerland: Springer International Publishing, 2019), 408.
[21] M. Omar, J. Baldwin, and A. Dehghantanha, "Leveraging Machine Learning Techniques for Windows Ransomware Network Traffic Detection," in *Cyber Threat Intelligence*, eds. A. Dehghantanha et al. (Cham, Switzerland: Springer International Publishing, 2018), 94.
[22] Sajad Homayoun, Marzieh Ahmadzadeh, Sattar Hashemi, Ali Dehghantanha, and Raouf Khayami, "BoTShark: A Deep Learning Approach for Botnet Traffic Detection," in *Cyber Threat Intelligence*, eds. A. Dehghantanha et al. (Cham, Switzerland: Springer International Publishing, 2018), 140.
[23] Homayoun, "BoTShark," 138.
[24] Z. Ye, Y. Guo, and A. Ju, "Zero-Day Vulnerability Risk Assessment and Attack Path Analysis Using Security Metric," in *AI and Security: 5th International Conference, ICAIS Proceedings* 1, no. 4, eds. X. Sun et al. (Cham, Switzerland: Springer International Publishing, 2019), 266.
[25] L. Sikos, D. Philp, C. Howard, S. Voigt, M. Stumptner, and W. Mayer, "Knowledge Representation of Network Semantics for Reasoning-Powered Cyber-Situational Awareness," in *AI in Cybersecurity* ed. L. Sikos (Cham, Switzerland: Springer International Publishing, 2019), 19.

[26] L. Chen, Ch. Yang, F. Liu, D. Gong, and Sh. Ding, "A Security-Sensitive Function Mining Framework for Source Code," in *AI and Security: 5th International Conference, ICAIS Proceedings* 1, no. 4, eds. X. Sun et al. (Cham, Switzerland: Springer International Publishing, 2019), 422.
[27] S. Khan and S. Parkinson, "Review into State of the Art of Vulnerability Assessment Using AI," in *Guide to Vulnerability Analysis for Computer Networks and Systems: An AI Approach*, eds. S. Parkinson et al. (Cham, Switzerland: Springer International Publishing, 2018), 25.
[28] J. Li, Y. Qu, F. Chao, H. Shum, E. Ho, and L. Yang, "Machine Learning Algorithms for Network Intrusion Detection," in *AI in Cybersecurity*, ed. L. Sikos (Cham, Switzerland: Springer International Publishing, 2019), 156.
[29] Ben D. Sawyer, Victor S. Finomore, Gregory J. Funke, Gerald Matthews, Vincent Mancuso, Matthew Funke, Joel S. Warm, and Peter A. Hancock, "Cyber Vigilance: The Human Factor," *American Intelligence Journal* 32, no. 2 (2015): 152.
[30] Sikos, *AI in Cybersecurity*, v.
[31] Yu Wenjin, Jiang Yixiang, and Lin Yizhen, "Active Defense System of Industrial Control System Based on Dynamic Behavior Analysis," in *AI and Security: 5th International Conference, ICAIS Proceedings* 1, no. 4, eds. X. Sun et al. (Cham, Switzerlsnd: Springer International Publishing, 2019), 632.
[32] Chen, "Security-Sensitive Function," 215.
[33] Ibid., 216.
[34] Tao, "Webshell," 408.
[35] Li, "Machine Learning Algorithms," 152.
[36] Homayoun, "BoTShark," 138.
[37] Robert D. Folker, Jr., "Arming the Intelligence Analyst for Information Warfare," *American Intelligence Journal* 30, no. 2 (2012): 13-14.
[38] E. Tyugu, "AI in Cyber-Defense," in 3rd International Conference on Cyber Conflict, IEEE
(2011), 4.
[39] Khan, Vulnerability Assessment, 17.
[40] Ibid., 18.
[41] Tyugu, "AI in Cyber-Defense," 8.
[42] Ye, "Zero-Day Vulnerability," 266.
[43] L. Muñoz-González and E. Lupu, "The Security of ML Systems," in *AI in Cybersecurity*, ed. L. Sikos (Cham, Switzerland: Springer International Publishing, 2019), 48.
[44] Ye, "Zero-Day Vulnerability," 268.
[45] Ibid., 266.
[46] Forbes Insight Team, "Should You Build or Buy Your AI?" *Forbes*, accessed May 5, 2020, https://www.forbes.com/sites/insights-intelai/2019/05/22/should-you-build-or-buy-your-ai/#789a9ef4441d.
[47] Khan, "Vulnerability Assessment," 19.
[48] M. Taddeo, "Three Ethical Challenges of Applications of AI in Cybersecurity," *Minds and Machines* 29, no. 2 (2019): 188.
[49] Y. Shi, Y. Sagduyu, K. Davaslioglu, and R. Levy, "Vulnerability Detection and Analysis in Adversarial Deep Learning," in *Guide to Vulnerability Analysis for Computer Networks and Systems: An AI Approach* ed. S. Parkinson et al. (Cham, Switzerland: Springer International Publishing, 2018), 211.
[50] H. Li, J. Zhang, and X. He, "Design of Data-Injection Attacks for Cyber-Physical Systems Based on Kullback-Leibler Divergence," *Neurocomputing* 361, (2019): 77-84.
[51] D. Zeng, Y. Dai, and F. Li, "Adversarial learning for distant supervised relation extraction," *Comput. Mater. Continua.* 55, no. 1 (2018): 121-136.
[52] Muñoz-González, "The Security of ML Systems," 75.
[53] B. Dickson, "The Malware of the Future Will Have AI Superpowers," Gizmodo, accessed May 5, 2020, https://gizmodo.com/the-malware-of-the-future-will-have-ai-superpowers-1830678865.
[54] O. Or-Meir, N. Nissim, Y. Elovici, and L. Rokach, "Dynamic Malware Analysis in the Modern Era – A State of the Art Survey," *ACM Computing Surveys (CSUR)* 52, no. 5 (2019): 16.
[55] Jessica Cussins Newman, *Toward AI Security: Global Aspirations for a More Resilient Future*, CLTC White Paper Series (2019): 18.
[56] Pieter Arntz, Wendy Zamora, Jérôme Segura, and Adam Kujawa, "When artificial intelligence goes awry: Separating science fiction from fact," Malwarebytes Labs, accessed May 5, 2020, https://resources.malwarebytes.com/files/2019/06/Labs-Report-AI-gone-awry.pdf.
[57] Kumar Patel, "Next-Generation Solutions for Next-Generation Security Risks," *CINN Group, Inc.* 130 (2019): 18.
[58] Or-Meir, "Malware Analysis," 16.
[59] Arntz, "Artificial Intelligence."
[60] Arntz, "Artificial Intelligence."



Roman Kolodii is an intern at the Center for Security Studies, ETH Zurich, and is currently completing an International Master's degree in Security, Intelligence, and Strategic Studies administered by the University of Glasgow (Scotland) jointly with Dublin City University (Ireland) and Charles University Prague (Czech Republic). Originally from Ukraine, he received both his bachelor's and master's degrees in International Relations and Chinese from Taras Shevchenko National University of Kyiv. After working for a private company on sentiment analysis and media intelligence, and then for the United Nations Development Program on e-governance and innovation under the Ukraine Parliamentary Reform Project, he has delved into the security and geopolitics of emerging technologies, exploring digitization, cyber intelligence, artificial intelligence, and military drones. His latest peer-reviewed publication for the international scholarly journal Aretè *discusses philosophical challenges to cyber-technological transformation of mankind. Fluent in Ukrainian, English, Russian, and Chinese, Roman is focusing his upcoming master's dissertation on examining, from a strategic perspective, cybersecurity cooperation among the United States, the United Kingdom, China, and Russia.*

Window Dressing:
Applying the RASCLS Framework in Foreign Policy

by Mason D. Goad

[Editor's Note: This article was originally approved for publication by the Center for the Study of the Presidency and Congress, located in Washington, DC, in its *Presidential Fellows Review* in July 2020. It was slightly revised and is reprinted here with the permission of the editor.]

OVERVIEW

This project's goal is to explore the feasibility and application of using the RASCLS framework in agent recruitment as a framework for foreign policy. RASCLS is an acronym standing for Reciprocation, Authority, Scarcity, Commitment and Consistency, Likeness, and Social Proof. The project seeks to explain the RASCLS framework, demonstrate its use throughout history, and then explore ways in which it could be implemented today. The project's design will explain the individual tenets of the RASCLS framework, explain how it has been utilized and the state and international levels, and how it could be applied when dealing with adversarial foreign countries, such as the Russian Federation. Through this research it is apparent that the RASCLS framework has been a well-used tool at the state level throughout history, and is fully applicable in contemporary international relations as framework for national doctrine regarding foreign policy.

Window Dressing (n.)
An adroit but superficial or actually misleading presentation of something; designed to create a favorable impression.

All the world's a stage, and all the men and women merely players;
They have their exits and their entrances;
And one man in his time plays many parts, his acts being seven ages.

— William Shakespeare,
from *As You Like It*

INTRODUCTION

The greatest theories are said to work across time and space, across gender and culture, across religions, environments, and anything else that may make two things distinct. However, the scope of the theory is often forgotten, as theories are often applied on the level at which they were first conceived. This could be an individual level, a regional level, a state level, and all the way up to the global level, and yet the greatest of theories will transcend even this. One such theory is the RASCLS framework, applied in agent recruitment within the human intelligence discipline. This theory is applied on an individual level, when an intelligence case officer is seeking to recruit an agent for the purposes of espionage. However, if RASCLS is truly a robust theory, we might be able to apply it to the international level as well, not as a framework for agent recruitment but as a framework for foreign policy and interstate interaction.

The tenets of the RASCLS framework are as follows: Reciprocation, Authority, Scarcity, Commitment, Consistency, Likeness, and Social Proof. One need only look to America's first foreign policy document, the *Declaration of Independence*, to see pieces of the RASCLS framework present at the international level. Therein, the founders spoke of the authority of government, the unfair reciprocation suffered, and the social proof that it offered as evidence. The British lost the allegiance of their citizens for having violated parts of the RASCLS framework, not in words but in deeds. By analyzing this episode, and others, perhaps this framework could be altered, in order that through foreign policy and global interaction one state might be able to win over the hearts and minds of the people of another state, even against that foreign government's wishes, and in spite of that government's best counter-efforts.

This reinvention of the RASCLS framework is designed for the strategic level. This is not simply propaganda, but a carefully constructed ploy, an international psychological game, to manipulate entire states. Explaining this theory will be done in seven sections, mirroring the RASCLS tenets and

ultimately laying the groundwork for a new approach to international relations. Presenting this theory is done in the hope that it will be a strategy for creating and maintaining an enduring peace, knowing that the art of peace need not be peaceful, only successful. It is the supreme art of peace to subdue an enemy by befriending it.

ACT 1: RECIPROCATION

Reciprocation is the art of returning in like kind: a compliment for a compliment, a blow for a blow. Individuals seek out relationships that are mutually beneficial; a parasitic relationship is avoided, but each has Reciprocation in common. Mutually beneficial relationships exist because that benefit is reciprocated: each party works for the whole group, not just itself. Parasitic relationships are avoided, as the benefit received by one party is never reciprocated. Like individuals, states seek out relationships with other states that are beneficial, with these benefits being reciprocated.

At the international level, beneficial Reciprocation can be seen in trade negotiations and military treaties, such as the cost-sharing formula based on gross national product that determines the size of each contribution to NATO.[1] Reciprocation is not only useful in economic decisions. Negative Reciprocation—though reciprocation nonetheless—can be seen in foreign policy and military decisions, such as "mutual assured destruction," which by its very name indicates that any attempt at assured destruction will be mutually reciprocated.[2] Using Reciprocation at the strategic level is a form of selfish altruism. In implementation, we would help others, so that they are obligated to help us. It can be anticipated that an adversarial government will take the benefit and not realize the inescapable trap into which it walked. Failure to reciprocate will leave it dealing with a public relations nightmare on the international stage, as the United States could easily lambast that government as a global parasite. However, reciprocating the benefit—especially on a continual basis—leaves it vulnerable to other tactical- or operational-level tenets of the RASCLS framework, such as Likeness and Social Poof. Continued Reciprocation also leaves the target vulnerable to increased traditional intelligence operations and strategic-level RASCLS tenets, such as Authority.

Reciprocation should not be considered as only applicable in the theaters of economics, trade, or defense. Essentially anything could be used to set the Reciprocation trap, such as national identity. Take the 75th anniversary of D-Day, which was held June 6, 2019, as an example. A celebration of the anniversary of the invasion to liberate France from Nazi Germany was held, with many world leaders in attendance, including the Chancellor of Germany. However, Russia had not been invited. The Second World War holds a special place in the collective Russian identity, and the nation's contributions to the war effort had been wholly dismissed by its former allies at this anniversary. It stands to reason that such a dismissal would resonate with Russians who hold fast to that identity.[3] Perhaps it is not surprising, therefore, that the day after the anniversary a Russian frigate dangerously maneuvered in proximity to a U.S. battleship in a clear display of aggression, making international headlines in hours.[4]

Reciprocation is the art of returning in like kind...

At first glance, the West seems to have lost a perfect opportunity diplomatically, but it is doubtful that all of the Western countries simply "forgot" to invite Russia. No, this was almost certainly agreed upon, probably to attack the Russian identity by dismissing its military. However, this dismissal was then negatively reciprocated with the Russians harassing the U.S. military the following day. This demonstrates that Reciprocation is constant—both negative and positive types—and every decision must be carefully weighed in terms of the trap being set. Will the adversary be forced to reciprocate the benefit, or will it be free to reciprocate the detriment? The media firestorm that arose in the aftermath of Russia's actions at sea was predictable. The United States had practically lambasted the Russians as international parasites, and Russia's official stance was a complete denial of the events as portrayed by the United States. Of course that was Russia's stance! Russia's hand was ultimately forced, as it could not justify its actions with a "why did you not invite us to your party yesterday?" That argument would only make Russia look petty and childish.[5]

To achieve constant positive Reciprocation, and implement the rest of the RASCLS framework, a closer analysis of each action, its perceptions, and its consequences must be conducted. This is especially true in fragile military relationships, in which unintended negative Reciprocation can prove fatal.

ACT 2: AUTHORITY

Authority inspires obedience, and without obedience there would be political instability. Therefore, safeguarding the Authority of the state is a priority for practitioners of national security. However, a challenge exists because Authority itself is an abstract concept. What causes the notion of Authority to take

hold in the minds of the citizens? What might destroy that notion? It is one thing to market the U.S. government to a target population, but true success will be found only when the adversarial regime collapses so that a more favorable one can be rebuilt.

Authority inspires obedience, and without obedience there would be political instability.

Based on concepts developed by sociologist Max Weber, there are three types of Authority to target: traditional, legal-rational, and charismatic.[6] Generally, these types work together, but one can see in modern times what happens when these pillars collapse. The Trump administration is an example of a political authority which does not reflect Weber's ideas at all. Traditionally, this administration is unprecedented. Donald Trump never held office before; even Ronald Reagan was the governor of California before becoming president. On a legal-rational basis, the fact that Trump did not win the popular vote in the election concerns those who erroneously believe the United States to be a direct democracy, and not a republic. On a charismatic basis, the Trump administration has purposefully crafted an image against this. Rather than the smooth-talking politician, as people of all nations are accustomed to, the Trump campaign and administration purposefully designed Trump's image as an average person. Such rejection of Weber's concepts has left the administration open to criticisms, which are easily conveyed to a mass audience.

Successful criticism of Authority undermines the legitimacy of the entire political body and its effectiveness in foreign policy. When such criticisms can be relayed to the public, unrest will brew in the disillusioned masses. In dealing with this rising unrest, the state will be distracted from implementing effective foreign policy. This was the case in 1970, when Chairman Andropov of the Committee for State Security, or KGB, sent a request to the Central Committee of the USSR to support the Black Panthers in their militant struggle against the U.S. government. This was to "distract the attention of the Nixon administration from pursuing an active foreign policy."[7] It should be noted that this attempt at undermining Nixon's effectiveness by exacerbating pre-existing domestic tensions took place in the middle of the Vietnam War. At the conclusion of that conflict, the U.S. ultimately failed its foreign policy objective of containing communism in Southeast Asia.

These attempts at undermining Authority were not limited to supporting militant groups such as the Black Panthers, but also in altering public opinion in general. For example, Gus Hall, General Secretary of the American Communist Party, wrote to the Soviet Union for assistance in granting Jesse Jackson an honorary doctorate in history from Moscow State University. Hall requested this conferral, as Hall understood that Jackson being able to claim "Dr." as a title would help to increase his status as an individual authority in American political circles. To the unaware observer this title would elevate Jackson, and thus his leftist leanings, to seemingly equitable authoritative status as other political leaders of the era. Whether or not Hall's request was approved is unknown. However, it shows that communist strategists worked to undermine the Authority of the U.S. government by using saboteurs to change perception of legal-rational Authority entirely, not simply to cause disruption and distract the political authority.[8]

Learning to create such political instability for others will help the U.S. bring down adversarial regimes. Stability exists when the actions of the Authority are legally and socially accepted. A stable Authority exists so long as there is strong correlation between the actions and expectations of government but, if that correlation falters, instability arises.[9] No government has a perfectly correlated line; at some point the justification and acceptance diverge, and that is where the faults in the perceptions of Authority can be exploited. Once those areas are found, covert campaigns could be waged to cause internal disruption and sway public opinion. At the tactical and operational levels, agents could be trained as saboteurs to continually disrupt a government's effectiveness in its day-to-day operations, much like what the Office of Strategic Services intended for the French in the Second World War.[10] The strategic level will necessitate broader campaigns against the Authority itself, such as by attacking the political system or the face of the regime directly.

ACT 3: SCARCITY

Scarcity, by definition, is the opposite of abundance; however, at the strategic level what is scarce is more abstract than material objects. What must be crafted in the application of Scarcity is the notion that some abstract concept in the minds of the people, such as security, is difficult to achieve due to its lack of abundance. In purposefully crafting such notions, both the target government and the target population can then be manipulated through various means. As a result of that manipulation, the actions of the targets can be exploited to support the applications of the prior two tenets: Reciprocation and Authority.

Scarcity must be applied in three parts, beginning at the tactical level, and working up to the strategic level. Beginning at the tactical level, tactical instruments can help to create the illusion that certain prospects and securities are scarce. Sanctions, for example, are tactical instruments which can help to craft the illusion that economic security is scarce. Consider for a moment that in 2019 the United States put sanctions on the Russian Federation with practically no fanfare or announcement. Although written a year ago, the lack of media attention when the sanctions were imposed took Russians by surprise.[11] The esoteric realities and consequences of such sanctions are extremely difficult for the target government to explain to the target population, and after the sanctions they will fade from the collective memory of the target population. Once the collective memory has faded, additional sanctions can be applied and then, once the memory of those sanctions has faded, additional sanctions can be applied, and that cycle can continue for as long as needed. Eventually, the target population will begin to believe that their scarce chances at achieving economic security are either of natural occurrence or due to the incompetence of the target government. Once the reality of desperation begins affecting the target population, and the notion that such scarce economic stability has been solidified in the minds of the population, the next stage in the application of Scarcity can begin.

Determining the target population's perceptions could be conducted by surveys and analyzing media publications (essentially HUMINT and OSINT collection and analysis).

Depending on the popular opinion—whether the target population believes that its situation was naturally occurring or it blames the target government—directs the next step in the process. Determining the target population's perceptions could be conducted by surveys and analyzing media publications (essentially HUMINT and OSINT collection and analysis). If the target population blames the target government, then Scarcity will complement Authority by giving another angle of attack for undermining the perceptions that the target government is a legal-rational authority. If the target population believes that its situation is naturally occurring, using prospect theory to manipulate the target population to turn against the target government is the next step. Prospect theory basically states that individuals value gains and losses differently. Losses have an emotional impact, and are thus avoided more. Gains, even the smallest of gains, are more preferred, and therefore when presented with a loss and a gain the target can be expected to choose the gain, even if that decision will ultimately work to the detriment of the target in the long term.[12] There is no way for a target government to win in this situation, once Scarcity has been properly applied. Either the Reciprocation trap will lead to further exploitation, or the Authority will be targeted in some way.

Take West and East Germany as examples, whose proximity to Western and Soviet power and importance to military partners made chances at surviving hostilities from either side scarce. It is not surprising, therefore, that the German Socialists, seizing the initiative, were the first to advocate the policy of *détente*, which was then quickly reciprocated by West German authorities. Lacking advancements in the Reciprocation trap, the Soviets opted to destabilize the West German government by exposing the Nazi past of Chancellor Kurt Kiesinger. It was understood that, if Kiesinger did not cooperate due to blackmail, his NATO partners would advocate for his removal from office in adherence to détente. Kiesinger resigned from office within a year of this plan being implemented.[13] The Soviets also exploited the Reciprocation trap in the United States after Scarcity was applied via détente. For example, in 1970 Soviet delegations were instructed to "further contacts with liberal and opposition circles" and "criticize as widely as possible the obstacles set by the USA along the path to improved relations," as the delegation operated within the United States.[14] Détente was the smokescreen. Scarcity was the strategy.

In summary, Scarcity—as a strategy—is a supporting tenet to assist in setting the Reciprocation trap, or to undermine Authority, It also provides the subtlety that RASCLS requires.

ACTS 4 & 5: COMMITMENT AND CONSISTENCY

The notion that an adversary can commit to any course of action and act consistently in any interactions are extremely important factors accounted for when one government seeks to work with another in any capacity. A government that is seen as non-committal may be too weak to work with. A government that does not act consistently may be somewhat irrational and impossible to work with. When attempting to undermine an adversary, one should look for ways to make it appear non-committal and inconsistent to other states and to the adversary's own citizens, while attempting to make oneself appear as committed and

consistent. Commitment and Consistency are applied in either a state of conflict or a state of cooperation, respectively.

To deal with a conflictual scenario, one must be able to commit. Think of this in terms of the game of "chicken," in which two parties are in a natural state of conflict. Imagine it as two cars driving down the road with a head-on collision being inevitable unless one of the cars swerves, but that driver will be branded a "chicken."[15] No better example of this exists than the Cuban Missile Crisis. After the failed Bay of Pigs invasion in 1961, Cuba requested that the Soviet Union place nuclear missiles on its territory to dissuade the U.S. from attempting anything of that sort again. Khrushchev agreed, but when American U-2 Spy planes discovered the missiles the Kennedy administration formed a naval blockade, issued an ultimatum that it would not permit any additional shipments to reach Cuba, and demanded that the missiles already in Cuba be removed.

The Crisis carried on for 13 days, and it was clear Kennedy would commit to his word and fire on any ship that attempted to run the blockade. Tense negotiations followed and, at the conclusion of the Crisis, the Soviet Union agreed to pull back all nuclear missiles from Cuba if the United States gave a public declaration that it would not attack Cuba. The United States also agreed to remove its missiles from Turkey, but this agreement was kept secret at the time. Therefore, to the entire world it appeared as if the Soviet Union, coming to the aid of a close ally, refused to commit its assistance. It was a national embarrassment for the Soviets.[16] The Kennedy administration's ability to commit to its course of action more than the Soviets were willing to do played out on a world stage, leaving lasting perceptions of the will of each government. In the end, the Kennedy administration successfully employed Commitment as a strategy, knowingly or unknowingly, by making the United States appear as if it was willing to stand firm, while the Soviet Union was not, not even by its allies.

On a cooperative basis, Consistency must be employed. It is best to think of this in terms of the famed anecdote of the "prisoner's dilemma." In this hypothetical scenario two prisoners are separated, and each is aware that if he/she confesses and incriminates the other, he/she will receive a lighter sentence. However, if the other confesses and incriminates both, he/she will receive a harsher sentence. When the scenario plays out once or twice, one prisoner will confess, but played out multiple times the prisoners will learn that if neither of them says anything neither can be convicted. As such, the prisoner's dilemma shows that, when two parties are thrown into a natural state of conflict, cooperation is the best way to alleviate conflict.[17] Therefore, how did Khrushchev know that cooperation with Kennedy during the Cuban Missile Crisis was possible? The reason is that it was proven only a few months earlier during the Berlin Crisis of 1961.

After the Soviet Union constructed the Berlin Wall and issued an ultimatum for the removal of Allied forces from West Berlin in 1958, the Allies refused. By 1961, just before the Cuban Missile Crisis began, a tank standoff was taking place at Checkpoint Charlie between the Allies and the Soviets. Kennedy and Khrushchev cooperated directly and reached an agreement that the Allies would not be so hardline vis-à-vis Berlin if the Soviets would back up their tanks first. Khrushchev agreed, and slowly all the tanks dispersed. The Berlin Wall remained, but so did the Allies, clearly in contrast to the Soviet ultimatum. However, the precedent that the Kennedy administration set by showing its ability to be consistent in both its commitments and cooperation may have saved the world only a few weeks after this incident.

Commitment and Consistency, as strategies in the RASCLS framework, are connected in a cycle, such as "yin and yang." One should commit to a stance that will invoke conflict, and then consistently seek to lessen that conflict via cooperation which only works to the adversary's detriment. As a result, the adversary will slowly begin to appear on the world stage as uncommitted to its role, inconsistent in its actions, and inept in its performance. This result will only make other tenets of the RASCLS framework more easily applicable.

ACT 6: LIKENESS

Distinctions divide two things from one another; Likeness blurs those distinctions and thus shortens the divide. Likeness is what draws us to other people who are fundamentally distinct from ourselves. Humans are drawn to other humans who have similar interests, appearances, hobbies, cultures, and philosophies of their own. It is natural, therefore, that as groups of humans develop into systems, and systems develop into states, Likeness continues playing out as a force of attraction at the strategic and political levels within international relations. Indeed, the Diplomatic Peace Theory within the field of international relations argues that democracies, alike in their political systems, do not wage war against each other due to their likenesses.[18]

The art of applying Likeness, as a strategy, entails pushing the narrative that two fundamentally distinct entities are not so different, by emphasizing whatever abstract likenesses they may share. Consider the

relationship between the United States and the Soviet Union. As distinct as the U.S. and the USSR were, and as adversarial the nature of their relationship was, there were some glaringly obvious likenesses between the two countries. First, both modernized themselves through a revolution by the intelligentsia classes against their respective domestic monarchies to bring about their respective visions of the ideal government. Second, both countries were allies in the Second World War. Third, both countries were technological pioneers. Fourth, neither nation truly wished to begin a nuclear war with the other. The overarching difference, however, was the ideal toward which each nation worked, and the importance of their respective ideals was a difference that seemed insurmountable.

Ho Chi Minh attempted to use Likeness as a strategy to win over U.S. support, going so far as to compare himself to George Washington.

Looking back in history, it may seem overly hopeful, or perhaps delusional, that to extend an olive branch in such a way could have any positive effect for the future. However, no one should forget the failure of accepting such an olive branch, which the OSS wished to do during its mission to Indochina near and after the end of the Second World War. There, OSS officers met with Viet Minh leader Ho Chi Minh, who deeply respected the United States. Ho Chi Minh attempted to use Likeness as a strategy to win over U.S. support, going so far as to compare himself to George Washington.[19] Ho Chi Minh even used the phrase "all men are created equal" and several other direct allusions to the United States' founding document in his own speech declaring the independence of the Democratic Republic of Vietnam.[20]

Ho Chi Minh's pleas fell on deaf ears. His correspondence with the United States was through the OSS, which saw itself as a group of covert military advisors more than it did diplomats. The United States refused to work with the communist leader, who was in open conflict with the French. The position of the United States was made perfectly clear to Ho Chi Minh when the U.S. sold France $160 million in military equipment to put down the Viet Minh resistance. Regardless, the French were beaten back at Dien Bien Phu, and Vietnam would soon become America's conflict as well. The importance of having persons trained in the RASCLS framework in more diplomatic roles was shown here.

Likeness does not only have to be applied with an individual leader or a small group of influential people, but also on a massive scale. By breaking borders via mediums that do not recognize international boundaries, such as radio waves, one can push the narrative of Likeness further than an adversarial government would want such a narrative to go. For example, one could use previously established white propaganda methods, such as Voice of America, to push a Likeness narrative in a foreign language by a foreign speaker to a target population. This operation may assist in cultivating public opinion abroad, ultimately bringing about the notion (the strategic goal) that the likenesses between the target population and the American population is stronger than asserted by the target government.

Naturally, as with any soft power policy or implementation of public diplomacy, the success of these operations will be extremely difficult to measure. In fact, it may be impossible ever to measure accurately the success of many of the tenets of the RASCLS framework as they are applied at the strategic level. However, that should not dissuade the United States from implementing them in its foreign policy. Eventually something will work.

ACT 7: SOCIAL PROOF

Social Proof is the art of creating a false narrative so that the target audience feels obligated to take action due to its misperceptions. At the individual level, a common example of this is "salting the tip jar." This is done when a business places its own money into the tip jar to make it appear as if tips are expected from the customer, and that other customers have tipped before them. This false narrative pressures the customer to tip so as not to break from the social norm, a social norm which does not actually exist. On a mass scale, narratives—both true and false—about what is socially normal are conveyed through various forms of media. Consider for a moment any family movie. Regardless of the plot, the reality of life in that country and in that culture are reflected as the true objective reality that a mass audience will accept and resonate with. Media that reflect social ideals will pressure the masses to pursue those ideals. Media that reflect social problems will pressure the masses to fix those problems.

As a strategy, Social Proof is quite straightforward. Social Proof will be successfully applied when a foreign audience believes that all aspects (social, governmental, etc.) of the American World Order surpass any other global order, and that the foreign audience feels pressured to adhere to the American World Order despite its government's disagreements. This is quite a clear strategy, but the strategy is difficult to apply as in past

decades due to a lack of the one thing needed to make this strategy work at the lower levels: mass communication. Indeed, it is easy for a government to ban films, books, art, and music to control the concept of social norms to which its citizenry holds fast. The embargo on such media and suppression of counter-culture was relatively easy to achieve when mass communication was not as commonplace. However, considering the technological revolution in the past two decades, Social Proof as a strategy can finally be acted upon.

In only the past few years social media platforms have transitioned from fun interactive websites to highly dangerous political weapons.

Recently, the perfect tactical and operational tool was invented that can assist the Social Proof strategy: social media. Indeed, in only the past few years social media platforms have transitioned from fun interactive websites to highly dangerous political weapons. In the modern world, two realities exist: the physical reality and the virtual reality, and anyone with a smartphone can live in either. The television, which used to serve as a black mirror most hours of the day, is now a 24-hour view of the entire world. With such mass media constantly present in modern society, it is no surprise that it has turned into an absolute battleground for Social Proof.

The weaponization of social media as a political instrument to disrupt social cohesion has already been demonstrated by Russia in the 2016 U.S. presidential election. In the election cycle, Russian bots directly retweeted President Trump 468,537 times. Twitter ultimately concluded that Russian propaganda had reached real users on 454.7 million occasions. Facebook concluded that approximately 126 million users received Russian propaganda.[21] This is a clear attempt by a foreign government to alter public opinion, and to construct a social narrative that a foreign population—the American population—would feel pressured to adhere to.

Additionally, as if an echo from the past, a spike in anti-Semitic language was seen during this time as well, with the perpetrators being bots rather than people.[22] The effect that this has is creating a narrative to convince real people that certain ideas are more acceptable than people originally believed. Such an alteration of reality—more specifically of virtual reality—can have steep consequences in the physical world. Even if people disagree with what is presented to them as socially normal, their false notion that their social ideal is shared by the minority keeps them from speaking out. People will draw their conclusions of reality based on the Social Proof that they believe is accurate, and then act accordingly. The Islamic State can be considered as an example in military terms: what it lacked in manpower, equipment, and territory it made up for in marketing via social media. The execution of James Foley, for example, practically changed American public opinion of war in the Middle East overnight.[23] Compared to the public's much less virulent reaction to Daniel Pearl's execution in 2002, the spectacle made of Foley's execution demonstrates the extreme effects that social media have on creating a narrative.

Social media is the tool that will allow for the art of Social Proof to be applied at a strategic level. A television, a smartphone, and a computer monitor are nothing but windows into the world. These windows are tinted, or tainted, with algorithms that relay content to massive audiences. With the application of artificial intelligence, this will become only easier, and more deadly. This particular tenet is of extreme importance, as without it the other tenets are doomed to fail. Any successful application of Reciprocation, Authority, Scarcity, Commitment and Consistency, or Likeness hinges on whether or not such tenets could be publicly proven, or at least seem to be. In an age of disinformation, disruption, and deceit, proof is of paramount importance. These screens are windows ready to be dressed, but first we must learn how to dress them.

CONCLUSION

In theater, an iron curtain is a device which is meant to protect the audience and the rest of the theater from a fire, should one start on stage. In the meantime, while the theater is safe, the actors in their costumes and masks dance about and entertain the audience. All the while, that which is happening behind stage, in the shadows and in the dressing rooms, is kept from sight. If a fire starts, the actors scatter, the iron curtain falls, and then even the stage itself is hidden from view. Such a phenomenon has been seen in the real world in recent times, when autocratic governments have constructed barriers to protect their theaters from a fire which could be spread by truth.

The story that is often told on the world stage, especially by authoritarians, can be undermined. Nevertheless, if the iron curtain exists as a failsafe, then we cannot simply go set fire to their theater to end the show. They will risk losing the audience, as members seek to leave the theater, and they will do everything they can to keep that from happening. The show must go on, but that is not to say

that the show cannot be stolen. This article has offered seven acts which can be performed in order to acquire the favor of the audience, and to undermine the regime: Reciprocation, Authority, Scarcity, Consistency, Commitment, Likeness, and Social Proof. If applied properly at the strategic level, on the international stage, the owners of the theater may not recognize what is being done until it is too late, and their audience is already against them.

In order to do this, however, we must understand the foreign audience in order to connect with it. We must understand the other actors in order to out-perform them. We must conduct ourselves subtly enough that all of our actions against both the foreign audience and actors seem completely genuine. If this is not accomplished, then the plays performed by authoritarians will continue, perhaps forever. The iron curtain was pulled back over 30 years ago. The window dressing still remains. That is not to say that it cannot be removed, or be made to work in our favor. It can be, and so it will be, with this new strategy for preserving peace and freedom in the world.

> *Look at this window: it is nothing but a hole in the wall, but because of it the whole room is full of light. So when the faculties are empty, the heart is full of light. Being full of light it becomes an influence by which others are secretly transformed.*
>
> *— Chung Tzu*[24]

NOTES

[1] NATO, *Funding NATO*, June 2018, https://www.nato.int/cps/ro/natohq/topics_67655.htm.
[2] Lawrence Freedman, *The Evolution of Nuclear Strategy*, 3rd ed. (New York: Palgrave Macmillan, 2003), 234-236.
[3] BBC, "D-Day anniversary: Putin says lack of invitation 'not a problem'," *BBC*, June 6, 2019, https://www.bbc.com/news/world-europe-48548200.
[4] Sam LaGrone, "Russian Destroyer Puts U.S. Cruiser at Risk with 'Unsafe' Maneuver," *USNI News*, June 7, 2019, https://news.usni.org/2019/06/07/navy-russian-destroyer-put-u-s-cruiser-at-risk-with-unsafe-maneuver.
[5] Èçâåñòèÿ, "Ïîÿâèëîñü âèäåî îïàñíîãî ñáëèæåíèÿ êðåéñåðà ÑØÀ è êîðàáëÿ ÂÌÔ ÐÔ" *Èçâåñòèÿ*. 7 èþíÿ, 2019, https://iz.ru/886738/2019-06-07/poiavilos-video-opasnogo-sblizheniia-kreisera-ssha-i-korablia-vmf-rf.
[6] Max Weber, *Basic Concepts in Sociology*, trans. H.P. Secher (New York: Greenwood Press, 1969), 81-83.
[7] Vladimir Bukovsky, *Judgement in Moscow: Soviet Crimes and Western Complicity*, trans. Alyona Kojevnikov (California: Ninth of November Press, 2019), 28.
[8] Bukovsky, *Judgement in Moscow,* 27.
[9] J. Eli Margolis, "Estimating State Instability," *Studies in Intelligence* 56, no. 1 (March 2012): 16-18, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-56-no.-1/pdfs-vol-56.-no.-1/Studies%2056-1%20Extracts-25April.pdf#page=21n.
[10] Office of Strategic Services, *Simple Sabotage Field Manual: Strategic Services Field Manual 3*, Washington, DC, 1944, https://www.cia.gov/news-information/featured-story-archive/2012-featured-story-archive/CleanedUOSSSimpleSabotage_sm.pdf
[11] Kenneth Rapoza, "Russia's Latest Sanctions a Year in the Making but Surprise Everyone," *Forbes*, August 2, 2019, https://www.forbes.com/sites/kenrapoza/2019/08/02/russias-latest-sanctions-a-year-in-the-making-but-surprises-everyone/#244380ce5de3.
[12] Amos Tversky and Daniel Kahneman, "Advances in Prospect Theory: Cumulative Representation of Uncertainty," *Journal of Risk and Uncertainty* 5 (Kluwer Academic Publishers, 1992): 297-323.
[13] Bukovsky, *Judgement in Moscow,* 296-297.
[14] Bukovsky, *Judgement in Moscow,* 331.
[15] Lawrence Freedman, *The Evolution of Nuclear Strategy,* 3rd ed. (New York: Palgrave Macmillan, 2003), 176.
[16] William Taubman, *Khrushchev: The Man and His Era* (New York: W.W. Norton & Company, 2003), 579.
[17] Freedman, *The Evolution of Nuclear Strategy*, 175-176.
[18] Karen A. Mingst and Ivan M. Arrenguin-Toft, *Essentials of International Relations,* 7th ed. (New York: W.W. Norton & Company, 2017), 161.
[19] Richard Harris Smith, *OSS: The Secret History of America's First Central Intelligence Agency* (Guilford, UK: Lyon Press, 2005), 308.
[20] Ho Chi Minh, *Selected Works*, Vol. 3 (Hanoi: Foreign Languages Publishing House, 1960-62), 17-21, http://historymatters.gmu.edu/d/5139/.
[21] P.W. Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media* (New York: Houghton Mifflin Harcourt Publishing Company, 2018), 144.
[22] Singer and Brooking, *LikeWar,* 146-147.
[23] Singer and Brooking, *LikeWar,* 151-152.
[24] Juliana Pilon, *The Art of Peace: Engaging a Complex World* (Piscataway, NJ: Transaction Publishers, 2016), 355-

Mason D. Goad graduated summa cum laude from the University of North Georgia, where he earned a BA degree in the Strategic and Security Studies program, in 2020. He will join the MA program in International Security at George Mason University in the fall. He has conducted additional research on quantum computing and national security, which culminated in his thesis titled "A Quantum of Solace" being published in summer 2020. He is interested in how rapid technological change continues to shift national security paradigms, and wrote the paper "Window Dressing," published here, during his time as a Presidential Fellow at the Center for the Study of the Presidency and Congress. Mason currently is working as a communications assistant at GMU's Schar School for Policy and Government and is also serving as a Russian language tutor.

The Historical Evolution of Israeli Intelligence

by Admir Barucija

THE HISTORICAL CONTEXT

Given the globalized nature of today's world, maintaining a robust intelligence system is an imperative for countries like Israel, which faces a host of threats at home and abroad. Although it proved unsuccessful, the ancient Israelites conducted one of the earliest Biblical intelligence operations. Israeli intelligence today largely operates through the agencies Mossad (foreign intelligence), Aman (military intelligence), and Shin Bet, which is focused on domestic intelligence, though Israeli police does have its own intelligence branches and processes as well. Israeli intelligence agencies are given significant leeway in terms of oversight and accountability, though they have often been under scrutiny for some of their operations, especially ones conducted in other countries. The Israeli government deeply values intelligence for the purpose of safeguarding national security, though that does not preclude Israeli agencies from spying on their own people. While Israel's intelligence agencies and methodologies have evolved over time and become much stronger, the country's geographic location in the heavily volatile Middle East has made possessing a robust intelligence community a necessity.

In *The Bible*, the ancient Israelites demonstrated a rudimentary intelligence process when they ventured into Canaan, which was a task given to them by Moses. He sent 12 men, one from each tribe, into Canaan to look at the land, the Canaanites' dwellings, and their agricultural harvest, with grapes specifically requested.[1] The activity of 12 spies heading into Canaan is a very basic example of human intelligence, though it gave a semblance of a model for how intelligence could be conducted. Once the spies had completed exploring Canaan after 40 days, only Caleb and Joshua gave a positive and honest assessment of what they had found, though the other ten gave an "evil" description.[2] The ten spies who gave a false report stated that Canaan was a land that eats up its inhabitants and the people in it are giants.[3]

Despite the fact that cognitive biases largely derailed what would have been a successful intelligence operation, the ancient Israelites set the stage for what would essentially be an intelligence process because they had a customer, a requirement, and a collection method, as well as a product. The Israelites' intelligence work in Canaan is not the first instance of Biblical spying, but it demonstrates that Israel can claim a very rich history of intelligence.

The Israelites' intelligence work in Canaan is not the first instance of Biblical spying, but it demonstrates that Israel can claim a very rich history of intelligence.

Before Israel officially declared its independence in 1948, Arabic-speaking Jews were performing their own intelligence operations. The Political Department of the Jewish Agency for Palestine, a legal body that the British authorities recognized, and the Haganah, which was illegal, conducted intelligence for the Israeli people.[4] Under the noses of the British rulers of Palestine, the Jews conducted intelligence, which largely contributed to Zionist efforts to bring about a Jewish state, efforts that were ramped up after the Holocaust of World War II. The Political Department contained an Arab Section, which was tasked with handling a network of Palestinian informants and clandestinely contacting Arab leaders in Palestine and throughout the Middle East.[5] In the face of readily apparent danger, Arab-speaking Jews routinely conducted intelligence to learn more about what was really going in the Arab world. Within the Political Department there was also an intelligence service, called the Shai, which fell under the control of the Haganah and the Jewish Agency. The Shai had three sections—Arab, British, and Internal.[6] Interestingly, the Internal Section had the mandate of spying on certain groups of Jews, such as those who were communists or leaned politically to the far right. The intelligence organizations and processes of the Jews under British rule led to the later creation of the Israeli Defence Forces (IDF), the Mossad, and the Shin Bet (Shabak).

Soon after Israel became independent, the government recognized the need to establish a durable intelligence structure, especially militarily. In June 1948, after consulting with Reuven Shiloah and Chaim Herzog, Prime Minister David Ben-Gurion decided to create three intelligence organizations, which ended up being Aman, Shin Bet, and eventually Mossad as well.[7] Ben-Gurion knew early on that Israel would be met with serious hostility, and made the logical decision to bolster the country's security and intelligence capabilities significantly. Aman's mandate was to collect intelligence on Arab states' militaries and protect Israeli internal security. Shin Bet was tasked with domestic intelligence and counterespionage,[8] while Mossad was the central authority for collecting foreign intelligence, including covert relations with other states and special operations.[9] As is true also with the Central Intelligence Agency (CIA) in the U.S., Mossad has generated a lot of controversy for its operations abroad, such as those pursuing former Nazi officials (e.g., Adolf Eichmann). Another intelligence liaison bureau in Israel was Nativ, which then-Prime Minister Moshe Sharett founded in late 1952. It was given the responsibility for making contact with Jews living in the Cold War-era Eastern Bloc of Europe as well as getting them to relocate to Israel.[10] Nativ experienced great success during the Cold War, with its agents clandestinely giving Jews living in the Soviet Union religious articles and Hebrew dictionaries, and eventually shifting to operating out of Israeli embassies. Although significantly reduced and no longer being able to carry out its original purpose, Nativ continues to operate.

Another Israeli intelligence organization that operated for much of the Cold War was Lekem, which was essentially the bureau of scientific relations. Until it ceased to exist in 1986, Lekem was responsible for collecting scientific and technical intelligence abroad through both open and covert methods.[11] Essentially, Israel was using Lekem to evaluate how its adversaries' capabilities measured up, though it likely also collected intelligence on allies as well. After a scandal arose in the U.S. when Jonathan Jay Pollard was arrested for espionage on Israel's behalf, which supposedly involved giving Lekem agents a plethora of classified documents, Lekem was officially disbanded.[12] Historically, the U.S. and Israel have been strong allies, though that did not appear to stop the Israelis from collecting intelligence within the U.S. The Israeli government, in response to the Pollard operation, claimed what Lekem did was unauthorized and that the official policy is not to conduct espionage against the U.S., though Pollard's and the Israeli participants' statements contradicted Israel's assertions.[13] It is unclear what benefits the Israelis gained from the documents Pollard gave them, but it is clear they valued building up their own technological capabilities to maintain security. While Lekem is no longer functional, Israel is highly likely still to have some dedicated personnel for the collection of scientific and technical intelligence.

After a scandal arose in the U.S. when Jonathan Jay Pollard was arrested for espionage on Israel's behalf, which supposedly involved giving Lekem agents a plethora of classified documents, Lekem was officially disbanded.

The historical U.S.-Israeli alliance also translates to cooperation in intelligence, which has been helpful for Israeli intelligence organizations, especially Mossad. In Israel, only Mossad is responsible for cooperating with foreign intelligence agencies, and it does so with the CIA through an ad hoc unit.[14] The CIA and Mossad both were founded in close succession, and their relationship has helped Israel maintain its national security despite fragile relations with states of the Middle East. The relationship between U.S. and Israeli intelligence stretches back to the early Cold War, in which U.S. intelligence agencies were in fierce contention with those of the Soviets.[15] Israel, having only just become a nation of its own, would be highly unlikely to account for its security without the help of the U.S., the preeminent global superpower following World War II. Strikingly, the CIA decided to work with Mossad despite initially believing that Israel should not be part of the West's Cold War coalition.[16] Although Israel has been involved in several wars since independence, its intelligence services have consistently proved to be strong and capable. The U.S. and Israel worked together in terms of intelligence, despite having two highly contrasting sets of priorities.

Perhaps Israel's greatest intelligence failure was its inability to anticipate the surprise attack that initiated the Yom Kippur War in 1973. One of the biggest factors was that Aman, the military intelligence directorate, held a monopoly on Israel's intelligence estimates, which is why Mossad's warnings went unheeded.[17] Although Israel subsequently restructured its intelligence system, the inability of different agencies to coordinate successfully could have proven much more devastating than ultimately was the case. Major General Eli Zeira, Aman's director in 1973, was confident in his assessment that the Arabs would not strike at that time, which affected the IDF's preparedness and ability to respond.[18] Zeira thought he knew more than his superiors about the threat Israel faced militarily, which initially proved disastrous, even though Israel eventually ended up winning the conflict. Another factor that played into the eventual Arab surprise attack was Egypt's strategic deception, which was meant to lull Israel into a sense of complacency.[19] While Egypt's deception did not pan out entirely, it did contribute to a delay in Israel preparing for the possible outbreak of war.

Although Israel did win the Yom Kippur War, with support from the United States, Israeli intelligence certainly learned a lesson from underestimating the scope of the threats the nation faced.

Throughout its history, Mossad has captured, and sometimes assassinated, individuals abroad deemed dangerous to the state of Israel. One of the most famous operations Mossad has conducted was the capture in Argentina by about a dozen Mossad agents of Adolf Eichmann, who was then taken to Israel.[20] Eichmann was subsequently put on trial in Israel and hung rather than facing justice through international tribunals, such as occurred in the Nuremberg trials. In September 1972, Palestine Liberation Organization (PLO) operatives murdered 11 Israeli Olympic athletes in Munich, Germany, which resulted in a wave of assassinations across Europe undertaken by Mossad.[21] Israeli intelligence officials, in essence, contributed to protecting Jews wherever they were located around the world, and were willing to do the dirty work to accomplish that mission. One of the participants in Mossad's raids against PLO officials was Ehud Barak, who later became prime minister, and some of the revenge missions spanned two decades.[22] Most countries would not allow their intelligence officials to run rampant abroad, but Mossad's actions stem heavily from Israel being situated in a hostile environment. Mossad is no stranger to criticism and scandalous behavior because of its methods, but has largely managed to fulfill its responsibilities to the state of Israel.

THE CONTEMPORARY CONTEXT

While Israel's intelligence community has undergone structural reforms and adjustments, Aman, Shin Bet, and Mossad are still today the main organizations. The Israeli Security Agency (ISA), a state-run organization designed to protect national security, had proper oversight of Shin Bet for the first time after passage of a 2002 ISA statute regarding the ISA.[23] This statute was intended to hold Shin Bet accountable for its actions and maintain adherence to the constitution of Israel, though it took over five decades for such changes to occur. On the other hand, Mossad's operations seem to require only the approval of the prime minister, which skirts around any laws that limit its authority or establish a means of oversight other than the personnel within Mossad who voice their concerns.[24] The government of Israel confers plenty of trust to Mossad, though it is a dangerous precedent because the only check on Mossad's actions is the whim of the prime minister currently in power. In response to the Arab Spring and technological changes, Aman has undergone organizational reforms as well, with a new commander being appointed for the special operations layout and the formation of a new technological unit responsible for all intelligence elements (e.g. SIGINT, HUMINT) being the main changes.[25] Aman's reforms are intended to improve communications across all levels of military intelligence, which will be supplemented with a standard network infrastructure. Just as intelligence had been integral to the formation of Israel as a state, it remains so today to maintain the security of the Israeli people.

The Israeli public, though reflecting division in terms of religion, appears to favor intelligence and defense organizations, which in their eyes make up for the shortcomings of the government.

Although public opinion is fairly divided, the people appear largely to favor Israel's intelligence and defense organizations. According to the annual Israel Democracy Index released in 2015, just over one-third of Israelis trust the parliament, known as the Knesset, but Jewish-Israelis reported that they heavily trust President Reuven Rivlin and the IDF.[26] The Israeli public, though reflecting division in terms of religion, appears to favor intelligence and defense organizations, which in their eyes make up for the shortcomings of the government. Nearly three-quarters of Israelis, roughly 74 percent, described their personal situation as being "good" or "very good," despite a severe erosion of faith in the political establishment.[27] The Middle East remains marred with instability and constant pressures, but the fact that most Israelis report feeling secure is a testament to the ability of their nation's intelligence organizations. Additionally, almost three-quarters, or 73.6 percent, of Jewish-Israelis responded that national security decisions should be made only if there is a Jewish majority.[28] While nationalist sentiments linger throughout the Israeli public, the people have largely been willing to support the national security establishment as long as it keeps the state intact. Whether real or perceived, Israelis attribute the maintenance of their personhood and security to the IDF and the intelligence agencies.

Another element of the reputation of Israeli intelligence, which ties into public perceptions, is the role of the media in assessing national security decisions and actions. Unlike the rest of Israel's intelligence establishment, Mossad does not have a formal spokesperson, which is largely due to its assessment that revealing critical information to the public would cause reputational damage.[29] Although the element of secrecy is a pivotal factor to consider for intelligence organizations speaking to the media, the ISA has managed to adapt and Mossad doing the same would likely make it more favorable to the Israeli people. Since the mid-1990s, the ISA has issued formal press releases, as well as holding

semi-formal briefings and press conferences.[30] The ISA is putting in the effort to cultivate a relationship with the media and be more transparent, which very well may contribute to the Israeli public conferring approval on state defense forces and the intelligence institutions. However, it is worth mentioning that internal services such as the ISA are often involved in contested political debate, which is atypical for Shin Bet and Mossad.[31] Due to the nature of being politically active, there is bound to be plenty of media exposure for the ISA, but Mossad especially is known to operate largely on its own, not answering to the public or most officials in government for that matter. The common stereotype of intelligence agencies being shrouded in secrecy holds true for Israel's agencies as well, though this has not stopped them from receiving public approval.

The government of Israel readily embraces its intelligence organizations, though it may also be too involved in their affairs at times. The government is involved in some instances with targeted killings, decisions that require input from intelligence officials, the Israeli Ministry of Defense, and ultimately the prime minister's approval.[32] Although Israel uses targeted killings as a measure of last resort, the ability of the prime minister to approve the murder of any target abroad deemed too dangerous is problematic. The Israeli government, in response to the persistent threat of a hostile and rapidly changing environment, tends to make national security decisions reactively, which results in ad hoc solutions to immediately pressing issues.[33] As a result, Israel's government often makes key national security decisions on the fly, which ends up placing incredible strain and pressure on its intelligence community because it must rapidly respond to crises. Just recently, Israel's government, due to the insistence of Prime Minister Benjamin Netanyahu, approved measures that allow Shin Bet to capitalize on its advanced cyber capabilities with cell phone data to track suspected carriers of coronavirus and to monitor those who are supposed to be in quarantine.[34] While the political opposition and civil society groups have opposed the move to track people using cellphone records, citing privacy concerns, Netanyahu maintains that the government is merely attempting to slow the spread of the virus.

Israel's military intelligence organization, known as Aman, regularly assesses the strategic implications of the country's security environment, especially in regard to the Middle East. The Arab Spring alerted Aman to new and old security threats, which include Hezbollah, Egyptian regime changes in 2011 and 2013, maintaining the 1979 peace agreement with Egypt, and the Israeli-Palestinian conflict.[35] Although any country's military intelligence organization has a tough task to begin with, Aman is responsible for maintaining Israeli national security in one of the world's most unstable regions. In September 2014, as part of a structural reorganization, Unit 3060 was formed with around 400 soldiers that specialize in technology, which is meant to develop apps that will allow the IDF, in real time, to follow enemy positions and determine exit routes from enemy territory.[36] Israel depends on its intelligence capabilities as a safeguard against terrorism, and staying ahead technologically will undoubtedly benefit security forces. Israel's security forces include the Musta'ribeen, undercover agents that are dressed like Arabs or Palestinians. They undergo advanced training, and are taught how to think and act like Arab persons normally would, which may also include language lessons.[37] Not much is known about the Musta'ribeen, but they are routinely present at Palestinian protests and often cause violence or serious chaos. Israel's military intelligence is formidable and serves as a critical piece of its national defense, though Aman's actions are not always morally defensible.

One area of concern, however, for Israeli military intelligence is that it often gets involved in controversial political issues, which do not fall into its domain of responsibility. Aman's research division, within the previous decade, started performing investigations into foreign left-wing organizations and those that engage in anti-Israeli activities in the West, which resulted in criticism by the Israeli Ministry of Foreign Affairs and the press.[38] While anti-Israeli sentiments abroad may promote hostility or violence against Jews, allowing Aman to investigate issues of a political nature creates a very slippery slope. For Aman, intelligence regarding the Palestinians has been the area most likely to suffer from "political distortion," though it has also come up in diplomatic negotiations in which the IDF wants to play a prominent role.[39] The goal of a proper intelligence organization is to maintain objectivity and bring truth to light, but Aman has allowed ideology and nationalist sentiments to invade its intelligence assessments regarding Israel's security. Another example of issues with Aman are repeated breakdowns in the relationship between intelligence officials and the Israeli Cabinet, especially in relation to Lebanon, a problem that first started decades ago.[40] Quality intelligence is meant to support decision-makers and reduce their uncertainty, not to determine their course of action. Israeli military intelligence officials have, on multiple occasions, sought to steer national security policy, which is a clear overstep of their authority.

Despite Israel being a relatively small country in terms of area and population, its intelligence structure is among the world's most capable, and it is key to the country's survival. Since Biblical times, though primitive by today's standards, the ancient Israelites set the tone for what would become a process of intelligence collection. Even before Israel became independent, while it was under British rule Arab-speaking Jews were gathering intelligence throughout the Arab world, and other bureaus kept tabs on the Jewish population to

prevent dissidents from derailing the establishment of a Jewish state. Aman, Shin Bet, and Mossad remain as crucial today for Israeli national security as they were in the late 1940s, and all three organizations operate with considerable power, which is seen as necessary given the environment in which Israel resides. Although oversight of Israeli intelligence is severely lacking and the prime minister has considerable leverage when it comes to national security decisions, Israel would be in a considerably worse position without a high-quality intelligence community.

NOTES

[1] *The Bible*, King James Version, Numbers 13:1-33.
[2] Ibid.
[3] Ibid.
[4] Ian Black, "The origins of Israeli intelligence," *Intelligence and National Security* 2, no. 4 (1987): 151-156, https://doi.org/10.1080/02684528708431920.
[5] Ibid.
[6] Ibid.
[7] Ami Pedahzur, *The Israeli Secret Services & the Struggle Against Terrorism* (New York: Columbia University Press, 2009).
[8] Ibid.
[9] Mossad, "About Us: Background," https://www.mossad.gov.il/eng/about/Pages/default.aspx, accessed April 10, 2020.
[10] Yossi Melman, "Fight Over Next Nativ Head Turns Ugly," *Haaretz*, September 11, 2005, https://www.haaretz.com/1.4940837.
[11] Federation of American Scientists, "Lekem: Bureau of Scientific Relations," https://fas.org/irp/world/israel/lekem/index.html, accessed April 10, 2020.
[12] Ibid.
[13] Ibid.
[14] Ephraim Kahana, "Mossad-CIA Cooperation," *International Journal of Intelligence and CounterIntelligence* 14, no. 3 (2001): 409-420, https://doi.org/10.1080/08850600152386873.
[15] Ibid.
[16] Ibid.
[17] Uri Bar-Joseph and Jack S. Levy, "Conscious Action and Intelligence Failure," *Political Science Quarterly* 124, no. 3 (2009): 461-488, https://www.jstor.org/stable/25655697?seq=1#metadata_info_tab_contents, accessed April 10, 2020.
[18] Ibid.
[19] Ibid.
[20] Yonah Jeremy Bob, "The Mossad's greatest hits: From Eichmann to al-Batsh," *The Jerusalem Post*, April 26, 2018, https://www.jpost.com/israel-news/the-mossads-greatest-hits-from-eichmann-to-al-batsh-552714.
[21] Ibid.
[22] Ibid.
[23] Shabak, "About," https://www.shabak.gov.il/english/about/Pages/about.aspx, accessed April 10, 2020.
[24] Ze'ev Segal, "A Legal Framework for the Mossad," *Haaretz*, March 1, 2010, https://www.haaretz.com/1.5034915.
[25] Amir Rapaport, "Revolution in the Intelligence Agencies," *Israel Defense*, April 19, 2014, https://www.israeldefense.co.il/en/content/revolution-intelligence-agencies.
[26] "Survey: Israelis distrust government, Jewish-Israelis distrust Arabs," *Jewish Telegraphic Agency*, November 10, 2015, https://www.jta.org/2015/11/10/israel/survey-israelis-distrust-government-jewish-israelis-distrust-arabs.
[27] Ibid.
[28] Ibid.
[29] Clila Magen, "Israel's intelligence services and the media: Four decades of a complex tango," *Israel Affairs* 24, no. 5 (2018): 799-818, https://doi.org/10.1080/13537121.2018.1505702.
[30] Ibid.
[31] Ibid.
[32] Avi Dicter and Daniel L. Byman, "Israel's Lessons for Fighting Terrorists and Their Implications for the United States," *The Brookings Institution*, March 2006, https://www.brookings.edu/wpcontent/uploads/2016/06/byman20060324.pdf.
[33] Charles D. Freilich, "National Security Decision-Making in Israel: Processes, Pathologies, and Strengths," *Middle East Journal* 60, no. 4 (2006): 635-663, https://www.jstor.org/stable/4330316?seq=9#metadata_info_tab_contents.
[34] Steve Hendrix and Ruth Eglash, "Israel is using cellphone surveillance to warn citizens: You may already be infected," *The Washington Post*, March 19, 2020, https://www.washingtonpost.com/world/middle_east/israel-is-using-cellphone-surveillance-to-warn-citizens-you-may-already-be-infected/2020/03/19/68267294-69e7-11ea-b199-3a9799c54512_story.html.
[35] Eran Zohar, "Israeli military intelligence's understanding of the security environment in light of the Arab Awakening," *Defence Studies* 15, no. 3 (2015): 203-234, http://dx.doi.org/10.1080/14702436.2015.1065612.
[36] Anna Ahronheim, "Inside the cutting-edge Israeli army intelligence unit that's 'like a start-up company'," *Business Insider*, January 3, 2018, https://www.businessinsider.com/idf-cutting-edge-israeli-army-intelligence-unit-2018-1.
[37] Linah Alsaafin, "Musta'ribeen, Israel's agents who pose as Palestinians," *Al Jazeera*, April 10, 2018, https://www.aljazeera.com/news/2017/12/musta-israel-agents-pose-palestinians-171218061118857.html.
[38] Eyal Pascovich, "Military Intelligence and Controversial Political Issues: The Unique Case of the Israeli Military Intelligence," *Intelligence and National Security* 29, no. 2 (2014): 227-261, http://dx.doi.org/10.1080/02684527.2012.748370.
[39] Ibid.
[40] Ibid.

Admir Barucija is a senior at Mercyhurst University majoring in Intelligence Studies and Political Science, with a concentration in International Relations. Originally from Sarajevo in Bosnia and Herzegovina, he plans on attending the University of Pittsburgh's Graduate School of Public and International Affairs beginning in the fall of 2021. He has been involved in multiple business intelligence projects and has worked as an intelligence analyst for a private firm for over a year. In the summer of 2020, he was scheduled to work on an intelligence project for the U.S. State Department as part of a team of student analysts.

Understanding the Gray Zone:
How Federal Law Enforcement Agencies Can Support SOF Operations Related to Counterterrorism Strategy

by Carvent L. Webb II

OVERVIEW

The strategic environment is changing rapidly, and the United States faces an increasingly complex and uncertain world in which threats are becoming ever more diverse and interconnected. While the Intelligence Community (IC) remains focused on confronting a number of conventional challenges to U.S. national security posed by our adversaries, advances in technology are driving evolutionary and revolutionary change across multiple fronts. The IC must become more agile, innovative, and resilient to deal effectively with these threats and the ever more volatile world that shapes them. The increasingly complex, interconnected, and transnational nature of these threats also underscores the importance of continuing and advancing IC outreach and cooperation with international partners and allies.[1]

INTRODUCTION

Perhaps the most widely used definition of Gray Zone (GZ) conflict is that established by the U.S. Special Operations Command (SOCOM): "Gray zone challenges are defined as competitive interaction among and within state and non-state actors that fall between the traditional war and peace duality. They are characterized by ambiguity about the nature of the conflict, opacity of the parties involved, or uncertainty about the relevant policy and legal frameworks." The central characteristic of GZ operations is that they involve the use of instruments beyond normal international interactions, yet short of overt military force. They occupy a space between normal diplomacy and commercial competition and open military conflict, and while often employing diplomacy and commercial actions, GZ attacks go beyond the forms of political and social action and military operations with which liberal democracies are familiar, to make deliberate use of instruments of violence, terrorism, and dissembling.

While "Gray Zone" refers to a space in the peace-conflict continuum, the methods for engaging our adversaries in that environment have much in common with the political warfare that was predominant during the Cold War years. Political warfare is played out in that space between diplomacy and open warfare, where traditional statecraft is inadequate or ineffective and large-scale conventional military options are not suitable or are deemed inappropriate for a variety of reasons. Political warfare is a population-centric engagement that seeks to influence, to persuade, even to co-opt. In 2015 General (USA) Joseph L. Votel, who was then the Commander, U.S. Special Operations Command, spoke at a security forum in Colorado. He stated: "The 'hyper connectivity' of the world today complicates an already complex set of global security issues."[2]
Accordingly, this article acknowledges and briefly discusses the larger construct of gray zone challenges across the world, but it focuses on U.S. national security interests, challenges, and solutions for Special Operation Forces (SOF) to effectively continue to operate in the Gray Zone.

UNDERSTANDING CHALLENGES IN THE GRAY ZONE

Gray zone challenges are understood as a pooling of diverse conflicts exhibiting common characteristics. Combining these challenges does not imply a single solution, since each situation contains unique actors and aspects. Overall, gray zone challenges rise above normal, everyday peacetime geopolitical competition and are aggressive, perspective-dependent, and ambiguous. As the world's leading superpower and de facto guarantor of the current world order, American national security interests span the globe and intersect with numerous circumstances fitting the definition of gray zone challenges. However, many of these challenges exist independent of U.S. agency or action and do not merit American involvement (e.g., civil conflicts in Africa).

Additionally, America's status as the global leader guarantees it will face multiple, constant gray zone challenges. U.S. national security interests are worldwide, and there is a set of rogue state and non-state actors defining themselves, at least in part, by standing in opposition to America and its values. The United States can

selectively avoid some, but not all, gray zone challenges. For example, the scale of al-Qaeda's 9/11 attack demanded a robust U.S. response, while other lesser known terrorist groups' actions have not risen to the level where they are a significant concern for the U.S. national security apparatus.

UNDERSTANDING UNCONVENTIONAL WARFARE

Unconventional warfare (UW) is fundamentally an indirect application of U.S. power, one that leverages foreign population groups to maintain or advance U.S. interests. It is a highly discretionary form of warfare that is most often conducted clandestinely, and because it is also typically conducted covertly, at least initially, it nearly always has a strong interagency element. It can be subtle or it can be aggressive. The U.S. indigenous irregular benefactor-proxy relationship, if successful, achieves mutually beneficial objectives (although there can also be divergent interests between benefactor and proxy).

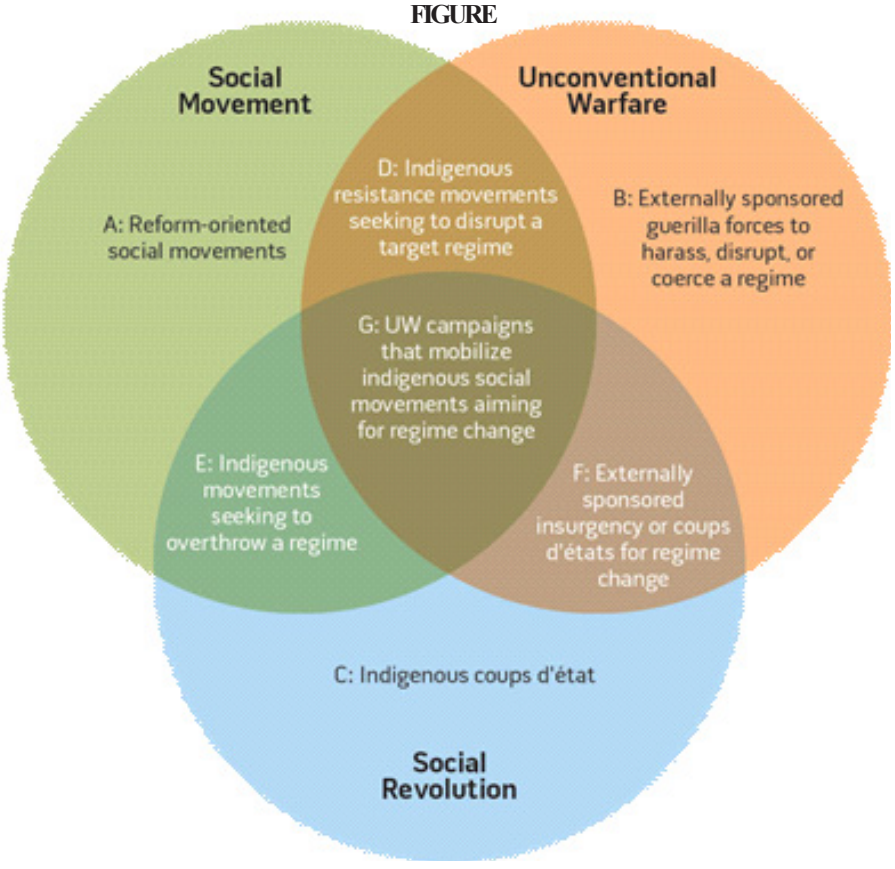
Recently, there has been growing interest in UW operations that leverage existing social movements and nonviolent, civil resistance-based social revolution. Contributing to this interest is the favorable track record of such movements in comparison with armed resistance. Based on one recent study of 323 resistance movements whose objective was regime change or expulsion of a foreign occupation force between 1900 and 2006, those movements that followed a strategy of "nonviolent resistance against authoritarian regimes were twice as likely to succeed as violent movements."[3]

The figure below(created by the Naval Postgraduate School's Doowan Lee) illustrates the relationship among social movements, social revolution, and unconventional warfare. An example of the scenario depicted by Sector G at the center of the diagram can be seen in U.S. support provided to resistance elements during Serbia's "Bulldozer Revolution" that resulted in the overthrow of dictator Slobodan Milosevic, then president of what remained of Yugoslavia.

USE OF SPECIAL OPERATION FORCES

Special Operations can be conducted directly against an adversary by forces acting in a single engagement, such as a raid against a critical communications node, or indirectly, for example, by organizing, training, and supporting an indigenous force for foreign internal defense (FID) or unconventional warfare (UW). They can also be conducted through the use of psychological operations (PSYOP) to influence the opposing

FIGURE



military or the local civilian populace. In either case, the results are normally disproportionate to the size of the units involved. Special operations missions may include more than one core activity. The special operations core activities are:

- Direct action
- Special reconnaissance
- Countering weapons of mass destruction
- Counterterrorism
- Unconventional warfare (UW)
- Foreign internal defense
- Security force assistance
- Hostage rescue and recovery
- Counterinsurgency
- Foreign humanitarian assistance
- Military information support operations; and
- Civil affairs operations[4]

LIMITATIONS WITHIN SPECIAL OPERATION FORCES IN THE GRAY ZONE

All special operations forces (SOF) share some common limitations, the first being that special operations (and by extension SOF) almost never achieve decisive strategic success on their own. Special operations and SOF alone can often achieve only decisive tactical success. Occasionally, special operations can have some strategic effect on their own, particularly in terms of signaling commitment and capability through discrete operations. However, absent other supporting elements—whether military, diplomatic, or economic—the achievement of decisive strategic effects by SOF is very rare.

According to the Department of Defense joint publication, *Special Operations*, there are four major limitations to take into consideration:

- Special operations are generally limited in scope by the size of the SOF unit.
- Improper employment of SOF runs the risk of rapidly depleting capacity. SOF cannot be quickly reconstituted or rapidly expanded because of the lengthy process required to recruit, train, and educate them.
- SOF are not a substitute for conventional forces (CF). In order to preserve SOF capabilities, SOF should not be employed to conduct operations where CF could be used to achieve the same objectives.
- Most special operations missions require CF logistics support. SOF are not structured with robust sustainment capabilities, therefore, SOF must frequently rely on external support for sustained operations. Limited SOF logistic capacity frequently requires support from CF supplemented by host-nation support (HNS) and/or operational contract support.[5]

CONTINUED LIMITED NUMBER OF SOF

U.S. SOF have more than doubled from around 33,000 personnel in 2001 to about 70,000 personnel as of early 2018. USSOCOM's Fiscal Year (FY) 2019 budget request called for growing the force to 71,000 personnel. USSOCOM currently sustains an average deployed force of about 8,300 personnel across 90 countries. In one country alone—Afghanistan—joint U.S. SOF conducted 2,175 ground operations where they advised and assisted Afghan commandos from June 1 to November 24, 2017—an almost six-month period. In 2017 the Department of Defense (DoD) reportedly moved more than 15 percent of its deployed SOF to assist African militaries, up from 1 percent in 2006, for a total of about 1,200 deployed to a dozen or so African countries. It has been suggested that over the past 16 years, U.S. SOF have become "the new American way of war." Some suggest that U.S. SOF have become an "easy button" for consecutive presidential administrations to push—a politically attractive alternative to sending thousands of conventional military personnel into complex and dangerous regions of the world.[6] The command is stationed and deployed in more than 70 countries.[7] As the "gray zone continues to expand in the realm of unconventional warfare the limited number of recruited, trained, and deployed SOF personnel will continue to restrict the areas in which SOF personnel will deploy. In May 2017 in a testimony to Congress USSOCOM Commanders told Congress":

> The rate of deployments was "unsustainable"[8] with one retired USSOCOM general officer reportedly noting, "We are not frayed at the edges—we're ripped at the damn seams. We've burned through this force."[9] Drug and alcohol abuse, family problems, and suicides among USSOCOM personnel and family members, as well as increased incidences of battlefield mistakes, have reportedly been attributed to USSOCOM's high operational tempo and its detrimental effect on readiness.[10] While USSOCOM efforts under its Preservation of the Force & Family (POTFF) and Warrior Care initiatives have helped to address these issues, high operational tempo continues to be a key catalyst affecting the health of the force and readiness.

HIGH-RISK DEPLOYMENT ZONES

Another limitation of SOF is the inherent high-risk nature of special operations. While this risk can be managed, it cannot be eliminated. This risk is of only moderate importance when policymakers are heavily committed to achieving an outcome such as victory in a major war. Yet policymakers often turn to SOF when seeking a limited liability military option—one just short of major war or intervention. In such situations, policymaker commitment to the objective may be sufficient to deploy SOF, but insufficient to sustain that deployment after a negative event occurs as a result of required risk taking.

This environment produces a paradox which limits SOF. If SOF are to continue being deployed in this environment, policymakers must either eschew necessary risk taking or assume reasonable risk, knowing a sufficiently negative incident could end the deployment. The former choice means operations will be sub-optimally effective, while the latter choice means a single negative event could end an entire SOF campaign (often with severe consequences for SOF careers).

INCREASED INDIRECT ACTION APPROACH

While SOF have general limitations related to congressional oversight, budgeting, and limited personnel, another limitation when measuring efficiency of SOF is the increased use of SOF in direct approach (direct action and special reconnaissance). Policymakers have high confidence that, when directed, U.S. SOF will execute missions as briefed. While confidence is welcomed by USSOCOM, it causes an undue burden on SOF personnel by creating the assumption that SOF are a "one-stop shop" for global issues.

INDIRECT APPROACH CONCERNS

In his book *Friends Like These: Counterinsurgency and the War on Terrorism*, Daniel Byman noted that a major limitation to the indirect approach described "U.S. interests often diverge wildly from the interests of local allies in counterterrorism and counterinsurgency campaigns. SOF efforts to work 'by, with, and through' indigenous allies are constrained by the need to manage these divergences in interest."[11] Typically, indigenous partners come in two varieties: proxies (sometimes called surrogates) and partners. Proxies are defined principally as sub-state actors (e.g., militias) having a direct relationship with the United States and only a limited or non-existent relationship with the nation in which they operate. Partners in contrast are an element of an existing nation-state's security apparatus.

SOLUTIONS TO INCREASING SOF EFFICIENCY IN THE GRAY ZONE

Gray zone challenges are not new. Monikers such as irregular warfare, low-intensity conflict, asymmetric warfare, military operations other than war, and small wars were employed to describe this phenomenon in the past. President John F. Kennedy was speaking about the gray zone during his 1962 address to the U.S. Military Academy's graduating class when he said: "This is another type of war, new in its intensity, ancient in its origin—war by guerrillas, subversives, insurgents, assassins, war by ambush instead of by combat; by infiltration, instead of aggression, seeking victory by eroding and exhausting the enemy instead of engaging him."[12]

Gray zone challenges are not new. Monikers such as irregular warfare, low-intensity conflict, asymmetric warfare, military operations other than war, and small wars were employed to describe this phenomenon in the past.

Massive investments in technology and unrivaled expertise in combined arms warfare give the United States a conventional military dominance not seen since the Roman Empire. There is widespread agreement that, going forward, we will require an unprecedented level of interagency coordination capable of synchronizing all elements of national power. Absent a forcing function, government organizations will simply do more of the same. The new national security structure must be responsive, integrated, and adaptable. This constitutes a major overhaul of our security infrastructure; it will be difficult, and it will not take place overnight. Having more institutional capability outside of DoD optimized to operate between the clearly defined lanes of law enforcement and full-scale war will help avoid predictable U.S. responses. Specifically, as it relates to the use of SOF, the need for overhaul to evaluate effectiveness is critical.

The solution to overuse and its effect on readiness appears simple: either significantly decrease the number of U.S. SOF deployments or create more SOF. In terms of decreased SOF deployments, the presidential

administration could potentially choose this course of action, but the trend toward ever-increasing U.S. SOF involvement worldwide seems to discourage this as a viable solution. If decreasing SOF usage is not an option, creating more SOF presents a number of challenges. While it is not known how many of the proposed 1,000 personnel increase for the next fiscal year will be "operators," it is assumed that a significant portion of those individuals will require selection and special training. If this is the case, USSOCOM would need to attract more candidates to attend specialized selection and training. If successful in this regard, USSOCOM will need to modify standards for training courses such as Ranger School, the Special Forces Qualification Force, Basic Underwater Demolition, and SEAL training to obtain sufficient numbers of troops to expand the force. Does USSOCOM have a sufficient training cadre to accommodate this expansion, and would this affect the readiness of operational forces if more training cadre are required? Another concern is the practical level of USSOCOM expansion (i.e., how much larger USSOCOM can grow before its selection and training standards will need to be modified to create and sustain a larger force).

There are no easy solutions for the United States to solve the ever-evolving and expanding Gray Zone, a new battleground that meets the needs of the U.S. National Security Strategy. While the serious implications affecting U.S. SOF capabilities cannot be ignored, certain changes, if explored, could prove to be effective.

INCREASED USE OF FEDERAL LAW ENFORCEMENT ADVISORY ROLES

One part of the overall U.S. National Security Strategy is the use of federal law enforcement agency deployment of Special Agents acting as advisors to host nations as part of the U.S. State Department, and host nation joint efforts to counter illicit drugs and counterterrorism programs. In this capacity, U.S. Special Agents from various agencies utilize LEGATT (legal attachés) working out of the U.S. embassies around the world. According to the U.S. State Department website, more than 27 U.S. government agencies work overseas and all agency representatives serve under the authority of the U.S. ambassador of the country in which they work. The Departments of Commerce and Agriculture, like the Department of State and U.S. Agency for International Development (USAID), depend on their internationally-focused officers to carry out the agency's programs abroad, working to promote U.S. products and services to ensure that American farmers and businesses can compete fairly and effectively abroad. In developing countries, the USAID is an integral partner with the Department of State in carrying out the President's foreign policies through economic development and humanitarian assistance. Most embassies have a Defense Attaché Office (DAO) headed by a defense attaché (the DATT). The DAO, which usually has representatives from more than one military branch, represents the U.S. Defense Department and advises the ambassador on military matters. Other U.S. agencies with offices abroad include: the Departments of Homeland Security (Coast Guard and Immigration and Customs Enforcement), Justice (the Federal Bureau of Investigation and the Drug Enforcement Administration), Treasury, the Centers for Disease Control (CDC), and the Library of Congress, among others.[13]

USE OF INCREASED COMBINED FEDERAL LAW ENFORCEMENT IN INDIRECT APPROACH

The demand for the force is high, but the supply is low and fixed by the National Defense Authorization Act (NDAA) SOF zero growth statutes. The high demand for SOF units will continue although they are already overworked and frayed due to their high operational tempo. DoD must transform and institutionalize the development of General Purpose Force Advisor Units. SOF cannot, nor do they need to, conduct every advisor position in a Gray Zone conflict; combat service support and other military specialty positions can be offset by General Purpose Force Advisor Units. The recommendation is to use highly trained federal law enforcement agents as foreign advisors.

Currently, there are 14 federal law enforcement agencies that have Special Operations Programs, or units.

Currently, there are 14 federal law enforcement agencies that have Special Operations Programs, or units. Many of those agencies have received tactical training and instruction from Special Operations Forces at Fort Bragg, North Carolina, or Fort Benning, Georgia. In addition, many of these Special Agents come from the USSOCOM community and have transitioned into civilian roles. A large component of SOF Doctrine includes Foreign Internal Defense (FID). Foreign Internal Defense refers to U.S. activities that support a host nation's (HN's) internal defense and development strategy and program designed to protect against subversion, lawlessness, insurgency, terrorism, and other threats to their internal security and stability. By utilizing U.S. federal agents as a primary component to FID operations with supplemental support from SOF, the United States can reduce SOF operational

personnel while still achieving SOF doctrine. Additionally, because federal law enforcement agencies are working outside the Continental United States (OCONUS), the Department of State and at the invitation of the host nation where Title 10 challenges impact the use of SOF in certain situations can provide overlap as working in advisory capacities and not under military code.

EXAMPLES OF U.S. FEDERAL AGENCIES OPERATING AS ADVISORS

A primary example of where this has been successful would be the DEA's Foreign-Deployed Advisory and Support Teams (FASTs). One FAST has been permanently stationed in Afghanistan to conduct counternarcotics and counterterrorism missions, with the support of a second, rotational FAST team. FAST units provide immediate tactical responses to emerging threats around the globe. Using training methods reserved for the nation's most elite special operations forces, FAST units can rapidly deploy and bring to bear enormous firepower and tactical skill to eliminate or apprehend narcotics kingpins or terrorist leaders. Another example where federal agents operating in advisory capacities are Diplomatic Security Service Mobile Security Deployment (MSD) teams. Special Agents defend U.S. embassies and consulates when there is violence in the streets. They augment the U.S. Secretary of State's protective detail for trips to the most dangerous international locations, and MSD prepares security personnel at diplomatic missions for everything from screening visitors to surviving a terrorist assault. MSD ûelds nine teams of Special Agents. Each team of six is a small, cohesive unit that travels to global hot spots, spending half of its time on deployment. It ensures that the Diplomatic Security Service provides a quick response when danger threatens diplomacy anywhere in the world. These agents also assist in training security of foreign security officials.

BENEFITS OF SHARED COST

Cost should be a significant upfront consideration. For example, with the use of traditional military, the cost for military personnel during Operation IRAQI FREEDOM was estimated around $200 billion. Assuming we established $200 billion as the top end to "invest" in Iraq, it would at least force us to review our actions and evaluate our return on investment as we blew through initial estimates on our way to spending in excess of $2 trillion.[14] The Center for Public Integrity, a bipartisan group of national security and budget experts convened by the Stimson Center, estimated in a May 16, 2018, report that the cumulative tally is at least $2.8 trillion, and that the annual spending rate—while less than it used to be—still amounts to about 15 percent of the nation's discretionary budget. The pace has slowed since 2008, when counterterrorism expenditures by the State, Defense, Homeland Security, and other federal departments reached an estimated $260 billion—or 277 percent more than the rate in 2002, the report said. In 2017, that annual spending rate stood around $175 billion.[15]

According to the FY18 Defense Authorization Act Section 1202. "The Secretary of Defense may, with the concurrence of the relevant Chief of Mission, expend up to $10,000,000 during each of fiscal years 2018 through 2020 to provide support to foreign forces, irregular forces, groups, or individuals engaged in supporting or facilitating ongoing and authorized irregular warfare operations by U.S. SOF.[16] The FY 2019 budget request proposes a total of $8.92 billion in direct budget authority to carry out the FBI's national security, criminal law enforcement, and criminal justice service missions.[17] Taking into consideration the amount of money allocated to total U.S. counterterrorism efforts, increased cost-sharing initiatives among the use of interagency agency advisory operations would provide additional funds allocated to joint efforts, as well as decreased congressional oversight directly coming from U.S. Special Forces.

CONCLUSION

In 2016, the U.S. Army War College published a report titled "Outplayed: Regaining the Strategic Initiative in the Gray Zone." The report noted that:

> U.S. defense strategists and planners must dispense with outdated strategic assumptions about the United States, its global position, and the rules that govern the exercise of contemporary power. In fact, the U.S. defense enterprise should rely on three new core assumptions. First, the United States and the U.S.-dominated status quo will encounter persistent, unmitigated resistance. Second, that resistance will take the form of gray zone competition and conflict. Finally, the gray zone will confound U.S. defense strategists and institutions until it is normalized and more fully accounted for by the DoD. These assumptions, combined with the gray zone's vexing action-inaction risk dilemma, indicate there is an urgent necessity for U.S. defense adaptation. Without it, the United States introduces itself to enormous strategic risk. The consequences associated with such failure to adapt range from inadvertent escalation to general war, ceding control

of U.S. interests, or gradual erosion of meaningful redlines in the face of determined competitors. These risks or losses could occur absent a declared or perceived state of war.[18]

The biggest mistake current U.S. policymakers can make is the continued overuse of SOF personnel and underuse of combined intelligence agencies.

Unconventional warfare, whether conducted by the United States or any other state seeking to advance its national interests through Gray Zone proxy warfare, has to continue to evolve to meet changing global conditions. One certainty in a world of continuing disorder, a world bereft of Cold War clarity and relative "stability," where globalization has enabled almost continuous change, is that the UW mission must continue to adapt and so must those responsible for executing it. The Gray Zone is the present and the future. The biggest mistake current U.S. policymakers can make is the continued overuse of SOF personnel and underuse of combined intelligence agencies. Future policymakers should be cognizant of the limitations of both SOF approaches. For the direct approach, the strategic effects are likely to be limited without additional supporting efforts. Direct action against terrorist and insurgent leadership can achieve tactical and operational effects, buying space and time for other efforts. Absent additional effort, however, direct action can only manage and limit strategic challenges, disrupting plots and degrading capabilities, not fully defeat them. For an indirect approach, it is imperative that U.S. policymakers identify ways to help offset the use of SOF personnel whether it be through increased support for indigenous forces or increased support from federal agencies through the utilization of specialized trained federal agents able to operate as advisors. Gray Zone conflicts may take years to gain an acceptable political positive result, but there are not enough SOF units that can deploy and engage in every Gray Zone conflict.

NOTES

[1] Office of the Director of National Intelligence, "National Intelligence Strategy 2019," n.d., https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf.
[2] Votel, Army General Joseph. *SOCOM Security Forum* (May 2015).
[3] Votel, Joseph L., Charles T. Cleveland, Charles T. Connett, and Will Irwin. "Unconventional Warfare in the Gray Zone," *Joint Force Quarterly*, January 2016. https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-80/Article/643108/unconventional-warfare-in-the-gray-zone/.
[4] DoD, Joint Publication, *Special Operations*. n.d. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_05.pdf (accessed 2014).
[5] DoD, Joint Publication, *Special Operations*. n.d. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_05.pdf (accessed 2014), p. 25.
[6] "U.S. Special Forces Operations Background and Issues for Congress." *Congressional Research Service.* March 28, 2019. https://fas.org/sgp/crs/natsec/RS21048.pdf.
[7] "ARSOF Fact Book 2019." *U.S. Army Special Operations Command.* n.d.www.soc.mil/USAOCHQ/Factbook2019_6%20Mar_edit01.pdf.
[8] Thomas, General Raymond A. III, interview by Senate Arms Service Committee. *U.S. Army Special Operations Command* (May 2017). WHY DOES IT START WITH III?
[9] Hennigan, W.J. "The New American Way of War." *Time.* November 2017. http://time.com/5042700/inside-new-american-way-of-war/.
[10] Hennigan, W.J.
[11] Byman, Daniel. "Friends Like These: Counterinsurgency and the War on Terrorism." *International Security* (MIT Press), 2006.
[12] Woolley, Gerhard, and John T. Peters. "Remarks at West Point to the Graduating Class of the U.S. Military Academy." June 6, 1962. *The American Presidency Project.* n.d. http://www.presidency.ucsb.edu/ws/?pid=8695.
[13] "Discover Diplomacy: What agencies work in U.S. Embassies." *U.S. State Department.* n.d. https://www.state.gov/discoverdiplomacy/docs/208086.htm.
[14] Trotta, Daniel. *"Iraq war costs U.S. more than $2 Trillion: Study.* 2013. http://www.reuters.com/article/2013/03/14/us-iraq-war-anniversary-idUSBRE92D0PG20130314.
[15] Donheiser, Julia. *War in Afghanistan and Iraq.* May 2018. https://publicintegrity.org/national-security/the-united-states-has-spent-at-least-2-8-trillion-on-counterterrorism-since-9-11/.
[16] *2018 Defense Authorization Act.* 2018. https://www.congress.gov/115/plaws/publ91/PLAW-115publ91.pdf.
[17] Federal Bureau of Investigation. *FY19 Budget Request Overview.* n.d. https://www.fbi.gov/news/testimony/fbi-budget-request-for-fiscal-year-2019.
[18] Nathan P. Freier. "Outplayed: Regaining the Strategic Initiative in the Gray Zone." Study, U.S. Army War College Press, 2016.

Carvent L. Webb II is a recent graduate of the Daniel Morgan Graduate School of National Security, completing a master's degree in National Security Studies. Earlier he received a graduate certificate in Intelligence from the University of Colorado at Colorado Springs and a BS degree in Criminal Justice from Fayetteville State University. He has been serving as an air marshal with the Federal Air Marshal Service since 2016. Additionally, he is the founder/CEO of a nonprofit organization that works to combat child illiteracy within low-income elementary schools. Since its launch in 2012, it has donated over 300,000 new reading books to elementary schools across the country. In his spare time, Carvent enjoys reading, writing, and weightlifting.

An Emerging Phenomenon:
Private Military and Security Companies in Latin America

by SFC (USA) Sebastian Moreno

INTRODUCTION

The proliferation of private military and security companies (PMSCs) in Latin America atomizes the security sector and eliminates the monopoly that nation-state governments have on the use of force. These PMSCs can potentially have effects on regional stability and U.S. military/Intelligence Community (IC) relationships with partner nation institutions, potentially as extensive as those on the individual nation-state governments in which they reside. However, there has been little study to date to ascertain their degree of impact, if any, on stability and friendly relationships.

Thousands of PMSCs now exist, employing an estimated two million people in the region, and that number is increasing.

According to the Inter-American Dialogue, Latin America is the world's most violent region, with a homicide rate three times the global average and eight of the ten most violent countries in the world.[1] The combination of drug cartels, narcoguerrillas, and "third generation" gangs' abilities to corrupt and conduct large-scale violence, along with rising socio-economic inequality, produces the conditions for a market to emerge in which PMSCs flourish.[2] Thousands of PMSCs now exist, employing an estimated two million people in the region, and that number is increasing.[3] The spread of privatized security creates a wide variety of challenges, from human rights issues to the growth of a security gap between socio-economic classes where the rich can pay for their safety while the poor remain exposed.

Due to U.S. economic and military partnerships across the region, and the immigration caused in large part by U.S. geographic proximity to it, Latin American regional stability should be a strategic concern for the IC. This includes better understanding of how PMSCs impact U.S. national security concerns in the region.

RELEVANCE TO THE INTELLIGENCE COMMUNITY

This topic is relevant to the United States due to how historically close the ties are among its IC and its military to those of partner nations in Latin America, and how the existence of PMSCs has affected and changed the "force calculus" in the region. These entities now exercise kinetic force, in addition to the traditional security forces of the nation-state governments themselves. Dating back to the Cold War and U.S. efforts to push back against communism in the Western Hemisphere, and continuing through to current counternarcotics efforts in Colombia and elsewhere, the U.S. military and the IC have been deeply embedded with partner nations and heavily invested in Latin American stability. Any phenomenon that has the potential to affect those partnerships should be studied carefully to best inform the direction of future policy in the region.

The study of the strategic effects of PMSCs in Latin America can inform immigration policy by forecasting socio-economic disparities regarding the detrimental effects of crime on the local populace. Such study can also inform military policy by helping the U.S. allocate resources properly and pursue transparency in how partner nation domestic security policy is being implemented. Moreover, this study can inform economic policy by exploring the conditions that led to the proliferation of PMSCs in the first place.

Four major topics on which to focus during the exploration of PMSCs and their effect on the stability of Latin America are (1) violence in Latin America, (2) the role and history of PMSCs in Latin America, (3) the role of state security sectors in Latin America, and (4) regulatory issues surrounding PMSCs. Understanding these topics allows us to understand how and why PMSCs have emerged as role players in regional stability.

VIOLENCE IN LATIN AMERICA

The emerging PMSC market is directly related to the high rates of crime in Latin America. Rising insecurity has created an increasing need for security forces to counter it. In the absence of the state security sector (military, law enforcement) supplying security, demand has made it inevitable that a private entity would step in to provide it. Understanding the perilous conditions brought about by poverty and organized crime can help us better understand the role that PMSCs play in Latin America.

Two styles of policing tactics that have stood out include* mano dura *(or firm hand) policies that are punitive and involve a heavy, overt presence of public security, and more community-based "citizen security" approaches that are more preventive and involve citizens in their own policing.

Transnational criminal organizations (TCOs) are among the greatest causes of insecurity that PMSCs were formed to confront. TCOs fuel corruption by bribing local law enforcement and judges, allowing the TCOs to operate with impunity. They impair the social and economic systems in a region, affecting a government's ability to govern and provide basic services. In addition, they paralyze communities in fear when their rivalries with other TCOs or with non-corrupt law enforcement entities cause bloodshed on public streets.[4] Different countries within Latin America have had varying experiences with TCOs. Some tactics used to combat them have been more successful than others, but the destabilizing effect on society is a common theme in each case.

Gathering insight into tactics that have been attempted in an effort to combat crime in Latin America gives us another view into the nature of the threat. Two styles of policing tactics that have stood out include *mano dura* (or firm hand) policies that are punitive and involve a heavy, overt presence of public security, and more community-based "citizen security" approaches that are more preventive and involve citizens in their own policing.[5] If the state security sectors can learn from past successes and apply these tactics, they can ensure that the state retains control over the use of force and the imposition of internal security. This would bolster public trust in institutions and contribute to a more stable environment across Latin America.

GROWTH OF PRIVATE MILITARY AND SECURITY COMPANIES

Latin America's violence and insecurity, driven by organized crime, street gangs, and government corruption, have been the catalysts for the enormous growth in PMSCs. Their composition in Latin America contributes to the difficulty in implementing existing regulations concerning their use. The PMSC industry is composed of a network of current and former military personnel, private security personnel, business elites, and government officials. The combination of well-trained operators with well-connected administrators produces an industry in Latin America that is very resistant to oversight, despite each country's efforts.[6] Improving accountability of PMSCs and ensuring they are not contributing more harm than good for the societies in which they operate should be a priority for all stakeholders.

LATIN AMERICAN STATE SECURITY SECTORS

The public security sector refers to all institutions whose duty it is to protect society from crime, disorder, and violence, including the military, law enforcement agencies, and intelligence agencies.[7] Their objective is to provide security as a public good and they are subject to laws and regulations no different than those of any other service.

Unfortunately, the state security sector in Latin America has been characterized by inefficiency and corruption for years due to the insidious influence of organized crime...

With respect to security, the relationship between the state and society must be built on trust and must be effective, legal, and accountable. Unfortunately, the state security sector in Latin America has been characterized by inefficiency and corruption for years due to the insidious influence of organized crime, and it has not been able to combat these dual threats effectively. However, there are examples of successful security sector reforms that can be used as models for other countries.

According to a senior official in the government of former President Juan Manuel Santos, the strategy of Colombian leadership to confront its internal security problems was three-pronged: aggressive military operations to regain the strategic initiative against armed insurgent groups, the planning and implementation of an end to the armed

conflict, and a transformation of the public security forces (military and police) to achieve dominance over adversaries far into the future.[8] The role that the public sector played in improving security in this large South American nation can serve as a case study on how a country can manage its own security without outsourcing to PMSCs.

REGULATORY ISSUES

Existing international regulation of PMSCs is unworkable due to outdated definitions and no mechanisms through which implementation is possible. National efforts to regulate PMSCs are ineffective in large part due to the widely varying definitions of them from country to country. Furthermore, the transnational nature of PMSCs makes them particularly hard to regulate. Firms can be created, broken up, merged, or moved from one country to another in order to escape oversight and jurisdiction. Self-regulation has been floated as an alternative idea to make up for the absence of effective oversight. However, there are no clear results on the effectiveness of this effort.[9]

Anne-Marie Buzatu discusses three types of regulatory initiatives regarding the use of PMSCs that have been undertaken at the international and national levels in recent years: private (industry internal), public (state and international), and public-private.[10] Understanding what efforts have been undertaken is important for formulating a decision as to which direction to take next with respect to PMSC regulation.

KEY QUESTIONS

The key questions that should guide further research into PMSCs in Latin America include:

1. Are the security sectors, public and private, respecting domestic/international law regarding use of force?
2. To what extent has the state ceded authority on the use of force in security matters?
3. To what extent has the use of PMSCs resulted in more internal security?
4. What side effects has the use of PMSCs had on social conditions?

[Editor's Note: To formulate a comprehensive plan for overseeing and regulating private military and security companies, which will continue to thrive as long as unfavorable socio-economic conditions in the region persist, these questions must be answered. As a former Foreign Area Officer for Latin America who sometimes felt threatened while serving in such countries as Colombia, Peru, and Panama, I am fully aware of the need for PMSCs to supplement public security forces and protect a vulnerable populace. At the same time, I can understand how these entities can have deleterious effects if not properly controlled. I agreed to be the thesis committee chair for this research because it is an important issue that needs to be addressed directly and soon.]

NOTES

[1] Robert Muggah, "Fighting Organized Crime in Latin America: Between *Mano Dura* and Citizen Security," in *Unfilled Promises: Latin America Today*, eds. Michael Shifter and Bruno Binetti, Inter-American Dialogue (Washington, DC, 2019), 28-29.
[2] Robert J. Bunker and John P. Sullivan, "Integrating Feral Cities and Third Phase Cartels/Third Generation Gangs Research: The Rise of Criminal (Narco) City Networks and Blackfor," *Small Wars and Insurgencies* 22, no. 5 (2011): 764.
[3] "Kinosian and Bosworth-2018-Challenges and Good Practices in Regulating Privat.Pdf," n.d., accessed September 20, 2019, https://www.thedialogue.org/wp-content/uploads/2018/03/Security-for-Sale-FINAL-ENGLISH.pdf.
[4] Phil Williams, "Transnational Criminal Organizations and International Security," *In Athena's Camp: Preparing for Conflict in the Information Age*, eds. John Arquilla and David Ronfeldt, by Alvin Toffler and Heidi Toffler, RAND Corporation, 1997, 315-338, http://www.jstor.org/stable/10.7249/mr880osd-rc.19.
[5] Muggah, 27-53.
[6] James Bosworth and Sarah Kinosian, "Security for Sale: Challenges and Good Practices in Regulating Private Military and Security Companies in Latin America," The Inter-American Dialogue (2018).
[7] Muggah, 27-53.
[8] Juan Carlos Pinzon, "Colombia Back from the Brink: From Failed State to Exporter of Security," *PRISM* 5, no. 4 (2016): 2-9, https://www.jstor.org/stable/26459207. [Editor's Note: Pinzon is a former Minister of Defense and Colombian Ambassador to the U.S.]
[9] Anne-Marie Buzatu, "Regulating Private Security Companies," *Towards an International Code of Conduct for Private Security Providers: A View from Inside a Multi-stakeholder Process* (London: Ubiquity Press, 2015), 9-27, http://www.jstor.org/stable/j.ctv6zdbkk.4.
[10] Ibid.

Sergeant First Class (USA) Sebastian Moreno earned a Master of Science of Strategic Intelligence degree at National Intelligence University. He is a Special Forces engineer most recently assigned to the 7th Special Forces Group (Airborne) based at Eglin AFB, FL. He has conducted several combat and non-combat deployments to Iraq, Afghanistan, Guatemala, Honduras, and Colombia. Sebastian previously served as an infantryman with the 1st Ranger Battalion based at Hunter Army Airfield in Savannah, GA.

Porter's Four Corners:
An Argument for Counterterrorism Analysis Utility

by Brianna N. Alverson

INTRODUCTION

Different academic disciplines can often be oddly resistant to utilizing methodologies from outside their field. Intelligence is no different. Go-to texts on analytic methods by authors within the national security realm often focus on discussion of such classic methods as Analysis of Competing Hypotheses, while competitive intelligence texts generally stick to discussion of traditional business tools such as SWOT analysis[1] or value chain analysis. What these texts lack is a cross-pollination of ideas from outside their own traditional spheres of analysis, and that really is a shame for disciplines that should always be trying to push the boundaries of analytic potential. Richards Heuer once wrote, "To penetrate the heart and soul of the problem of improving analysis, it is necessary to better understand, influence, and guide the mental processes of analysts themselves."[2] We, as analysts, should be thinking outside of the boxes of our specific disciplines and endeavor to expose ourselves to new methods across the analytic spectrum, even if at first glance they may seem irrelevant to our specific intelligence subsets. This article aims to lay out a logical argument for expanding the use of Porter's Four Corners, a competitive intelligence model used within the realm of business, to the realm of counterterrorism analysis for the purpose of helping to formulate estimates concerning terrorist group and counterterrorism partner courses of action.

WHAT IS PORTER'S FOUR CORNERS?

Porter's Four Corners is an analytic model used in the field of competitive intelligence to analyze a business's competition. Created by Harvard business professor Michael Porter, the Four Corners model was designed as a predictive tool for helping an analyst to determine a competitor's likely courses of future action based on four main factors: the competitor's drivers or goals, assumptions, current strategy, and capabilities. Analyzing these factors provides a more holistic picture of a competitor and helps competitive intelligence analysts formulate robust estimates of competitors' likely future strategies within the context of their goals versus limitations. Brandon Conroy, a competitive intelligence analyst at Northrop Grumman, writes: "Looking at the motivations of a competitor…and at the gaps between assumptions and reality contributes to the development of more accurate predictions of future actions with a relatively high level of confidence."[3] The following six sections expand on each of the "corners" of Porter's model and discuss the model's overall strengths and weaknesses.

Drivers/Goals

The drivers/goals corner of Porter's model aims to answer the question: "What drives the competitor?"[4] This involves an analysis of both the overtly stated and implied future goals of the competitor. In a business example, some of a company's identified goals may include an overtly stated desire to grow beyond the company's traditional customer base or an implied desire to patent new technology within a particular division based on recent patent applications and changes in research and development allocations. Understanding a competitor's drivers is important for identifying the potential courses of action that would be most conducive to achieving its goals.

Assumptions

The assumptions corner of the Porter's Four Corners model aims to identify the assumptions a competitor holds about itself, its industry, and the external environment in which it operates.[5] These assumptions will influence the competitor's strategic decisions, and analysis of these assumptions can also help in identification of biases and blind spots.[6] Identification of these biases and blind spots then opens up the potential for strategic exploitation of them to gain a competitive advantage over the competitor. For example, perhaps the competitor assumes that the environment in which it operates will remain favorable for business, while the analyst has identified macro-level events that indicate otherwise, such as a new law or policy stance that in actuality would negatively impact the competitor's business.

Current Strategy

The current strategy corner of the Porter's Four Corners model aims to answer the question: "How is the business currently competing?"[7] It is important to note that there can be differences between a competitor's intended strategy and its actual strategy. The former refers to the competitor's expressed strategy "as stated in annual reports, interviews, and public statements," while the latter is the competitor's actualized strategy "as evidenced by acquisitions, capital expenditure, and new product development."[8] If a current strategy is proving fruitful for a competitor, it can be reasonable to estimate that the competitor is likely to continue using it. Current strategies might include growth strategies, research and development strategies, marketing strategies, recruitment strategies, or indicators of downsizing or streamlining.

Capabilities

The capabilities corner of the Porter's Four Corners model aims to identify both the strengths and weaknesses the competitor possesses.[9] For example, a competitor's limited finances could be a significant weakness, while a management team comprised of individuals with many years' experience in their roles could be a significant strength that gives the competitor a strategic advantage. Other capabilities analyzed might include a competitor's marketing skills or the skills and training of its work force.[10] Overall, the capabilities corner is meant to help analyze the way a competitor might act through the lens of what the competitor is realistically capable of doing. While the drivers, assumptions, and current strategy of an organization "will determine the nature, likelihood, and timing of a competitor's actions," its capabilities "will determine its ability to initiate or respond to external force."[11]

Putting the Corners Together: Future Strategy/ Competitor Response

The end result of a Porter's Four Corners analysis is an estimate of the competitor's likely future strategy or response to certain events based on the information collected and considered in each of the model's corners. Looking at drivers, assumptions, current strategies, and capabilities allows an analyst to compare a competitor's ideal course of action versus what it is actually capable of doing, helping to build a clearer picture of likely future scenarios. The final estimate and insight gained from each of the corners can help an analyst identify weaknesses and opportunities to gain competitive advantage. This information helps decision-makers build effective offensive and defensive strategies. The competitor analysis achieved through the Four Corners model can help build offensive strategies that "can be implemented more quickly and with greater impact to capitalize on your [company's] strengths," as well as defensive strategies that "can be employed more deftly to counter the threat of the competitor companies exploiting your company's weaknesses."[12]

Strengths and Weaknesses of the Four Corners Model

The Porter's Four Corners model has several strengths and a few notable weaknesses.[13] In terms of strengths, the model can help an analyst reveal a competitor's strategic weaknesses, identifying areas ripe for exploitation by the analyst's company. The model also aids in anticipation of a competitor's likely response to strategic pressure from the analyst's company and other competitors, as well as to changes in the environment in which the competitor operates. Additionally, the model encourages a proactive approach to competitors instead of simply reacting to competitor strategies as they are implemented. Finally, by virtue of being a structured analytic approach, Porter's Four Corners serves the important utility of helping an analyst organize and visualize the interrelationships of important factors in a competitor's decision-making process. Richards Heuer writes:

> The limited capacity of working memory is the source of many problems in doing intelligence analysis. It is useful to consider just how complicated analysis can get, and how complexity might outstrip your working memory and impede your ability to make accurate judgements… There are two basic tools for dealing with complexity in analysis—decomposition and externalization.[14]

The Porter's Four Corners model aids in breaking down the problem into its core component parts (decomposition) and allows the analyst to get the problem out of his/her head and down on paper (externalization), subsequently aiding in overall better analysis.[15]

The biggest criticism of Porter's model is fairly specific to its use in business. Businesses have to worry about being an industry leader (innovative and different) versus an industry follower (simply mimicking what competitors do). In business, obsessively profiling competitors can lead to copycat behavior to match the competition or a blindness in regard to identifying new emerging competitors or macro-level threats and opportunities. Another weakness that I would argue Porter's Four Corners faces lies with its assumptions corner. Identifying a competitor's assumptions runs the risk of falling victim to cognitive biases, such as mirror-imaging one's own assumptions as the likely assumptions of the competitor. As such, I would argue that the assumptions corner would benefit from another layer of analytic methodology, such as an Analysis of Competing Hypotheses, to reduce the likelihood of faulty assumptions being used in the final analysis.

APPLICATION IN COUNTERTERRORISM ANALYSES

Analysis of Terrorist Groups

Porter's Four Corners is designed to analyze an organization. Though its creation was intended for the narrow scope of application to organizations within a business environment, it is arguably well-suited for an analysis of any organization, including terrorist groups. These groups, such as al-Qaeda, ISIS, and Boko Haram, possess goals and drivers, assumptions, strategies, and specific strengths and weaknesses. Some of the groups even resemble businesses in their operations, with structured financing systems, supply chains, training, recruitment, and marketing strategies, for example. As such, it is logical to posit that Porter's method designed for making an analytic prediction of a business organization's future courses of action based on these factors could also be applied by a counterterrorism analyst seeking the same insights concerning a terrorist organization.

For example, drivers may include statements drawn from sermons, public statements, written documents, intercepted communications, interviews, or propaganda videos on the terrorist group's end goals. They could also include likely shorter-term goals based on intelligence and past actions, such as the elimination of a certain ethnic group, removal of a political figure, capture of a specified city, or acquisition of certain classes of weapons. Assumptions may include the group's belief in its ability to carry out certain attacks successfully, its beliefs concerning the capabilities of the United States and its willingness to carry out operations, and beliefs concerning the group's relationship with governments or other terrorist organizations.

Identification of assumptions of continued friendly relationships with governments or other groups could prove especially beneficial for planners seeking opportunities for carrying out surprise operations against a terrorist group. For example, leadership in the group may assume it still has the support and protection of a nation-state ally, while the U.S. has actually negotiated a new counterterrorism partnership behind closed doors with the nation-state. If the terrorist group has been determined to believe it still benefits from a favorable relationship with this partner, planners may have the opportunity to coordinate traps or perform surprise operations against targets the group assumed were unknown to or out of reach of U.S. counterterrorism efforts.

Current strategies and capabilities can also be determined and analyzed within Porter's Four Corners model. Current strategies may be overt statements of tactical intentions to carry out suicide attacks to instill public fear, or may be determinations of strategies relating to recruitment, financing, and movement gleaned from intelligence reports or analysis of information found publicly, such as from jihadist websites or social media. Capabilities would encompass the strengths and weaknesses of a particular group: Is the group well-financed? Is the group backed by a nation-state ally? Is the group supported by the local populace? Does the group have a strong marketing capability for spreading its message and recruiting new members? What is the group's structure? How many members does it currently have? What is the experience or influence of its core leadership? All of these are questions that can help gain insight into a terrorist group's realistic ability to carry out certain attacks, establish itself in certain areas, grow, and evade U.S. counterterrorism efforts.

Much like its use in business, the Four Corners model can help reveal strategic weaknesses, as well as help anticipate responses to certain actions and pressure put on groups by counterterrorism efforts.

Analyzing Porter's four corners—drivers, assumptions, current strategies, and capabilities—can provide a structured and holistic understanding of a terrorist group and allow an analyst to make a confident estimate of the group's likely future courses of action based on the interplay of these factors. Much like its use in business, the Four Corners model can help reveal strategic weaknesses, as well as help anticipate responses to certain actions and pressure put on groups by counterterrorism efforts. It also has the added benefit of providing a highly-structured chain of logic that can be referred to when supporting an argument for a particular assessment or when re-assessing flaws in estimates based on actual outcomes. I argue that, overall, the Porter's Four Corners model is a useful analytic tool that would have good utilization in structuring an analysis of a terrorist group.

Analysis of Counterterrorism Partners

The argument that Porter's Four Corners could also be used to evaluate counterterrorism partners is inspired by Stephen Tankel's discussion of countries' differing threat perceptions and conflicting priorities when partnering with the U.S. against terrorist threats.[1616] Stephen Tankel, *With Us and Against Us: How America 's Partners Help and Hinder the War on*

As Tankel writes, "How a partner perceives threats to itself and the extent to which its threat perceptions are congruent with U.S. threat perceptions are critical factors in determining the potential for counterterrorism cooperation."[17] The U.S.

benefits from partnerships in order to extend its counterterrorism reach to the foreign countries from which the terrorist groups originate and in which they operate. However, partners may not always be fully cooperative. Tankel's argument is that often many of these partners both simultaneously help and hinder the U.S.'s efforts. For example, Pakistan is an important counterterrorism partner that actively aids the U.S. in operations against some terrorist groups, while also actively sheltering and warning other groups it perceives as important for its geopolitical interests. Due to such difficulties, a thorough analysis of partners' likely true courses of action would be beneficial to the decision-makers forming and operating within these tenuous alliances.

Here, too, Porter's Four Corners has the potential to be a useful analytic tool. Through analysis of the primary factors built into Porter's model, an analyst can come to a structured conclusion of a country's likely strategy concerning counterterrorism and a U.S. partnership. Drivers may include overt declarations, such as China's 2025 plan, or more subtle goals, such as strategic geopolitical advantage over a neighboring nation. Assumptions may include perceptions of threat and utility of the terrorist group in question, assumptions about internal politics, assumptions concerning the U.S., and assumptions concerning wider international politics. Strategies may consider current internal and external political strategies, as well as counterterrorism strategies. Finally, a country's capabilities may be assessed to determine its realistic likely contribution to a counterterrorism partnership. Does the country have a well-trained military? Does it have financial resources to support counterinsurgency operations or programs designed to counter violent extremism? Does it face public support for the terrorist group of concern? Does the country suffer from serious ethnic or religious schisms? All of these are questions that could help assess the strengths and weaknesses of a country in relation to its counterterrorism capabilities. Once each of the corners of Porter's model has been assessed, an analyst would have a structured and holistic picture of a country in which to base a robust estimate of its likely counterterrorism strategy and strategy concerning a U.S. partnership.

CONCLUSION

Porter's Four Corners is a useful tool for structuring analyses of motives and means to estimate likely future courses of action. Though it was designed for analyzing competitor businesses, it is arguably well-suited for analyzing any organization and could have excellent use in cases of counterterrorism analysis. Porter's model could help counterterrorism analysts organize and better assess the interplay of the important components of a terrorist group's or partner country's decision-making process, allowing them to arrive at robust and confident assessments of their likely actions for the decision-makers burdened with deciding how to allocate limited resources, to what extent information should be shared with partners, and how best to combat and prevent terrorist threats.

NOTES

[1] "SWOT" stands for "strengths, weaknesses, opportunities, and threats."
[2] Richards Heuer, Jr., *Psychology of Intelligence Analysis*, 2nd ed. (Washington, DC: Center for the Study of Intelligence, 2001), 173.
[3] Brandon Conroy, "SCIP DC-Greater Metro Area Chapter Presents: Porter's Four Corners Revisited," *SCIP Insight* 4, no. 3 (2012), accessed March 29, 2019, http://www.growthconsulting.frost.com/web/images.nsf/0/ABBEA2B55E00B4A3862579C700477B46/$File/SCIP12_Vol4_I3_ChapternewsBrandon.htm.
[4] Babette Bensoussan and Craig Fleisher, *Analysis Without Paralysis: 12 Tools to Make Better Strategic Decisions*, 2nd ed. (Upper Saddle River, NJ: Pearson Education, Inc., 2013).
[5] Craig Fleisher and Babette Bensoussan, *Strategic and Competitive Analysis: Methods and Techniques for Analyzing Business Competition* (Upper Saddle River, NJ: Prentice Hall, 2003).
[6] Jim Downey, "Strategic Analysis Tools" (Topic Gateway Series No. 34, London: The Chartered Institute of Management Accountants, 2007), accessed March 29, 2019, https://www.cimaglobal.com/Documents/ImportedDocuments/cid_tg_strategic_analysis_tools_nov07.pdf.pdf.
[7] Fleisher and Bensoussan, *Strategic and Competitive Analysis*.
[8] Downey, "Strategic Analysis Tools," 10.
[9] Fleisher and Bensoussan, *Strategic and Competitive Analysis*.
[10] Downey, "Strategic Analysis Tools."
[11] Ibid., 10.
[12] Bensoussan and Fleisher, *Analysis Without Paralysis,* 46-47.
[13] Ibid.
[14] Heuer, *Psychology of Intelligence Analysis*, 85-86.
[15] Ibid.
[16] Stephen Tankel, *With Us and Against Us: How America's Partners Help and Hinder the War on Terror* (New York: Columbia University Press, 2018).
[17] Ibid., 13.

Brianna N. Alverson is a second-year graduate student in Mercyhurst University's Applied Intelligence program. She holds an undergraduate degree in International and Global Studies with a double major in Political Science from the Rochester Institute of Technology, where she first became interested in intelligence and counterterrorism. Her current interests span the spectrum of the intelligence discipline but primarily focus on global conflicts, counterterrorism, cyber threats, and analytic methods.

The Dilemma Between Morality and Intelligence Efficiency in the United States

by Tanguy Osman

Intelligence agencies around the world do whatever it takes in order to ensure their national security, often going far beyond standard ethical boundaries. While most agencies around the world run their activities unencumbered due to lack or regulation or lack of the population's interest in knowing what they are up to, the Intelligence Community (IC) of the United States is unique. The IC has often been proclaimed as a collection of the most effective intelligence-gathering agencies in the world. Its successful operations have at times been glorified in movies and literature for its crafty tactics. This allows for a rather peculiar trend in which the population of the U.S. generally knows about and is enamored by the operations of the intelligence agencies. This, combined with the distrust U.S. citizens feel toward their government and the political system in place, however, has caused some great difficulties for the IC. The activities it conducts have been called into question for their apparent lack of morality, forcing the IC and the executive branch to try and juggle between the values of morality and the pursuit of intelligence effectiveness without hindering national security. The democratic system of the United States allows the opinions of its citizens to play a pivotal role in deciding national affairs and certain aspects related to intelligence gathering. As a result, I will discuss certain scenarios that are crucial to the success of the IC, examining how the political system together with the question of morality is endangering that success and the impact it has on national security.

Saudi Arabia has traditionally been considered a strong ally of the United States when it comes to the Middle East region. It has provided unprecedented benefits to the U.S., whether in the form of enormous arms purchases or in carrying out U.S. foreign policy.[1] One of the greatest benefits of Saudi Arabia is its ability to share crucial intelligence on anti-Western organizations that wish to infringe on the sovereignty of the United States.

The rise of Islamic fundamentalism and its anti-Western views, specifically against the U.S., has proven to be a major threat to national security. Al-Qaeda, ISIS, and Hezbollah are just a few of many groups that would be delighted with the destruction of the U.S.[2] The attacks on 9/11, the Boston Marathon bombing, and the Orlando shooting were all devastating, horrific acts that occurred on U.S. soil. Additional attacks that were targeted against U.S. citizens but occurred outside the country included the embassy bombings in Kenya and Tanzania and the USS *Cole* bombing in Yemen, among others.[3] The ideology which drives these acts is at an all-time high and the implications it has for U.S. security are extremely serious.

The democratic system of the United States allows the opinions of its citizens to play a pivotal role in deciding national affairs and certain aspects related to intelligence gathering.

While it is true that a great number of these organizations are funded by Saudi citizens, the government of Saudi Arabia has made it clear that this ideology is producing an existential crisis and that it is willing to direct a great number of its resources in order to extinguish it.[4] If the United States wishes to combat Islamic fundamentalism, it cannot do so without the help of local allies. In 2010 Crown Prince Mohammed Bin Salman helped the U.S. discover a plot by Al-Qaeda to insert bombs on UPS and FedEx planes.[5] Additionally, in 2011, the CIA was allowed to set up a drone base in Saudi Arabia in order to target Al-Qaeda in the Arabian Peninsula.[6] Even though Saudi Arabia is partly to blame for the financial success of these organizations, it would be unwise to claim that it has been of no benefit to U.S. intelligence-gathering capabilities.

The U.S. relationship with Saudi Arabia has largely remained unquestioned, even amid a variety of controversial activities by the Saudi Kingdom, such as it being responsible for violating human rights in Yemen, its oppression of activists, and its lack of equality. However, all that changed with the death of *Washington Post* columnist Jamal Khashoggi. With the majority of evidence pointing to the Crown Prince himself having had a central

role in the murder, Saudi Arabia's morality was thrust clearly in the spotlight.[7] Morality is not an issue unless the public knows and is aware of it. Suddenly, all of its previous morality issues were brought up and the general population of the United States, together with a majority in Congress, exclaimed that the activities of Saudi Arabia could no longer be tolerated. This, in turn, caused a great number of people to demand the severing of ties with Saudi Arabia.[8] However, cutting ties with the Kingdom also means ceasing intelligence sharing and cooperation. Such a decision would have major implications for the United States' ability to prevent potential terrorist attacks by Islamic fundamentalists, many of whom are based in the Middle East and Central Asia. Such a scenario provides us a perfect example of how abiding by our moral values would potentially harm our personal safety.

While Saudi Arabia has overlooked its share of what could be considered universal moral norms, morality has never been an issue exclusive to foreign countries. What if one's own country is overstepping moral boundaries for the sake of national security? One will not try to sever ties with his/her own country; rather, he/she would try to change the activities of the government. This begs the question: Are people aware of the possible consequences their actions might have? Pursuing moral values sometimes brings a risk to personal safety. When is the risk to personal safety sufficiently high to supersede moral values? While we cannot directly measure the personal risk they bring, we will explore the issues at hand and how immoral intelligence activities address those issues.

One category of crime—hate crime—could substantially benefit from an invasion of privacy.

Ever since Edward Snowden exposed the NSA's surveillance program, the invasion of privacy has become a hot topic.[9] While the program consisted of only limited surveillance, we will discuss how privacy invasion could help with lowering the overall crime rate and detecting possible terrorist attacks before they happen. One category of crime—hate crime—could substantially benefit from an invasion of privacy. The severity of hate crimes in today's world is drastic. In 2018 Robert Bowers killed 11 people and injured six at a synagogue, and James Fields, Jr., drove his car over an ethnically diverse group in 2017. The increasing patterns of hate crimes and the increasing number of casualties they are producing are a threat to national security and the lives of U.S. citizens. However, proper monitoring and surveillance may be able to mitigate that threat. Bowers repeatedly posted on his Gab accounts regarding his hatred toward the Jewish community, and Fields promoted white supremacist views on his social media and called for violence against non-white people.[10] [11] One form of monitoring and surveillance would allow intelligence agencies to access social media platforms and personal phone calls by individuals. Doing so would allow them to detect people who conduct a pattern of hateful speech and, in turn, flag them as ones who are more inclined to commit hate attacks. Continuous monitoring of these accounts could prove pivotal in preventing numerous hate crimes, which have begun flourishing of late.

This is one of the many difficulties in working for the IC; its personnel must work within the boundaries of what is morally acceptable, while simultaneously ensuring the best security possible.

An example of successful monitoring which benefits national security would be that conducted under the Foreign Intelligence Surveillance Act. FISA gives the U.S. government legal permission to spy on foreign entities for the sake of safeguarding the nation. According to the CIA, the Act has been crucial to learning more about terrorist organizations abroad and preventing their plans from coming to fruition.[12] However, we know today that the threat to U.S. national security does not exclusively come from outside the country; the threat from inside is just as grave. The question now for the overall U.S. population is whether or not this is a sufficient reason to allow intelligence agencies to spy on them for the benefit of personal safety. Until today, the majority of people did not think so, because they were not directly responsible for protecting their nation. They will not see the necessity of such a program until they themselves are subjected to its consequences. However, unlike the general population, the IC cannot wait for a disaster to occur to validate the use of such a program. The IC is responsible for doing everything it can in order to prevent such attacks from happening in the first place. This is one of the many difficulties in working for the IC; its personnel must work within the boundaries of what is morally acceptable, while simultaneously ensuring the best security possible.

The CIA especially, ever since its beginnings as the Office of Strategic Services (OSS) during World War II, has been continuously lambasted for its methods. A more recent example is that of Gina Haspel, current Director of the Agency, who was allegedly pursuing enhanced

interrogation techniques (EIT). This program, which would be correctly translated to torture, among other things, has been criticized for its lack of ethical values. The CIA claimed that EITs were necessary in order to hinder terrorist plots successfully. In one of its declassified memos it stated, "We believe that intelligence acquired from these interrogations has been a key reason why al-Qaeda has failed to launch a spectacular attack in the West since 11 September 2001."[13] Moreover, James Mitchell, who helped create the CIA's 9/11 interrogation techniques, countered, "In my mind, the temporary discomfort of a terrorist who has voluntarily taken up arms to destroy our way of life does not outweigh my moral obligation to do what I can to save hundreds, maybe thousands of people."[14]

The interests of U.S. citizens have diverged from the government's interests on a number of occasions. U.S. citizens in general are suspicious of their government, constantly question its operations, and vocally express any changes they wish to occur.

No matter the efficiency, the political system in the U.S. prevents the IC from pursuing projects simply according to measures of effectiveness. The public's approval of IC behavior is crucial to Congress. Subsequently, the IC cannot freely operate within its own realm. In turn, it needs the approval of Congress.

Congress is the only branch of the U.S. government that is directly elected by the people; therefore, it is crucial for the Senators and the Representatives to gain the favor of the population. If they wish to be reelected, they must satisfy the wishes of the people who reside in their state. Specifically, this applies to members of the House of Representatives, since they do not have the luxury of losing support in the short term with hopes of regaining it later on, as their 2-year term is relatively short to begin with. If the people disagree with the operations of the executive branch, it is up to Congress to defend those interests. The interests of U.S. citizens have diverged from the government's interests on a number of occasions. U.S. citizens in general are suspicious of their government, constantly question its operations, and vocally express any changes they wish to occur. According to a national election study, the majority of U.S. people distrust their government. Today, only 3 percent trust their government "always" to do the right thing and only 14 percent trust their government to do the right thing "most of the time."[15] Additionally, the way that the political system is structured in the U.S. allows the people to take action on their concerns through Congress.

As of today, Congress oversees the activities of the IC in the executive branch and has the power to take corrective measures when appropriate. The House Permanent Select Committee on Intelligence (HPSCI) and the Senate Select Committee on Intelligence (SSCI) represent the House of Representatives and the Senate, respectively, and each has a responsibility for overseeing the activities of the IC.[16] Additionally, Congress is credited as having the "power of the purse" because it can for the most part control how the budget of the government is spent through the appropriations committees of the House and the Senate. If the IC wants to undergo an operation or program, it has to include it in its upcoming budget requests which the executive branch passes to Congress for approval of funding. If the appropriations committee does not accept the request and finds that it is not in the best interest of the American people, then it can reject it completely or ask for certain modifications to be made.

This system was made for the purpose of removing the possibility of the executive branch abusing its powers. However, seeing how morality and intelligence efficiency conflict on numerous issues, there is a possibility the system places the U.S. at a disadvantage compared to other countries. Dictatorships have nearly autonomous control in how to run their intelligence operations; even democracies that lack certain regulations have greater freedom than the U.S. In a world of continuous competition, the U.S. may find itself struggling to keep up with other world powers such as Russia and China, whose moral values are rather ambiguous. For example, China passed a law in 2017 in which it has permission to monitor citizens, organizations, and institutions both domestically and internationally. In addition, domestic entities are legally required to cooperate and support any intelligence operation if the Chinese government requires them to.[17] If such a program were to be proposed in the U.S., the people would reject it immediately and prevent it from coming to fruition. China, however, is able to accomplish this even without the people's support because of its political structure. Such a law gives it a clear-cut edge over the intelligence-gathering capabilities of the U.S. Its lack of respect for moral values allows it to explore methods and programs out of reach by U.S. intelligence agencies.

Moral values are without a doubt a fundamental characteristic that is important to uphold as it defines our humanity. Yet, in a world largely driven by the aphorism "information is power," how much intelligence can a government risk? In this Information Age, the answer is not much. The world is dynamic and ever-changing. Every piece of intelligence is vital and may be key in giving a country an edge over others. The government of the United States and its IC are responsible for providing a

maximum secure environment for its citizens while simultaneously abiding by the moral boundaries upon which they insist. With the average citizen not knowing the effects of the direct and indirect implications that moral sustainment can have on intelligence gathering, the efficiency of the Intelligence Community will remain obstructed to a certain degree.

NOTES

[1] Irina Ivanova, "Saudi Arabia Is America's No. 1 Weapons Customer," CBS News, October 12, 2018, https://www.cbsnews.com/news/saudi-arabia-is-the-top-buyer-of-u-s-weapons/.

2 Christopher Henzel, "The Origins of Al Qaeda's Ideology: Implications for US Strategy," Spring 2015, https://www.cia.gov/library/abbottabad-compound/AC/AC109E252F2BC6B9C7D32EB31C211AA9_henzel.pdf.

3 CNN Library, "USS Cole Bombing Fast Facts," CNN, March 27, 2019, https://www.cnn.com/2013/09/18/world/meast/uss-cole-bombing-fast-facts/index.html.

4 Ian Black, "Saudi Arabia and Isis: Riyadh Keen to Show It Is Tackling Terror Threat," *The Guardian*, January 21, 2016, https://www.theguardian.com/world/2016/jan/21/saudi-arabia-isis-riyadh-terror-threat.

5 Mark Mazzetti, Robert F. Worth, and Eric Lipton. "Bomb Plot Shows Key Role Played by Intelligence," *The New York Times*, October 31, 2010, https://www.nytimes.com/2010/11/01/world/01terror.html.

6 "CIA Operating Drone Base in Saudi Arabia, US Media Reveal," BBC News, February 6, 2013, https://www.bbc.com/news/world-middle-east-21350437.

[7] Josh Lederman and Dennis Romero, "CIA Concludes Saudi Crown Prince Mohammed Bin Salman Ordered Killing of Khashoggi," NBCNews.com, November 16, 2018, https://www.nbcnews.com/news/us-news/cia-concludes-saudi-crown-prince-mohammed-bin-salman-ordered-killing-n937476.

[8] Iqsquared, YouTube, March 12, 2019, https://www.youtube.com/watch?v=qi0T0owgW3M.

[9] Patrick Toomey, "The NSA Continues to Violate Americans' Internet Privacy Rights," American Civil Liberties Union, August 23, 2018, https://www.aclu.org/blog/national-security/privacy-and-surveillance/nsa-continues-violate-americans-internet-privacy.

[10] Saeed Ahmed and Paul P. Murphy, "Here's What We Know So Far about Robert Bowers, the Pittsburgh Synagogue Shooting Suspect," CNN, October 28, 2018, https://www.cnn.com/2018/10/27/us/synagogue-attack-suspect-robert-bowers-profile/index.html.

[11] Gabriela Saldivia, "Fingerprints, DNA and Social Media Posts Helped FBI Identify Bomb Suspect Cesar Sayoc," NPR, October 27, 2018, https://www.npr.org/2018/10/27/661407090/fingerprints-dna-and-social-media-posts-helped-fbi-identify-bomb-suspect-cesar-s.

[12] David Shedd, "How the Section 702 Program Helps America Thwart Terrorist Plots," The Heritage Foundation, accessed April 29, 2019, https://www.heritage.org/terrorism/commentary/how-the-section-702-program-helps-america-thwart-terrorist-plots.

[13] Ryan Browne, "New Documents Shine Light on CIA Torture Methods," CNN, June 15, 2016, https://www.cnn.com/2016/06/15/politics/cia-documents-torture/.

[14] Alexandra King, "CIA Contractor: Enhanced Interrogation Techniques 'Saved Lives'," CNN, December 20, 2016, https://www.cnn.com/2016/12/17/politics/james-mitchell-advanced-interrogation-cnntv/index.html.

[15] "Public Trust in Government: 1958-2019," Pew Research Center for the People and the Press, April 19, 2019, https://www.people-press.org/2019/04/11/public-trust-in-government-1958-2019/.

[16] "About the Committee," About the Committee | Intelligence Committee, https://www.intelligence.senate.gov/about.

[17] Bonnie Girard, "The Real Danger of China's National Intelligence Law," *The Diplomat*, February 23, 2019, https://thediplomat.com/2019/02/the-real-danger-of-chinas-national-intelligence-law/.

A dual citizen of Lebanon and Belgium, Tanguy Osman has been shaped by his experience in two contrasting worlds and his curiosity in expanding his knowledge. He played professional basketball in Lebanon, acquired a bachelor's degree in Business Administration, worked for a technological firm that provided governmental services, and is currently pursuing a master's degree in International Security at George Mason University, after first studying at the Daniel Morgan Graduate School of National Security in Washington, DC.

Support NMIF in inspiring a new generation of intelligence professionals!

www.nmif.org

Seeking Help Is a Sign of Strength: Suicide Prevention within the Military

by Megan E. Connell-Cox

[Editor's Note: Although not addressing military intelligence personnel or issues per se, nonetheless I feel this essay is instructive for all military types who either served in the past, or may serve in the future, in a combat environment. PTSD and suicide do not discriminate by service, branch, specialty, gender, rank, or age. All of us are subject to these threats and should find these observations by the author illuminating. Her efforts to support the military, while enhancing her abilities through lifelong higher education, are truly admirable.]

OVERVIEW

Since the creation of the U.S. armed forces, there have been, and currently are, service members who experience service-connected events so traumatic, they live with psychological scars that can be life-threatening. These effects can be long-term mental health issues that can manifest in multiple ways from intimate partner violence to substance abuse, chronic post-traumatic stress and, increasing in numbers over the years, suicide. The number of suicides among service members has continued to rise since the Vietnam War and, more recently, the 9/11 attacks. Statistics state "20 service members' lives lost daily to suicide equates to 263,000 lives lost since 1979; that is more casualties than World War II, the Vietnam War, and the Korean War combined."[1] This has raised concern among policymakers, military leaders, and the general population as a whole, resulting in countless attempts by lawmakers to create policies that intend to eliminate suicide completely. Ironically, the non-profit associations like Save A Warrior (SAW), for example, that are *not* connected with the Department of Veterans Affairs (VA), are the groups seeming to make the biggest difference in reversing the statistics. This discussion presents three alternative policies, but will focus mainly on the equity, effectiveness, and efficiency of the policy promulgated by *The Defense Strategy for Suicide Prevention (DSSP) 6490.16*, policy in addition to suggesting alternative options to help guide policymakers in addressing and eliminating the military suicide epidemic.

WAYS THE PROBLEM HAS BEEN ADDRESSED

Veterans Bill of Rights and *PREVENTS Initiative*

There have been a number of policies presented and programs created because of the implementation of *DSSP 6490.16,* including one recent approach presented in March 2019 titled the *Veterans Bill of Rights (VBoR)*, created by a former West Virginia state senator and U.S. Senate candidate, Richard Ojeda (D), who is also an Army veteran.[2]

The state-level political group Future Now assisted Ojeda in the development of this model policy. The *VBoR* "would establish veteran health navigator services to identify federal and other health benefits coverage available for veterans and their families, assisting them with enrolling in coverage, identifying mental health benefits, and directing clients to services for post-traumatic stress disorder, depression, and suicide prevention."[3] The *VBoR* also targets the types and causes of financial instability experienced within the military community, as well as the limited health care options available to members, along with veteran homelessness, which the policy authors and supporting state representatives believe ultimately lead some to choose suicide as a solution.[4]

Another recent approach was the executive order signed by President Trump on March 5, 2019, titled the *PREVENTS Initiative* (*President's Roadmap to Empower Veterans to End the National Tragedy of Suicide*). The policy "establishes a task force of the Secretaries of Veterans Affairs, Defense, Health and Human Services, and Homeland Security...to develop a comprehensive public health roadmap for helping veterans pursue an improved quality of life and ending the national tragedy of veteran suicide."[5]

This strategy does not appear to be as clear at first regarding the specific intentions as the *Veterans Bill of Rights* policy; however, upon further inspection, there are

current programs supporting the *PREVENTS Initiative*, as well as non-profit agencies, research studies, and celebrities, such as Florida Georgia Line (FGL), endorsing the executive order. The band members from FGL have partnered with a monetary funding cooperative called The Independence Fund, and with VA corroboration a program called Operation RESILIENCY is helping combat veterans, their families, and caregivers through mobility programs, adaptive sports, advocacy, and suicide prevention. The Independence Fund and Operation RESILIENCY work with leaders in the House and Senate, VA leadership, and individuals from the public and private sector to create "...a unique reunification retreat for the wounded warriors of the hardest hit units in the Global War on Terror. They regain the camaraderie lost after leaving their unit...the goal is to ensure the unit that experiences the battle together, experiences healing together."[6]

Both strategies previously mentioned address the issues regarding suicide and its long-term effects on soldiers and their family members. The information provided is intended to educate the individuals on suicide awareness, prevention, and postvention; help-seeking behavior through appropriate resources for support; and the mental health treatment options available within the designated community agencies or the corresponding community VA Healthcare System.

EVALUATION OF FOCUSED POLICY

History and Mission

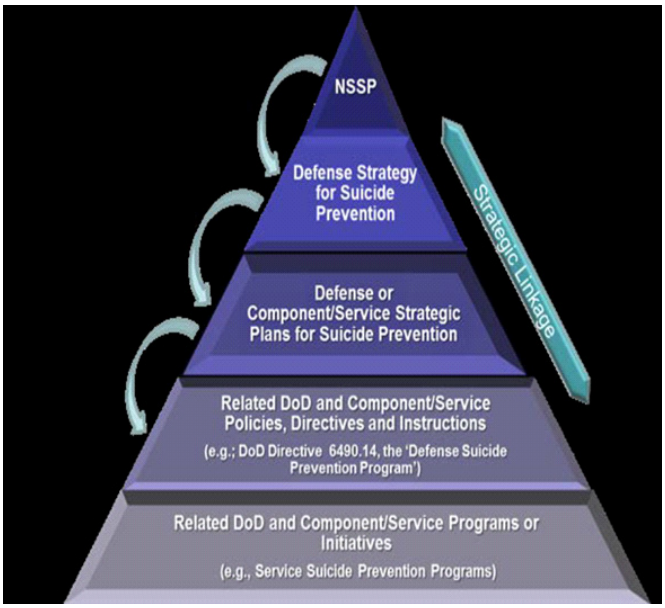
The *Defense Strategy for Suicide Prevention (DSSP) 6490.16* is unique because it was the "first DoD-wide comprehensive policy on suicide prevention determining applicability, standardized definitions and assigned responsibilities within the Department of Defense."[7] It has led the way for all other suicide prevention programs within DoD and the VA, undergoing revisions and updates based on continued research of suicide statistics over the years. The *DSSP* was created using the framework of a previously published reference policy, originally written in 2001, titled *National Strategy for Suicide Prevention.*[8] The *NSSP* was created to help launch the nationwide effort to prevent suicide across the United States and was drafted through a joint effort of the Office of the U.S. Surgeon General and the National Action Alliance for Suicide Prevention. It was revised and updated in 2012, and DoD aligned its version of the *DSSP* to fit those specifications.[9] To better explain what the policy intent is, the following is from the Executive Summary:

> The *DSSP* is tailored to meet the unique needs of the DoD, but is also consistent with the existing Service Suicide Prevention Programs... Underpinning this strategy is the belief that each suicide is preventable; therefore, the strategy will guide Department efforts as it strives to reach the aspirational goal of zero suicides...through education of Military Community Members about suicide risk and related behaviors; promotion of health, resilience and help-seeking behavior; research, development and delivery of effective programs and services; and removal of all barriers to care... It retains the *Four Strategic Directions* of the *NSSP* and their respective underlying goal numbers; however, the terminology in the goals (and their underlying objectives) has been made suitable for DoD. Additionally, the *Themes Shared Across Strategic Directions* have been retained from the *NSSP.*[10] (See Figures 1[8, 10] & 2[10] following the footnotes on this page.)

Equity. While considering the different aspects of the *DSSP* policy in terms of evaluating program fairness, one who is familiar with this specific issue may be struck with a feeling of disconnect. The military culture values strength, courage, resilience, and personal sacrifice.

Figure 1

The Strategic Relationship of the NSSP, DSSP, and other DoD Suicide Prevention Efforts[8]

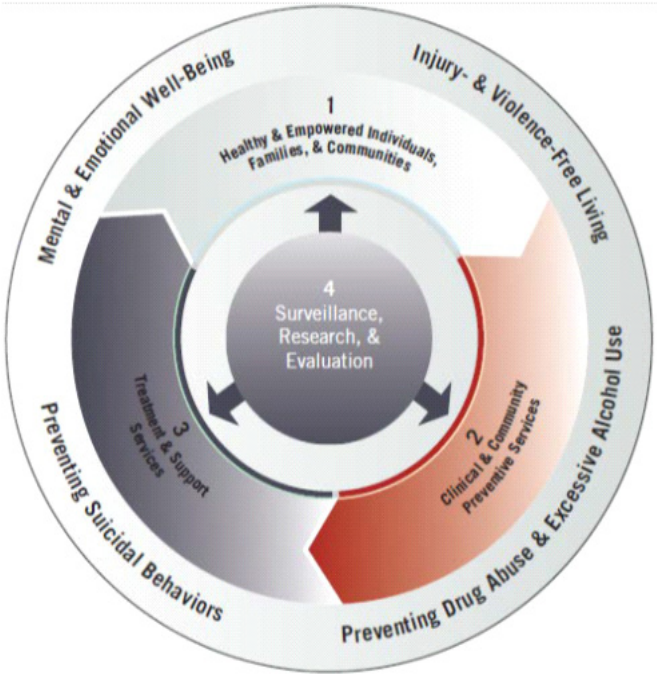


Note. "The *DSSP* is intended to provide strategic linkage from existing DoD and Component suicide prevention

programs to the *NSSP*. Additionally, a strategic plan to initiate and guide the activities of this strategy will be developed for the Department."[10]

Figure 2

The Four Strategic Directions and Themes (Source 2012 NSSP)



Note. The outer edge of the circle lists the *Four Themes Shared Across Strategic Directions*: (1) Mental & Emotional Well-Being; (2) Injury- and Violence-Free Living; (3) Preventing Suicidal Behaviors; and finally (4) Preventing Drug Abuse & Excessive Alcohol Use. The (numbered) *Four Strategic Directions:* (1) Healthy & Empowered Individuals, Families & Communities; (2) Clinical & Community Preventive Services; (3) Treatment & Support Services; and in the center (4) Surveillance, Research & Evaluation. The *DSSP* notes when all of these elements are "working together, they help to prevent suicide."[10]

Weakness is not tolerated and service members are expected to "shake it off" or "suck it up" when experiencing hardship, loss, defeat, or illness. Research has shown that suppression and avoidance are linked to mental health problems and emotional distress, including suicidal ideation and suicide attempts.[11] Despite these facts, suppression and avoidance are taught and reinforced within the military as coping strategies. In the short-term aspect after experiencing a stressful or traumatic event, suppression can actually reduce emotional distress and cultivate adaptation to extreme adversity. This is relevant in combat situations, especially when emotional distress can impede judgment, become a liability, and is not adaptive or conducive to survival. In other words, suppression and avoidance are key elements to blocking emotional reactions in certain military objectives.[12]

Typically, we ask for help when we are struggling, but this help-seeking ability is in direct conflict to what the military is taught during training. Self-sufficiency can be beneficial and productive, but it can also create a void between human interactions. Isolation and avoidance, even if unintentionally mastered for self-perseverance purposes, can be dangerous for individuals at risk of suicidal ideation. In fact, the military has specific manuals that list possible situations in case of missions gone awry, personnel taken hostage, aircraft landing in enemy territory, etc. ...that are focused specifically on teaching individuals physical and psychological survival tactics which employ varying degrees of suppressed emotion and avoidance of feelings.[13]

Effectiveness. The 18- to 24-year-old category of enlisted males (rather than officers), regardless of component, is the demographic which research shows is "most at risk for suicide in the military."[14] Statistics also show "70 percent of veterans do not regularly use the VA or even have access to a federal department that may be viewed as central to suicide prevention."[15] The reasons military members do not use VA services vary greatly from the stereotypical stigma associated with seeking mental health services to fear of losing their security clearance and/or their gun rights if they are diagnosed with a mental health issue. If service members are *not* registered with VA Healthcare Services and therefore *do not use* the programs created to help prevent suicide within the VA, then how are the policies being created for suicide prevention within the VA and the DoD benefitting the target population most at risk for suicide among the military population?

Most people who are unfamiliar with military standards and lifestyle might be fooled into thinking the *DSSP* policy addresses the obvious and immediate concerns of military members who struggle with suicidal ideation. However, these examples are focused on a problem *after the fact*; so why are military command officials not preparing service members *before* thoughts of suicide become a problem? How are the symptoms of depression and post-traumatic stress being addressed before they consume an individual's mental state on a daily basis and become a problem?

Efficiency. The question stands: If the programs the U.S. government is supporting, funding, and implementing are *not* bringing down the incidence of military deaths by suicide, *should* the millions of dollars funneling into those programs (as well as the time and effort spent creating and implementing them) continue? Perhaps enlisting other sources of expertise on the subject within the military is more realistic in attempting to end this epidemic?

If the non-profit groups making the biggest impact in saving soldiers' lives were to share their knowledge of Warrior-led, *volunteered* services with government officials, where would the money come from and whose pockets would be filled? Peer-to-peer organizations like *Save A Warrior (SAW)* that are funded by generous donors have no use for insurance-approved policies, there is nobody designated as a leader in the therapy program punching a time clock, there are no retirement homes to pay off, no kids to send to college, and no astronomically-priced MRI or X-ray machines needed to help those attending the week-long alternative treatment who are desperately seeking a reprieve from the traumatic, long-term effects suffered from post-traumatic stress experiences.

POLICY ALTERNATIVES

Programs like SAW are producing actual results every week when cohorts graduate with a transformed outlook of their life and a renewed sense of peace. Eight years after SAW began in Malibu, CA, with a second location now open in Newark, OH, more than 1,000 lives have been saved after completing the intense 5.5-day holistic program. SAW states in its mission statement that the program is:

> committed to ending the staggering suicide rate plaguing our veterans, active-duty military and first responders. We conceive, originate and invent Integrated Intensive Retreat (IIR) experiences to transform the way our heroes live their lives.[16]

Save A Warrior is unlike any treatment program available to anyone, ever. The simple core values of (1) Belief in a Higher Power, (2) Service to Others, and (3) Daily Meditation/Maintenance seem almost too simple – but that is the point based on the grateful and humble comments made by previous graduates of the Integrated Intensive Retreat program. Eligible warriors participate in an interview-type series of questions in a "rostering" phone call with a former SAW graduate who is either a service member or a first responder (in some cases both) to determine their placement in a future cohort, either in Ohio or California, at one of the two organization locations. Equine-assist therapy, alternative practice techniques from a variety of notable treatment theorists/practitioners and, the most important factor, peer-to-peer communication, leadership, and trust, are just some of the incredible elements of this life-changing program.

CONCLUSION

While intentions and attitudes may be nothing more than good old try hard and solid efforts at the end of the day, the programs created by lawmakers' policies are not working. Perhaps some of the inability to connect the dots may be because the people presenting the policies do not have (a) personal experience with the subject of suicide and/or (b) are not educated or trained in the field focused on biopsychosocial aspects of long-term trauma or suicidal ideation.

Karl Marlantes, a cum laude graduate of Yale University and a Rhodes Scholar at Oxford University, was a 17-year old Marine during the Vietnam War. He has since been awarded the Navy Cross, the Bronze Star, two Navy Commendation Medals for valor, two Purple Hearts, and ten Air Medals. He authored "What It Is Like to Go to War" in 2011, his nonfiction personal account of experiencing the ordeal of combat and the long-term effects of the trauma suffered during the Vietnam War. He examines how military leaders, government officials, medical professionals, and our society might better prepare soldiers for war. In his introduction, he summarizes his viewpoint based on 40-plus years of first-hand experience:

> The violence of combat assaults psyches, confuses ethics and tests souls. This is not only a result of the violence suffered; it is also a result of the violence inflicted. Warriors suffer from wounds to their bodies, to be sure, but because they are involved with killing people, they also suffer from their compromises with, or outright violations of, moral norms of society and religion. These compromises and violations are not generally discussed, and their impact on a warrior's mental health and soul is minimized, or even ignored entirely, not only by current military training, but society at large.[17]

And that is the bottom line – the current policies, like those mentioned in this discussion, are missing the root cause of military deaths by suicide. Before military officials begin training focused on killing and war-type strategies, enlisted recruits need to be advised and trained in courses focused on mental health coping skills as a type of psychological barrier to the effects and consequences of killing another human during conflicts of war. Service members need to know their options for

resources *before* handling combat ordnance. They need reassured confidence from support systems at the micro, mezzo, and macro levels, and they need to be reminded that struggling alone and in silence is not an option. Stigma associated with, but not limited to, diagnoses of mental health issues (like PTSD) and/or seeking treatment can be changed through open channels of communication at all levels in the military chain of command, community-wide education, and marketing messages of hope, understanding, and acceptance through social media platforms that are organized/facilitated by experienced veterans or active duty peers who volunteer in communities throughout the country. Soldiers risk their lives for our freedoms every day. The least our government can do for them is help them continue to live their lives in peace once returning home from the battlefield by finding the solutions needed to stop the suicide epidemic of 22 soldiers' lives lost every day.

NOTES

[1] Jake Clark, *Save a Warrior*: *Home Page Statistics Information* [Website], 2012, www.saveawarrior.org.
[2] Akela Lacy, "Lawmakers From 11 States Have a Plan to Tackle Suicide and Other Issues Veterans Face," *The Intercept* [Online], May 28, 2019, https://theintercept.com/2019/05/28/veterans-bill-of-rights/.
[3] Lacy, *The Intercept*, May 28, 2019, https://theintercept.com/2019/05/28/veterans-bill-of-rights/.
[4] Lacy, *The Intercept*, May 28, 2019, https://theintercept.com/2019/05/28/veterans-bill-of-rights/.
[5] "President Donald J. Trump Issues a National Call to Action to Empower Veterans and End the National Tragedy of Veteran Suicide," *Whitehouse.gov* [Online Fact Sheet], March 5, 2019, https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-issues-national-call-to-action-to-empower-veterans-end-national-tragedy-veteran-suicide/
[6] "PREVENTS Initiative: Executive Order to Combat Veteran Suicide – The Independence Fund," Independence Fund [Online], 2017, https://www.independencefund.org./prevents/.
[7] Defense Suicide Prevention Office, *Defense Strategy for Suicide Prevention (DSSP)*, U.S. Department of Defense (DoD) [Online], 2015, https://www.dspo.mil/PORTALS/113/Documents/TAB%20B%20-%20DSSP_FINAL%20USD%20PR%20SIGNED.PDF.
[8] Office of the Surgeon General (U.S.) and Center for Mental Health Services (U.S.), *National Strategy for Suicide Prevention: Goals and Objectives for Action: A Report of the US Surgeon General and of the National Action Alliance for Suicide Prevention*, U.S. Public Health Service, Rockville, MD [Online], 2012, https://www.ncbi.nlm.nih.gov/books/WBK44268.
[9] Office of the Surgeon General (U.S.) and Center for Mental Health Services (U.S.), *National Strategy for Suicide Prevention...*, 2012, https://www.ncbi.nlm.nih.gov/books/WBK44268.
[10] Defense Suicide Prevention Office, *Defense Strategy for Suicide Prevention (DSSP)*, U.S. Department of Defense (DoD) [Online], 2015, https://www.dspo.mil/PORTALS/113/Documents/TAB%20B%20-%20DSSP_FINAL%20USD%20PR%20SIGNED.PDF.
[11] Dean Mobbs et al., "The Ecology of Human Fear: Survival Optimization and the Nervous System," *Frontiers in Neuroscience*, Vol. 9, 2015.
[12] Mobbs et al., 2015.
[13] U.S. Department of the Army, *US Army Survival Manual*, FM 21-76 [Online], 2016, https://archive.org/details/FM2176USARMYSURVIVALMANUAL/page/n5/mode/2up.
[14] Jennifer Steinhauer, "VA Officials, and the Nation, Battle an Unrelenting Tide of Veteran Suicides," *The New York Times* [Online], April 14, 2019, https://nyti.ms/2DbEZgk.
[15] Steinhauer, "VA Officials, and the Nation...," April 14, 2019, https://nyti.ms/2DbEZgk.
[16] Jake Clark, *Save A Warrior*: *Home Page Statistics Information* [Website], 2012, www.saveawarrior.org.
[17] Karl Marlantes, "What It Is Like to Go to War," translated by Bronson Pinchot, Grove/Atlantic, Inc., and Blackstone Audio, Inc. [Audio], 2011.

Megan Connell-Cox is a 40-year-old non-traditional student working toward a BS degree in Social Work at The Ohio State University. She graduated with honors from Central Ohio Technical College in August 2019 with an associate's degree in Human Services. She is a disabled Operation ENDURING FREEDOM veteran and a member of Phi Theta Kappa, as well as the former chapter secretary. She is a certified Chemical Dependency Counseling Assistant (CDCA II). She is an active member of the Associates of Vietnam Veterans of America, local Chapter 55, and Post 85 of the American Legion. Megan is passionate about advocating on behalf of service members who struggle with PTSD, TBI, suicidal ideation, depression, and substance use disorder. She imagines her future consisting of lobbying at the state and federal levels for changes needed in targeting the root cause of the military suicide epidemic.

An Intelligence Community Leader: General Vernon Walters

by MSgt (USAF) Zachary S. McNair

The present always benefits from knowledge of the past. Leaders, known and unknown, small and large, impact the multitude, frequently going unnoticed by the greater public. Vernon Anthony Walters is a legend in some circles and perhaps virtually unknown in most others. This work serves to highlight three challenges upon which he made influential changes, thereby impacting monumental events as a leader serving his country. Let us begin with a brief overview of our subject.

Lieutenant General Vernon A. Walters served the nation for half a century in various capacities, rising from the Army's enlisted ranks to Deputy Director of the Central Intelligence Agency (CIA), and from Presidential interpreter to Presidential ambassador and envoy.[1] He had an early start on his meteoric rise. As a by-product of attending numerous schools in Europe, Walters developed a linguistic ability enabling him to speak a phenomenal four languages by the age of ten and later learned no fewer than eight languages during his lifetime. This unique skill, according to Walters, was paramount in his being called to serve presidents directly and in his rise to global statesman.[2] Through his lifetime of work, among many other roles, he found himself interpreting, leading international discussions of critical importance, navigating the Watergate incident, and representing American values and interests worldwide.[3] What follows is a brief selection of his leadership moments, an examination of leadership traits displayed, and implications for leaders of today.

In the first instance, then-Lieutenant Walters is summoned by the Pentagon in 1943 to interpret for a delegation of Portuguese officers. Portugal had yet to choose a side in the war and sent a delegation to tour the United States in order to decide whether or not to back the U.S. in spite of Germany. While the Portuguese valued and supported American interests, they were concerned about German repercussions and retaliation. The tour's objective was to bring the Portuguese to the American side by showing the delegation our military industrial machine, our capability, and our firm intent going into the war. Essentially, it was to show proof that we intended to, and could in fact, win. Walters was to show them many key facilities during the two-month tour but there was one problem. He did not speak Portuguese, only Spanish and French. However, he was a quick study in the language, accomplished this specialty work for the Pentagon, and did it well enough to receive both letters of appreciation from the Portuguese and a rapid promotion to Captain.[4] What leadership qualities can be gleaned from this fascinating experience? To answer that question, one must first ascertain which characteristics of Walters brought about his selection for the job.

Walters was selected for three key reasons. First, he demonstrated flexible linguistic expertise. Second, there is evidence in the story of his likability and referent power, which aided in building rapport with the delegation and earning its appreciation later on.[5] This type of extraversion is considered to be a trait critical for effective leadership.[6] Finally, although he reluctantly accepted the assignment on orders and was of lower rank than the members of the senior delegation, he demonstrated his emergent leadership, characterized by those who can combine both success and affiliation orientations to motivate others.[7] What lessons might a leader today take from this situation?

A leader today might study how Walters took on his role with the Portuguese in spite of not knowing the language, won over the delegation, and succeeded in his mission. The result enabled the U.S. to use Portugal's Azores Islands in its anti-German submarine efforts.[8] Walters' personal efforts in overcoming a lack of knowledge by leveraging the skills he did have led to strategic gains. Although we like to envision ourselves as always strong, trained, ready, and equipped, a strategic leader today will routinely face challenges in which deficiency in one or more of those areas may exist. Instead of an impasse, one might view the perceived inadequacy as an opportunity, either for self-improvement or as a chance to earn rapport with those around him as he or she positively navigates and overcomes the uncertainty. Next is an example of battlefield courage and diplomacy.

In this instance, Second Lieutenant Walters would make such an impact on the Allies' landing in East Africa that he received a battlefield promotion to First Lieutenant. On the eve of battle while traveling in a convoy of ships across the Atlantic, he wrote the following: "To this moment I have felt no weakness, no regrets, only pride. Standing on the deck at night, looking out over the black immensity that hides both friend and foe,

God seems near and eternity close. I am calm, serene and ready."[9] This was to be his first experience in combat and his steadfast mentality carried him through two harrowing ordeals. Upon arrival, he and his five men boarded the landing craft and were deployed to seize the shore. The fighting had begun before Walters landed and the shelling and small arms fire continued all around him as his team came ashore. His job as an intelligence officer during this time was to interrogate French prisoners. To accomplish this task while under continued threat of being wounded, he set up a small workspace in a warehouse, provided intelligence to the nearby 2nd Armored Division Commander, Major General Ernest Harmon, and did so for nearly 55 hours without sleep or food.[10]

After resting, his next major task was to locate a French Colonel Signard who controlled the area Walters' landing party had just captured. Signard's soldiers were responsible for the continued, though diminished, small arms fire. As the Allies were there to fight the Germans, not the French, General Harmon ordered Walters to find this colonel at his post and persuade him to order his unit to stand down, allowing the Allies to press farther inland. Additionally, so as to appear diplomatic, this journey required Walters to ride unarmed and exposed to potential sniper fire while traveling into enemy territory. With much consternation, he did as he was told. He traversed an explosives-laden bridge and convinced two armed guards to allow him to reach his destination. Upon arrival at the post, his final act was to persuade the senior officer. Doing so was not easy as Colonel Signard was under orders specifically to stop the Allied advance. However, as Walters knew, the colonel was under German orders and, as the Germans were rolling through France, Walters, through a brief but powerful exchange in French, leveraged this French nationalistic atrocity to convince Signard to relent and allow undeterred passage by the Allies. The impassioned convincing worked, so well in fact that, at Walters' request, Signard even accompanied him back to the Allied garrison where he met General Harmon, who was delighted. He exclaimed, "Walters, I'll make you a first lieutenant for this."[11] Later that day, that is exactly what he did. What characteristics of leadership did Walters display?

Though under orders, Walters not only satisfied the objectives given to him but did so with finesse and aplomb. Despite this being his first combat experience, he summoned the courage to act, organize his team, and conduct his intelligence mission under the dual pressures of being just yards away from an intelligence-hungry general and while under enemy fire. Walters' leadership quality, ability, and character were tested and his accomplishment typifies leadership during crisis.[12] Later, his diplomatic approach to dealing with Colonel Signard is apparent. He could have attempted coercive power or pleaded with the colonel.[13] Instead, he pitted his command of the French language and knowledge of the war's impact against Signard's orders and identified within Signard the possibility of negotiation based on his demeanor. Walters was respectful and persuasive while leveraging his knowledge in the negotiation. Walters swayed Signard's thinking of "just following orders" to that of nationalistic loyalty. He initially drew out how Signard felt about the French being overrun by the Germans and then continued the persuasion by insisting that each American and French life spent now was one less that could join the celebration upon victory over Germany.[14] This concept, framed as *Egosystem versus Ecosystem Motivation*, focuses on the end result and how both the leader and follower can mutually benefit once the objective is met. It is critical in this motivational concept not to focus on the individual behavior, in this case following orders, but instead on the intended consequences.[15] This is exactly what Walters accomplished to great effect. What lessons could a leader today take from these challenging situations?

Though circumstances change, negotiation is a timeless leadership skill. Further, there will likely never be a time when one should hold critical negotiations without considering the influential environmental factors. Indeed, to have a solid footing, the leaders should know both the other's motivations as well as the environment in which he or she resides. Understanding these considerations is essential to forming and articulating a mutually beneficial outcome. This knowledge predicates a persuasive argument as to why the opposing side should relinquish something for mutual benefit. Next is an example in which Walters perhaps saved the CIA as we know it.

This final example was perhaps Walters' most impactful. As President Nixon's Watergate scandal was unfolding, then-Lieutenant General Walters was pressed by the Nixon administration to provide cover for the individuals who committed the Watergate Hotel break-in.[16] However, based on his conviction that the CIA was essential to the continuation of the United States as a free democracy, Walters flatly refused. Accepting this proposed action would have placed responsibility for the incident with the Agency and, after internal discussions, it was determined that the Agency in fact had no involvement. When pressed, Walters refused again, saying it could destroy the Agency's credibility and that, if forced to carry out the request, he would resign in such a way as to make it known publicly what was being attempted. Finally, the representative relented and Walters was not pressed again.[17] Let us examine the traits of leadership present in this decision.

The primary form of leadership displayed by Walters in managing this crisis was authentic leadership.[18] Walters understood the long-term consequences of a misstep; his strong morals and professional ethics were reflected in his decision. He also deeply understood his purpose, was passionate about the CIA mission, and felt free to lead based on his values. The fact that President Nixon and Walters had been personal friends for years prior to this event lends further proof of the latter's leadership traits.[19] Walters was unrelenting

and unapologetic in his dedication to the organization he was leading and would rather have sacrificed his career than to have led the CIA down a dark path and tarnish its reputation. What might a leader today glean from how Walters averted this potential catastrophe?

These lessons translate well for those making tough decisions having the potential to cost his or her career or the organization's reputation. Walters could have approached this problem using a number of easier methods. He could have relented, notified the press, or brought in senior CIA members to help him decide. A modern leader must be able to read the environment, take the pressures of a decision, make a call, speak truth to power, and assume responsibility with an organization's best outcomes in mind. Critically, authentic leadership enables the leader's sense of purpose to guide him or her.[20] Walters' purpose was to protect his organization. There is little doubt of the appreciation which must have been felt later by Agency employees as they came to realize how this man was willing to sacrifice his position in defense of the honor of each and every one of them and the organization which they served.

In conclusion, General Vernon Walters left an indelible mark on many people whom he encountered, as his mastery of languages, politics, negotiation, and interpersonal relations made him difficult to forget. For present-day leaders, there is much to learn from him, at least for those willing to dedicate themselves to the pursuit of the requisite knowledge, fortitude, and passion. This article serves to highlight three of Walters' challenges which demonstrated his leadership ability and served to show how the characteristics that made him successful translate well to the challenges faced by leaders today.

[Editor's Note: This article is adapted from MSgt McNair's MSSI thesis, and I serve as chair of his thesis committee. Shortly arriving to NIU in 2019, the author indicated intense interest in Vernon Walters and a desire to dig through the personal papers and artifacts of Walters left by the general to then-JMIC before his death in 2002 at the age of 85. Unfortunately, the COVID-19 crisis has resulted in students being shut out of the NIU facility beginning in mid-March 2020, having to take the remainder of their coursework online and forcing many of them to revise their research strategy due to availability and classification of records. Despite Walters' full archives being unavailable, the author has been able to access many other primary sources related to the general's career, some of them via the State Department with the expert assistance of his thesis committee reader, a fairly recent NIU graduate himself, a Naval Reserve officer, and an employee at State. This article looks at just a small portion of Vernon Walters' stellar, and unique, career while the author's complete thesis will be a series of leadership case studies spanning several phases of the general's professional life.]

NOTES

[1] Henry R Appelbaum, "Vernon Walters – Renaissance Man," Central Intelligence Agency, accessed September 26, 2019, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol46no1/article01.html.
[2] "Modern Presidents," C-SPAN, uploaded March 14, 1998, https://www.c-span.org/video/?100520-1/modern-presidents.
[3] Appelbaum, "Vernon Walters – Renaissance Man."
[4] Vernon Anthony Walters, *Silent Missions* (New York: Doubleday, 1978), 60-69.
[5] B.H. Raven, "A power/interaction model of interpersonal influence: French and Raven thirty years later," *Journal of Social Behavior & Personality*, no. 7 (1992): 217-244.
[6] Peter Guy Northouse, *Leadership: Theory and Practice* (Thousand Oaks, CA: SAGE, 2016), 27.
[7] Richard M. Sorrentino and Nigel Field, "Emergent leadership over time: The functional value of positive motivation," *Journal of Personality and Social Psychology* 50, no. 6 (1986): 1091-1099, http://dx.doi.org/10.1037/0022-3514.50.6.1091.
[8] Walters, 69.
[9] Ibid., 28.
[10] Walters, 35-44.
[11] Walters, 46-49.
[12] Allan Schoenberg, "Do Crisis Plans Matter? A New Perspective on Leading During a Crisis," *Public Relations Quarterly* 50, no. 1 (Spring 2005): 2.
[13] Northouse, 12.
[14] Walters, 48.
[15] Nitin Nohria and Rakesh Khurana, *Handbook of Leadership Theory and Practice: A Harvard Business School Centennial Colloquium* (Boston, MA: Harvard Business School Publishing, 2010), 398-399.
[16] Appelbaum, "Vernon Walters – Renaissance Man."
[17] *Vernon A. Walters: Pathfinder of the Intelligence Profession*, June 3, 2004, Conference Proceedings, Joint Military Intelligence College (JMIC), Washington, DC, 45-46.
[18] Northouse, 196-197.
[19] Benjamin B. Fischer, "Panel on LTG Walters' Central Intelligence Years," in *Vernon A. Walters: Pathfinder of the Intelligence Profession*, June 3, 2004, Conference Proceedings, Joint Military Intelligence College (JMIC), Washington, DC, 61.
[20] Northouse, 197.

Master Sergeant (USAF) Zachary S. McNair is an Air Force imagery analyst and presently a student at the National Intelligence University (NIU) in Bethesda, MD, where he is pursuing a Master of Science of Strategic Intelligence degree with a Leadership and Management concentration. Enlisting in August 2001, he initially served seven years as a weapons load crew member and deployed in support of Operations SOUTHERN WATCH and IRAQI FREEDOM. He has served overseas tours in Japan, Italy, and South Korea. He holds a BS degree in Interdisciplinary Studies from Park University and AAS degrees in Aircraft Armament Systems, Intelligence Analysis, and Instructor in Technology from the Community College of the Air Force. He speaks some Italian, enjoys SCUBA diving, and researches avenues of financial investment in his free time. Following graduation from NIU, Zach anticipates an assignment to the 480th Intelligence, Surveillance, and Reconnaissance Wing at Joint Base Langley-Eustis, VA.

The Transformational Leadership Approach of CIA Director John Brennan

by M. John Bustria

Former Director of the Central Intelligence Agency (CIA) John Brennan (March 2013-January 2016) left a legacy of integrating disparate divisions with fixed habits. He instituted new ways of doing business, ensuring the long-term survival of the CIA by changing the culture and promoting creativity. This article argues Brennan is a transformational leader who changed CIA's organizational culture through his understanding of ingrained cultures, as well as the changing environment, and his alignment of CIA's culture with a new vision and a revision of its norms.

Before October 2014, "stove-piping" was prevalent in the CIA. The relationships among the four directorates (Operations, Analysis, Science &Technology, and Support) were uneven. Such uneven relationships included irregular consultation with stakeholders and limited linkages, with each directorate innovating on its own. The functions of each directorate and its divisions were separate and distinct from each other. Once in a while, some officials from one side were able to work with the other side on critical issues. They relied on ad hoc work and personal networks. This work arrangement demonstrated a semblance of quasi-cooperation. Yet, the scope and frequency of communications were still limited. Incremental changes to processes had enabled the directorates to answer amply, but myopically, some taskings from policymakers.

Aside from this internal challenge, the changing global environment and its uncertainties have served as critical contextual factors that influenced the leadership thinking of Brennan. The mission of the CIA has broadened, including tracking a broad array of cross-cutting global challenges and issues. The threats and opportunities facing the nation have been changing and becoming more complex, with U.S. adversaries becoming more diverse and capable, and technological developments challenging expertise and tradecraft.

This array of cross-cutting global challenges and issues has expanded CIA's mission. Brennan testified before Congress in June 2016 that "if we are to meet the national security challenges that confront us, we must constantly adapt and innovate."[1] Under his leadership, senior leaders reviewed existing processes and established new ones. They grappled with organizational development through an effort called "modernization." His leadership executive team created a matrix that integrated the Agency's four directorates.[2] Part of Brennan's vision saw modernization leading to a culture of integration among the different directorates.

Part of Brennan's vision saw modernization leading to a culture of integration among the different directorates.

Brennan faced an organization with ingrained culture and complex external challenges. To challenge the status quo, he adopted two forms of leadership. His decisions reflected both the transformational and transactional leadership categories in overcoming this culture. Under transformational leadership, he changed "the basic values, beliefs, and attitudes of followers,"[3] allowing him to move forward the goals of his vision in the initial stage of change. Nevertheless, Brennan used transactional leadership, coupled with trust, to ensure his effort would succeed.

For example, a panel group recommended in December 2014 that Brennan start with a "pilot project" to implement a "Mission-Center" approach, but they did not want to toss out the current organizational chart.[4] He then used transactional leadership for compliance on quick implementation. He rejected the advice to go slow, overruled the study group, and decided to implement a new structure wholesale. He noted: "I know this place well. I know the culture very well... If we continued to do things the old way, we would not be successful."[5] These instances show Brennan viewed his role both as a transactional and transformational leader.

Warner Burke and George Litwin have developed a model of organizational change. Their model makes a distinction between transactional and transformational leadership

styles. Transformational leaders are "leaders who inspire followers to transcend their own self-interest for the good of the organization and who are capable of having a profound and extraordinary effect on their followers."[6] On the other hand, transactional leaders are "leaders who guide or motivate their followers in the direction of established goals by clarifying role and task requirements."[7] Burke and Litwin added that transactional leadership is sufficient for causing first-order change, but transformational leadership is required for producing second-order change.[8]

The authors note that in first-order change some features of the organization change but the fundamental nature of the organization remains the same. Aside from the transactional aspect, first-order change goes by other labels: evolutionary, adaptive, incremental, or continuous change.[9] In second-order change, the nature of the organization is fundamentally and substantially altered—the organization is transformed. Aside from the transformational aspect, second-order change is labeled transformational, revolutionary, radical, or discontinuous change.[10]

Brennan understood that transformational leadership increased the motivation of the CIA staff more than transactional leadership. Nonetheless, he used a combination of both to overcome the Agency's deep-rooted culture and influence and gain the trust of his followers.

These definitions explain which type of leadership Brennan had employed for modernization: "Organizational Development interventions directed toward structure, management practices, and systems (policies and procedures) result in first-order change [transactional change]; interventions directed toward mission and strategy, leadership, and organizational culture results in second-order change [transformational change]."[11] The structural change through Mission Centers results in first-order change or transactional change. However, normative change directed toward the organizational culture results in transformational change. A case in point is diversity in the CIA workforce, which allows the Agency to meet challenges in the external environment through different "attitudes, backgrounds, ethnicities, and perspectives."[12] In other words, transactional and transformational leadership "are not mutually exclusive, nor is transformational leadership a panacea for all of a leader's problems."[13] Brennan understood that transformational leadership increased the motivation of the CIA staff more than transactional leadership. Nonetheless, he used a combination of both to overcome the Agency's deep-rooted culture and influence and gain the trust of his followers.

Despite this caveat, Brennan is generally a transformational leader. What makes him such is that he developed and communicated a vision.[14] He said he envisioned a CIA version of the Goldwater-Nichols Pentagon reform that created joint combatant commands which melded the armed services. Similar integration had already worked in the CIA's Counterterrorism and Counterproliferation Centers; Brennan wanted more.[15] He realized the need for significant improvement and developed a vision based on the needed changes. He commented: "I don't want the CIA to be the Kodak of the future."[16] Based on Edgar Schein's definition of organizational culture,[17] Brennan was thus a transformational leader who remained steadfast in implementing change to develop, as part of his vision, new ways for the Agency workforce to think and act to cope with environmental challenges. He saw modernization as a flexible method against CIA's entrenched culture.

Brennan's transformational leadership approach to implementing change also involved employing Gary Yukl's two most important strategic leadership functions: monitoring the environment and formulating a competitive strategy.[18] Brennan scanned the environment by asking the panel of nine senior officers in September 2014 to conduct a 90-day study of reorganization.[19] The panel members identified information and used multiple sources by talking to 80 senior officials, polling 4,000 CIA employees, and conducting 15 focus groups.[20] Brennan and his executive team then formulated a mix of creative strategies. They chartered ten Mission Centers (six regional and four functional), kept the old directorates, and created a Directorate of Digital Innovation to adapt to a world in which technology has transformed espionage.[21]

Brennan's vision has changed the old ways and introduced new norms. Modernization has increased the face-to-face engagements among directorate officers and fostered better teamwork among analysts and operators. This outcome has resulted in more robust finished intelligence, as indicated by policymakers who expressed that they are benefitting from more integrated briefings and support. This result has come about because modernization has provided an avenue wherein Mission Center officers can communicate more and collaborate further with each other as a cohesive team. Additionally, praises from customers indicate modernization is adding value to CIA's finished products. In a way, Brennan was a radical leader who took a risk with his vision to allow the right information to get into the right places at the right time.[22]

Throughout, Brennan used motivation to move his vision into reality. He continued emphasizing the direction of CIA and the benefit that modernization would bring to the Agency. Nevertheless, his motivation had a persistence dimension, which allowed the staff to maintain their effort[23] during the various phases of modernization. He and his team positively reinforced the behavior with acknowledgment of a joint effort among officers to achieve a mission. Aside from this, they motivated the staff using intrinsic rewards.[24] They changed, among other things, the promotion criteria and personal growth opportunities. These rewards ensured that personnel would likely repeat the positively reinforced behavior on how to think and act like an intelligence officer in a Mission Center.

Director Brennan's transformational leadership approach to leading others seems to have come from the leadership definition of Peter Northouse, who defines leadership as "a process whereby an individual influences a group of individuals to achieve a common goal."[25] Brennan's process was not just a linear event but it also included interaction with his panel members, other stakeholders, and followers. He affected the workforce through influence, which derived from his leadership position, policy experience, and previous role as operations staff member and analyst. He also directed his energy toward the stakeholders who were working to achieve a mutual purpose. He influenced them to accomplish the common goal of overcoming the environmental challenges facing CIA.

Brennan's approach to influencing the CIA's organizational culture elicited different reactions from the staff regarding his attempts to bring about change by senior influence. Four possible outcomes occurred during the effort: resistance, compliance, identification, and internalization.[26] Many complied when they received constant communication from Brennan and senior leaders. Others identified and internalized modernization, indicating they were committed to the change effort because they saw the wisdom of Brennan's "influence attempts."[27] As for those who resisted, he and his team continued to engage them. They solicited ideas from the staff and noted the importance of their ideas, a process that indicates innovation is the engine of change.

In short, the tendency to restructure an IC agency, such as the modernization of the CIA through the integration of various directorates into Mission Centers to cope with the changing security landscapes, is complex and fraught with difficulties and challenges. Through Brennan's leadership, the new processes brought about by the structural and normative changes have enabled the staff to adapt and work together in addressing complex, external challenges.

Transformational leaders who motivate their followers to perform and identify with new organizational goals can drive higher levels of performance. When they motivate their staff to perform based on goals, the latter feel engaged and rewarded. As a result, they give extra effort, leading to better organizational performance. The leader, team members, and board members benefit together from the output of the product, service, or report.

The tendency to restructure an IC agency, such as the modernization of the CIA through the integration of various directorates into Mission Centers to cope with the changing security landscapes, is complex and fraught with difficulties and challenges.

Leaders also must see through the various stages of change—beginning, transition, and final—to ensure execution, control, and closure. They must continuously communicate during the beginning and transition period. They should encourage their management team to update their employees often on the status of ongoing initiatives. In so doing, the staff will become more informed about the change, the reason behind the change, and how the change will benefit the mission. As a result, most of the personnel will become motivated to accept change because they will know it. This will make them realize more readily that change is necessary.

During the transition period, leaders must overcome fear on the part of the workforce not only through constant communication but also by implementing new processes that allow officers to learn new procedures as well as new behaviors and ways of thinking. The education and support provided to the employees should be part of the planning and execution processes. Throughout the process, however, leaders must remind their team members of the rationale for the change, including the benefit once the organization implements the change initiative.

During the implementation stage, the leader also should emphasize not only the structural change but the normative as well. In the case of modernization, this change is about more than lines and boxes on CIA's organizational chart. Brennan noted that his change effort "is also a mindset—a commitment to innovate constantly so we can keep up with a changing world."[28] A key part of this mindset is making the CIA workforce as diverse as the world the Agency covers. Hence, leaders should recruit people with diverse backgrounds for innovation and creativity.

Toward the final stage of organizational change, leaders must reinforce and solidify the changes to the systems, policies, processes, structures, goals, etc. They must institutionalize the changes to make them accepted as the new norm. In this way, the employees do not return to their previous ways of thinking and other set ways before the change. Leaders also should model the way in cementing the new processes and behaviors into their organizational culture. The new processes and policies will then become an acceptable way of thinking and behaving.

Consequently, leaders must use their skills to change some of the essential organizational elements. As such, a new mission amid challenges in the internal and external environments means changes in the following: strategy, organizational culture, performance system, structures, systems, and management practices—reflecting a mix of transformational and transactional changes. Leaders should also balance these changes by incrementally updating existing policies and adapting or continuing existing policies that officers have deemed effective. These are necessary for leaders to implement change effectively—introducing revolutionary changes while acknowledging and giving importance to the outputs and creativity of followers.

When leaders task their followers regarding new policy directions, they can succeed in implementing the policies using incremental and radical changes in key elements. They can opt for changes that are transformational and transactional—coupled with the use of the right balance of trust, influence, and motivation—to ensure a successful desired state, just like what Brennan did at the CIA with his transformational leadership style to implement his vision.

NOTES

[1] Statement by Central Intelligence Agency Director John O. Brennan before the Senate Select Committee on Intelligence, June 16, 2016, https://www.cia.gov/news-information/speeches-testimony/2016-speeches-testimony/statement-by-director-brennan-as-prepared-for-delivery-before-ssci.html, accessed March 27, 2020.
[2] David Ignatius, "Will John Brennan's CIA modernization survive Trump?" *The Washington Post*, January 17, 2017, https://www.washingtonpost.com/opinions/will-john-brennans-controversial-cia-modernization-survive-trump/2017/01/17/54e6cc1c-dcd5-11e6-ad42-f3375f271c9c_story.html, accessed March 27, 2020.
[3] Patrick F. Walsh, "Making Future Leaders in the US Intelligence Community: Challenges and Opportunities," *Intelligence and National Security* 32, no. 2 (2016), 4.
[4] Ignatius, "Will John Brennan's CIA modernization survive Trump?"
[5] Ignatius, "Will John Brennan's CIA modernization survive Trump?"
[6] Wendell L. French and Cecil H. Bell, Jr., *Organization Development: Behavioral Interventions for Organization Improvement*, 6th ed. (Upper Saddle River, NJ: Prentice Hall, 1999), 77.
[7] French and Bell, *Organization Development*, 77.
[8] French and Bell, *Organization Development*, 77.
[9] French and Bell, *Organization Development*, 76.
[10] French and Bell, *Organization Development*, 76.
[11] French and Bell, *Organization Development*, 77.
[12] Statement by CIA Director before the SSCI, June 16, 2016.
[13] Kevin Donohue and Leonard Wong, "Understanding and Applying Transformational Leadership," *Military Review* (Army University Press, August 1994), 30.
[14] Donohue and Wong, 28.
[15] Ignatius, "Will John Brennan's CIA modernization survive Trump?"
[16] Ignatius, "Will John Brennan's CIA modernization survive Trump?" Brennan was referring to Eastman-Kodak, "an organization so captivated by its past that it was too slow in changing along with its environment." In Josh Kerbel, "The U.S. Intelligence Community's Kodak Moment," *National Interest*, February 16, 2016.
[17] Edgar Schein, *Organizational Culture and Leadership*, 3rd ed. (San Francisco, CA: Jossey Bass, 2004), 17.
[18] Gary Yukl, *Leadership in Organization*, 7th ed. (Upper Saddle River, NJ: Prentice Hall, 2010), 394.
[19] Ignatius, "Will John Brennan's CIA modernization survive Trump?"
[20] Ignatius, "Will John Brennan's CIA modernization survive Trump?
[21] Ignatius, "Will John Brennan's CIA modernization survive Trump?"
[22] Amy Zegart, *Spying Blind: The CIA, the FBI and the Origins of 9/11* (Princeton, NJ: Princeton University Press, 2007), 2.
[23] Stephen Robbins and Timothy Judge, *Essentials of Organizational Behaviors*, Global ed. (Pearson Canada, 2018), 130.
[24] Robbins and Judge, *Essentials of Organizational Behaviors*, 100.
[25] Peter G. Northouse, *Leadership: Theory and Practice*, 7th ed. (Sage Publications Inc., 2016), 6.
[26] Donohue and Wong, "Understanding and Applying Transformational Leadership," 25.
[27] Donohue and Wong, "Understanding and Applying Transformational Leadership," 26.
[28] Statement by CIA Director Brennan before the SSCI, June 26, 2016.

M. John Bustria has worked for nearly ten years in various capacities as an analyst covering geographic and functional accounts for the U.S. government. Before his federal service, he was a research fellow, policy analyst, and temporary adjunct in Michigan. Previously, he was a diplomat, career executive service officer, academic, and researcher in the Philippines. A few of his key leadership positions in the past include being co-chair, workforce council; analytic project lead; office representative, management advisory group; project management lead; Charge d'Affaires, a.i.; division chief; policy desk officer; acting director; executive assistant; committee chair, academic department; vice president, community association; and club president. John earned a Master of Science of Strategic Intelligence degree from the National Intelligence University in 2020.

Counterintelligence Assessment of Jeffrey M. Carney, U.S. Air Force

by Lee E. Taylor II

INTRODUCTION

Jeffrey M. Carney is no household name, but this former U.S. Air Force linguist proved to be one of the most damaging defectors ever for the Department of Defense (DoD). By Cold War's end, Carney would plead guilty to charges of espionage, conspiracy, and desertion, securing a prison sentence of 38 years.[1] Prior to his apprehension in 1991, Carney exploited his position as an intelligence specialist to spy for the East German Ministry for State Security, ultimately compromising over one hundred classified military documents. This is a truly underappreciated case study, one this counterintelligence assessment explores in an effort to better understand key components of Carney's motivations, his handling under the East German intelligence service, and factors that led to his discovery and capture. This assessment is largely supported by information from Carney's self-published book. Understandably, such work should be read with some skepticism and, where possible, attached to corroborating information—however, a mandatory pre-release review by DoD left many redactions, suggesting there may be a substantial amount of truth to the literature.

BACKGROUND

Jeff Carney first approached his U.S. Air Force (USAF) recruiter at the age of 16 with no high school diploma or GED, no parental consent, and a history of experimental drug use. All mitigating factors would be outweighed by the needs of DoD at the time, given heightened tensions during the Cold War era. Carney had studied German throughout his high school career, demonstrating an aptitude for foreign languages. This would make him an attractive candidate for a position in linguistics intelligence, one of the USAF's critically-manned career fields. Seeking an outlet to escape a troubled life at home, Carney worked with the local recruitment office—an office eager to fill a critical billet—to secure an enlistment date as soon as possible. Here he started to demonstrate another quality: susceptibility to coercion and manipulation. In his book, Carney describes how recruiters coached his answers concerning drug use and parental consent, in one case constructing a plan for an out-of-state relative to endorse his under-age enlistment.[2] Carney did not protest, granting the recruitment officials guiding influence over him throughout the process. Despite this, his military career looked rather promising at the outset. By the spring of 1981, now 17 years of age, Carney had graduated from USAF basic training with distinction and a TS/SBI clearance.[3] Set to attend the Defense Language Institute, Carney would spend 32 weeks perfecting his German language skills, again graduating with honors and an award for "achievement in understanding a foreign culture."[4]

Carney's skillset as a German linguist would be employed in West Berlin, with his assignment to the 6912th Electronic Security Group. This unit directly supported the National Security Agency's (NSA) Berlin-Marienfelde site, considered one of the U.S.'s most important eavesdropping installations and one of the Cold War's most closely guarded secrets.[5] As a signals intelligence (SIGINT) post, primary responsibilities included electronic espionage: to intercept, translate, and convey enemy radio and telephone conversations. This form of technical intelligence collection also includes monitoring clandestinely planted audio devices, commonly known as "bugging." Carney's first experience in this realm was in direct support of President Reagan's Berlin visit in June 1982, listening for potential threats and operational compromises.[6] To enhance mission effectiveness, operators are read into sensitive operations to help discern potentially valuable intelligence from white noise. In this case, Carney had detailed knowledge of Reagan's itinerary and logistics. This operational role in Berlin granted Carney unfettered access to some of the U.S.'s most sensitive involvements.

Berlin itself was the frontline for espionage during this era, commonly referred to as "Spy City." The division of East and West Berlin following World War II became a tangible representation of Churchill's "Iron Curtain" expression. Western democratic powers could not lose their foothold here, fully committed to combating and

containing the communist Eastern Bloc countries under Soviet influence. The construction of the Berlin Wall in 1961, however, significantly complicated intelligence-gathering efforts for both sides. The United States, as the technologically dominant superpower, focused operations heavily on technical intelligence (TECHINT) collection, "as its strength in spying always lay in technical spying, not in human spying."[7] This underscores the U.S. Intelligence Community's demand for and reliance on positions such as Carney's. Located on the other side of the Wall was the East German intelligence service, the Ministry for State Security (Stasi, or MfS). With strong ties to the USSR's KGB, the Stasi maintained a consistently aggressive human intelligence (HUMINT) collection program, earning itself a reputation for being one of the Cold War's most effective intelligence agencies.[8]

MOTIVATION: MICE/R

Money, ideology, coercion, and ego—abbreviated as MICE—these are the primary factors compelling individuals to commit espionage and betray their governments. Hank Crumpton, a well-respected former CIA case officer, argues there is a subcomponent of "ego" so prevalent in espionage it deserves its own categorization: revenge.[9] This was a significant driving force behind Carney's ultimate decision to betray his listening post and the U.S. government. A cursory Google search of this case study reveals that Carney became disgruntled with the Air Force, but referencing his aforementioned book is required for further detail. His first expression of frustration follows shortly after his arrival at the Berlin station. Forced to participate in upgrade and on-the-job training (essentially a complete recap of technical training), Carney felt his new routine was both "monotonous and a waste of time," leading to a decided lack of motivation.[10] Carney also expressed extreme discontent for the USAF rating and promotion system, complaining that annual performance reports do not accurately represent the quality of an airman's work, but rather his/her likability within the unit. Carney received less-than-perfect marks on his first report, resulting in an unprofessional argument with his supervisor and subsequent reprimand for conduct.[11] Additionally, Carney's lack of motivation blossomed into complacency and carelessness. He would be reprimanded several more times for this; however, the specific incidents described throughout Carney's book are meticulously redacted.[12]

Ultimately, Carney would fail his upgrade training exam and carry feelings of resentment with him: "I have always been a person who carries a grudge, and it is a weakness I freely admit."[13] Carney fell to sensations of alienation and loneliness, something he blamed explicitly on the USAF. On several occasions he expressed to his superiors a desire to quit, threatening to revoke his own clearance, but he feared substantial retribution for doing so. His command recommended him to the Mental Health Office for stress counseling, but Carney found this to be an unproductive outlet for his issues. Instead, he further isolated himself, channeling his anger toward U.S. defense policy and affairs, heavily criticizing President Reagan. No longer maintaining faith in his own government, Carney viewed the White House's Strategic Defense Initiative as "arrogant brinkmanship."[14]

Following a night of heavy drinking to subdue his overwhelming feelings of depression and disillusionment, Carney made his way to Berlin's Friedrichstrasse crossing with the intention of defecting to East Germany. Having traveled to East Germany several times prior and growing a small attachment, he made the conscious decision to announce his defection to the German Democratic Republic's (GDR) gate guard in April 1983, the official time that Carney's espionage began, as recognized by the PERSEREC reports.[15] Noticing Carney's military ID, the guard dispatched a notice to an officer from the HVA, the Stasi's foreign intelligence branch. Carney was introduced to the case officer who would soon become his handler, Ralph Dieter Lehman. Lehman interviewed and assessed Carney, immediately identifying the key traits already recognized throughout this assessment: strong potential to be manipulated, disapproval of U.S. foreign policy, expressions of resentment, and a desire to "fit in." Carney explained his only desire was to defect immediately and begin living in the GDR; however, Lehman continued his interview, inquiring about Carney's access to information. "I get to read reports from all over the world: Nicaragua, Cuba, North Korea…"[16] Lehman cross-referenced Carney's answers throughout the interview, conducting his own counterintelligence assessment. Lehman surmised the airman was not a false defector and pitched him on the spot, suggesting that life in the GDR was earned, and Carney would prove his worth by reintegrating himself into West Berlin, acting as a penetrating agent ("mole") on behalf of the Stasi. Carney accepted, donning his new code-name "Kid." While Carney would be paid by his Stasi handlers for services rendered, he noted this was never the primary motivation. Lehman recognized this, too, occasionally reassuring Carney throughout the handling process that he was "making the right choice" in seeking revenge against the U.S. government.[17] Carney also began to realize and accept his own homosexuality during this time. While this fact remained unknown to the Stasi (to his knowledge), Carney describes a traumatizing event that included a close friend being searched and arrested by the Air Force Office of Special Investigations (AFOSI) under suspicion of being homosexual. This further solidified his anger and resolve to commit espionage.

STASI TECHNIQUES AND AGENT HANDLING

The quick recruitment of Carney certainly posed a counterintelligence threat to the Stasi, but this is indicative of its risk-accepting, aggressive nature as an intelligence organization. This is, in part, what made it so successful as a HUMINT-gathering service within Berlin. "Carney passed on approximately 65 pieces of information to the Stasi between 1983 and 1986. . . [H]is material received high marks—24 received the highest rating [of] 1."[18] Lehman left instructions with Carney at the conclusion of their very first meeting, dictating how they would connect in the future and pass information. Because inter-city travel was not completely restricted for personnel, just mildly regulated, Carney's case officer arranged for their meetings to take place in East Berlin. The Stasi had a cadre of supporting assets in place to assure Carney's travel would not be impeded or easily monitored by Western services. This is how he made it back into West Berlin after his attempted defection, as one of Lehman's insiders escorted Carney through the "Diplomats" lane for crossing, avoiding a passport stamp—these supporting assets would continue ensuring Carney's safe passage. Information was primarily passed between the two parties via face-to-face encounters, facilitated by more supporting assets that provided safe houses—risky dead-drop operations could be avoided for the most part, although Carney does recall at least one instance in which he was asked to do so in West Berlin for particularly sensitive documents.[19] Carney provided his handlers with "information about his unit's listening activities in the [GDR], activities against Soviet and East German targets, and orders from the NSA to its Berlin stations."[20]

Carney was able to access and deliver sensitive information with relative ease, given major holes in his unit's information security (INFOSEC) process. Sensitive and classified information was not well compartmentalized, allowing Carney to locate and extract myriad information he determined might qualify as "of value" to his handlers. Additionally, Carney had been formally trained as an augmentee for security personnel, due to a manning deficit. This means Carney (among many of the airmen) had detailed knowledge of entry control monitoring, security logistics, and—most importantly—personal search and pat-down procedures.[21] This is a practice that still occurs within the Air Force today.[22] It is a major factor that led to the successful smuggling of documents past security officers, knowing exactly where and how to conceal items while avoiding suspicion.

The Stasi appreciated the value of long-term gains in its intelligence practices and the handling of Carney, where other services might have been more inclined to seek quick returns on their investment. In one example, Lehman suggests to Carney he should pursue Officer Training School to become of even greater use to the GDR, offering to support Carney financially through his bachelor's degree.[23] In fact, Carney had spent merely six months in Berlin after meeting Lehman on his first attempt to defect. In 1984 he was relocated to Goodfellow AFB, Texas, to instruct the technical training courses for new operators. At a training site, Carney believed he would no longer be of use to Lehman and his handlers. Rather, the Stasi practiced patience and maintained him as an agent-in-place. As an instructor, Carney provided East Germany with educational training plans, allowing Stasi analysts to determine that "American intelligence was listening to the SED's (East German Communist Party) conversations, monitoring GDR air traffic, and conducting electronic warfare."[24] Carney's handlers arranged for meetings in Mexico City and Rio de Janeiro, although they did little to establish a suitable cover for his travel. Carney felt exposed, assuming all of the risk by arranging and managing logistics for visits to Mexico and Brazil. This was a major breaking point for Carney. Feeling solely responsible for his own safety and security, Carney devised a plan to defect once and for all to East Germany via the GDR's embassy in Mexico City in 1985.

APPREHENSION

Jeffrey Carney successfully defected back to East Berlin, where he lived until his arrest in 1991, shortly after the fall of the Berlin Wall. Carney's decision to flee is directly tied to an overwhelming sensation of paranoia and fear that AFOSI agents would arrest him at any moment. At the time, American media outlets were portraying the "Year of the Spy" due to an unprecedented proliferation in arrests for espionage. Witnessing the capture of many high-profile traitors deeply rattled Carney. However, it is not clear whether AFOSI had the slightest inkling of Carney's actions prior to his run for the embassy in Mexico. Only when co-workers recognized Carney's absence did OSI begin attempting to track his movements. This effort came with a great degree of difficulty, as Carney recalls from his post-arrest debrief that "OSI was confronted with a rapidly vanishing trail… [T]he initial lack of serious criminal suspicions on the part of OSI had indirectly given me breathing space."[25] OSI's only true break in its manhunt came following the unexpected publication of Stasi records after the GDR's collapse, allowing foreign investigators to identify and prove Carney's actions definitively.

Air Force OSI would have been the primary authority responsible for initially discovering Carney's espionage, tracking him down after defection, and arresting him. Established in 1948, its mission is to provide "a full suite of investigative (criminal and fraud) and counterintelligence (CI) support to the Air Force."[26] AFOSI's counterintelligence

mission includes both offensive and defensive techniques, including classic CI (catching espionage agents) and CI support to force, asset, and infrastructure protection.[27] However, OSI counterintelligence efforts actually did little to thwart or later find Carney. Without the help of two former Stasi intelligence officers turned informants, AFOSI had very little trail to follow otherwise. Carney would discover during his trial that Hans-Joachim Lehmann and Gerd Lips provided crucial information used to identify Carney as a Stasi agent.[28] Lehmann (not to be confused with Carney's handler, despite the name similarities) had served as a Stasi intelligence officer, as Lips was Carney's former psychological evaluator and psychiatrist. Both men had informed for other U.S. intelligence services, and that information was later passed along to AFOSI. While this particular penetration of Stasi intelligence itself did not explicitly identify Carney as the agent, it did prompt AFOSI to widen its investigation and consider the defector as a suspect for espionage. AFOSI's practices during this era were mediocre, failing to identify and assess proactively the damage Carney was doing, even after many operational compromises. Recognizing past mistakes and CI deficiencies, Air Force OSI now does considerably more to debrief airmen regularly and deliver CI awareness briefings. This includes tailored briefings for "high risk units" with access to information and programs that could do grave damage to national security, a direct result of the massive amount of spying that occurred in the 1980s.[29]

Jeffrey Carney's journey as a spy and subsequent defector cost the U.S. government approximately $14.5 billion in damages.[30] This case is unique, and it surely deserves greater attention. His betrayal proves that money is not the only motivator for committing espionage. In fact, since 1990 only 7 percent of individuals involved in espionage against the U.S. spied solely for monetary gain.[31] The case also reinforces Crumpton's assertion that revenge demands more attention as a motivating factor. This assessment also identified significant organizational factors that made the East German Ministry for State Security such a successful intelligence service. A risk-acceptant, aggressive approach to HUMINT collection allowed the Stasi to uncover and thwart numerous U.S. operations. Finally, poor U.S. Air Force INFOSEC and CI practices—referring to both of Carney's units and the AFOSI—allowed the airman to provide his Stasi handlers with sensitive information for over five years. While this assessment skims only the surface of an underappreciated case study, much still remains to be learned from the actions of Jeffrey Carney.

NOTES

[1] PERSEREC Report, "Espionage & Other Compromises of National Security – Case Summaries: 1975 to 2008," U.S. DoD, November 2009, https://fas.org/irp/eprint/esp-summ.pdf.
[2] Jeffrey Carney, *Against All Enemies: An American's Cold War Journey* (Middletown, DE: CreateSpace Independent Publisher, 2013), 48-50.
[3] Ibid., 55.
[4] Ibid., 69.
[5] Kristie Macrakis, *Seduced by Secrets: Inside the Stasi's Spy-Tech World* (Cambridge, UK: Cambridge University Press, 2008), 96.
[6] Carney, *Against All Enemies*, 102-103.
[7] Macrakis, *Seduced by Secrets*, 97.
[8] "Overview of Intelligence and Law-Enforcement Agencies," Crypto Museum, https://www.cryptomuseum.com/intel/.
[9] Henry Crumpton, *The Art of Intelligence: Lessons from a Life in the CIA's Clandestine Service* (New York: Penguin Books, 2013), 35.
[10] Carney, *Against All Enemies*, 100-104.
[11] Ibid., 104-105.
[12] Ibid., 122-123.
[13] Ibid.
[14] Carney, *Against All Enemies*, 133.
[15] PERSEREC Report, "Espionage & Other Compromises," U.S. DoD, November 2009.
[16] Carney, *Against All Enemies, 154.*
[17] Carney, *Against All Enemies*, 185-191.
[18] Macrakis, *Seduced by Secrets*, 98.
[19] Carney, *Against All Enemies*, 214-215.
[20] Macrakis, *Seduced by Secrets*, 98.
[21] Carney, *Against All Enemies,* 92.
[22] Author's personal experience on active duty with the USAF.
[23] Carney, *Against All Enemies*, 259-260.
[24] Macrakis, *Seduced by Secrets*, 98.
[25] Carney, *Against All Enemies*, 449.
[26] William Arnold (Col, USAF, Ret), "The AFOSI Counterintelligence Mission: Past, Present, and the Future," *American Intelligence Journal*, Vol. 20, Nos. 1 & 2 (2000-2001), 7.
[27] Ibid.
[28] Carney, *Against All Enemies*, 588-589.
[29] Arnold, "The AFOSI Counterintelligence Mission," 13.
[30] Alison Gee, "Jeff Carney: The Lonely U.S. Airman Turned Stasi Spy," BBC, September 2013, https://www.bbc.com/news/magazine-23978501.
[31] PERSEREC Report, "Espionage & Compromises of National Security," U.S. DoD, November 2009.

Lee Taylor II is an MA candidate attending Georgetown University's School of Foreign Service. As a student in the Security Studies Program, he focuses his coursework on intelligence studies with an emphasis on counterintelligence cases. Prior to attending Georgetown, he earned a BA degree in International Studies from Hawai'i Pacific University. Lee served as an enlisted member of the U.S. Air Force from 2010 to 2018, directly supporting U.S. combatant commanders and government leaders across 23 countries while assigned to Hawaii's Special Air Missions.

NMIF Bookshelf

AROUND THE CORNER: REFLECTIONS ON AMERICAN WARS, VIOLENCE, TERRORISM, AND HOPE.

John William Davis.
Huntsville, AL, Red Bike Publishing. 2018.
237 pages.

Reviewed by MSgt (USAF) C. William Strong, an intelligence analyst for the U.S. Air Force Special Operations Command who earned a Bachelor of Science in Intelligence degree from National Intelligence University in 2019 and is currently pursuing an MS degree in Systems Engineering from Johns Hopkins University.

[Editor's Note: Will Strong epitomizes the sort of young NCO who reflects the bright future of military intelligence. Even though I never had him as a core or elective course student, other than for mandatory writing sessions that all the Air Force students at NIU were subjected to by their senior service advisor, he regularly stayed in contact with me and showed an intellectual interest in writing about intelligence that is rare in someone of his grade and experience. He attended the NMIF Awards Banquet in 2019, cheering on others from his service who were honored, and has been very supportive of the Foundation and this *Journal*.]

Retired U.S. Army counterintelligence officer and linguist John W. Davis has written his follow-up to *Rainy Street Stories*, providing further reflections on his career and other anecdotes, through a distinctly *noir* lens. Davis indicates this is intended to be the second in a trilogy of memoirs and states that the title came from a professional and personal life spent "going around the corner…into the unknown."

The author provides 66 short narratives within *Around the Corner*, many of which stem from his professional experiences working in Europe during and following the Cold War. Others derive from his childhood, were recounted to him by others, or are about individuals who influenced him, but all were either formative or help the author reinforce the themes of the book. As Davis states, many of these vignettes are stranger than fiction, and the collected book is an altogether captivating recounting of this important historical period.

Each story in *Around the Corner* has a lesson to impart, akin to a fable by Aesop. One of the longer essays, "Once and Future Principles of War," provides the author with the opportunity to display his familiarity with historical military strategy. Davis cites Clausewitz and Sun Tzu as predictors of successful strategy during the Napoleonic Wars, and compares the failed German World War II Operation BARBAROSSA with Napoleon's pursuit of Kutuzov into the Moscow winter. Davis hints that much of our modern military strategy is based on attrition and technological superiority, and stresses that a return to traditional military strategy would foster greater modern military success. He insists, "We have a bounty of precedents to learn from, which are applicable to all combat on the battlefield, and off."

The central theme of *Around the Corner* is autobiographical reflection with a great deal of focus on military implications. As such, there are few sections that deal directly with intelligence. "Counterintelligence: Seeing Through the Enemy's Eyes" is the most intelligence-centric portion of the book. In it, Davis recounts the World War II military surprise of the lack of a French military reserve and the implications that it had for French and British forces following the May 1940 German circumvention of the Maginot Line. The author asserts that a lack of British red teaming led to the surprise and states that U.S. counterintelligence analysts should first evaluate U.S. capabilities prior to those of the adversary.

It is evident in reading *Around the Corner* that the author's motivation is to impart his and others' life experiences on the reader. Davis is an obvious student of history, as much of the book is spent communicating historical lessons woven in with ones from his own life. He seamlessly connects these anecdotes with one another and the greater themes of the book in order to inform the reader while appearing to be searching for some greater retrospective meaning for himself.

There are drawbacks to the author's narrative style in *Around the Corner*. He makes a many references to other authors, military strategists, philosophers, and historians; hence, some may assume these references are made to imbue the author's perspective with greater credibility. It is also entirely possible that, in doing so, and through the decidedly academic style of writing that is employed throughout the text, Davis may unwittingly alienate the alleged target audience of younger decision-makers by writing a book that would appeal more to his own age and experiential bracket. Those issues aside, if you are a student of military history and are well-read, you will likely find *Around the Corner* to be as relatable as I did.

Davis' personal and professional experience is evident throughout *Around the Corner*, as is his deep appreciation for military history. He makes sure to draw multiple parallels in each story to demonstrate how his life was informed by historical precedents while hinting that the reader should prepare for the same over the course of his/her life. Davis clearly takes pride in his experiences and very much cares about the future of U.S. national security. This quality draws the reader in and makes him/her want to read the next story. The reader will not be disappointed in doing so.

• •

THE WOMAN WHO SMASHED CODES: A TRUE STORY OF LOVE, SPIES, AND THE UNLIKELY HEROINE WHO OUTWITTED AMERICA'S ENEMIES.

Jason Fagone.
New York, Harper Collins Publishing. 2017.
464 pages.

Reviewed by Avery G. Agostinelli, an undergraduate student and research assistant in the Art History Department, Auburn University.

As females within American society become increasingly appreciated, many historians look to the past to prove that women have consistently played a critical part in our nation's success, especially during times of great turmoil due to political narrow-mindedness, precarious international relations, and economic difficulties. A refreshing surge of attention to these remarkable individuals has sparked special interest in recovering evidence of their contributions to organizations such as the National Aeronautics and Space Administration (NASA), the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA), overturning the long-held belief that the success of these institutions' development in the 20th century was due solely to the effort of men.

In Jason Fagone's *The Woman Who Smashed Codes,* William and Elizebeth Friedman are credited with significantly advancing the United States' cryptanalytic capabilities that eventually led to the Allies' ultimate success in World War II. Throughout their vibrant careers as masterful breakers of code, William was continually credited with both his own achievements and those of his wife, essentially erasing Elizebeth's accomplishments from history. Fagone compensates for such a travesty in this biographical work by showcasing Elizebeth Friedman's key role in advancing codebreaking techniques, arguing that, without her selfless and lifelong contributions, the outcome of the Second World War might have unfolded in the Axis' favor.

To establish Elizebeth's cryptanalytic skill firmly and prove her codebreaking genius incontrovertibly, Fagone traces the honing of her abilities to her humble beginnings working as a research assistant, thoroughly following the development of her career up to her appointment as a lead cryptologist in Washington, DC. By colorfully characterizing both heroes and villains involved in Elizebeth's journey, Fagone allows his readers to gain an understanding of her personal outlook and struggles, making this nonfiction read like a gripping novel as opposed to a monotonous history textbook. In order to contextualize further this individual's extraordinary achievements, the author includes clear explanations of basic codebreaking techniques, giving the reader insight into the complex and unique obstacles Elizebeth overcame.

The Woman Who Smashed Codes covers a broad period of time in our nation's history, including a comprehensive historical analysis of the industrialization of northern America in the 1910s to the second wave of feminism in the 1970s. While primarily an account of an American woman's professional development in the United States, Fagone strategically incorporates relevant information regarding international politics and foreign relations to offer the reader a valuable historical context. For example, a portion of this work discusses Germany's codebreaking stations in South America, a lesser known dynamic that complicated international relations in World War II, revealing the unique circumstances and motivations felt by Ms. Friedman during her career. Because *The Woman Who Smashed Codes* is a biographical work, the author drew upon primary sources, among which are letters exchanged by the Friedmans, works they published, and diaries of their friends and colleagues. Fagone dedicates almost 80 pages to recording meticulously every source from which he pulled each piece of information, evidencing the complete accuracy of this unlikely tale.

For an investigative reporter, Jason Fagone's writing is both entertaining and accurate, rendering *The Woman Who Smashed Codes* a gripping novel as well as an informative history. He has published many pieces in prestigious news sources such as *The San Francisco Chronicle*, *The Huffington Post*, and *The New York Times*. He specializes in writing investigative works revealing lesser-known aspects of both current and past American habits, events, and individuals. He primarily writes articles, but has also published several books in addition to *The Woman Who Smashed Codes.* Though Fagone does not specialize in cryptanalysis himself, he possesses an apparent understanding of codebreaking techniques, allowing him insight into Ms. Friedman's exciting and exceptional career.

Within this work, the author seeks to expose the long-neglected and underappreciated contribution of Elizebeth Friedman to the U.S. Intelligence Community and its codebreaking methods. In conjunction with this educational goal, Fagone also delivers a relatable, inspirational tale of a successful woman who

overcame the cultural limitations of the robber-baron society in early 20th century America along with the institutional obstacles posed by male-dominated governmental organizations. Fagone is successful in both endeavors as he provides both an enlightening history and an entertaining story wrapped together in one book. He considers dozens of diverse sources in his collection of events, individuals, and consequences of Elizebeth's extraordinary career, leading readers to trust in the accuracy of his assertions and conclusions.

Because *The Woman Who Smashed Codes* reveals the monumental influence that a fundamentally unacknowledged individual had on the technical advances and national success of the U.S. in World War II, readers are compelled to consider the possibility and additional unknown figures who achieved similarly significant contributions but are left unnamed. Readers are especially encouraged to appreciate the likelihood that there are countless women worthy of celebration, recognition, and gratitude for their contributions to the well-being of the country, though left anonymous due to the societal limitations imposed by widely accepted cultural norms.

After reading Fagone's book, one can be hopeful that other women's intellectual influences upon our culture will be explored and properly credited, creating a more accurate history of America. Fagone's overwhelming number of sources used in writing this book evidences the existence of records that can prove the involvement of underappreciated figures in the success of the U.S. who are currently unrecognized by historians. Therefore, one can look forward to further proof of women's contribution to American culture that will challenge the male-dominated canon of our history.

A reader will view this work as an interruption to the watered-down version of American history systematically presented in the classroom as an all-inclusive chronicling of the past. One's knowledge of intelligence history and codebreaking methods will be increased by this informative work. It will also be an advantage to those seeking a more in-depth understanding of America's cryptanalytic development and help them more fully understand the technical details and international motivations that led to our nation's current codebreaking practices. Most importantly, *The Woman Who Smashed Codes* helps readers realize potential for the growth and success of intelligence and cryptography due to the increasing numbers of women entering this professional field.

[Editor's Note: This book was previously discussed in *AIJ* in a review essay by NIU's Dr. Jennifer A. Davis, which compared and contrasted it with a related book published in 2017 by Liza Mundy, *Code Girls: The Untold Story of the American Women Code Breakers of World War II.* See Vol. 36, No. 1, 2019. However, the present review goes into much more detail on Fagone's book.]

• •

MINDHUNTER: INSIDE THE FBI'S ELITE SERIAL CRIME UNIT.

John Douglas and Mark Olshaker.
New York, Gallery Books. 1995.
409 pages.

Reviewed by Laurelyn Ostrowidzki, an undergraduate student majoring in Chemistry and minoring in Political Science, Auburn University.

[Editor's Note: Obviously, this is not a new, or even recent, book. Nevertheless, I approved this student reviewing it for *AIJ* because the subject is timely given all the political controversy surrounding the Bureau in the last few years. This book is used fairly often in college programs and therefore merits a fresh look. Moreover, the popular TV series "Criminal Minds" just completed a successful run, and it was built around a quasi-fictional Behavioral Analysis Unit operating out of Quantico, VA, also the home of the FBI Academy and an NIU academic center at which I taught part-time students for three years, some of them FBI agents and analysts. Two newer TV series about the FBI are still on the airwaves and turning out to be nearly as popular. All touch on criminal profiling to one degree or another.]

Known as the "FBI's Modern Sherlock Holmes," John Douglas has a diverse background and a long list of credentials. From applying psychological techniques to intimidate the opposing football team to making judgments about the identity of a serial killer, Douglas has used every opportunity in his life to develop and validate the method now known as behavioral analysis. In *Mindhunter,* John Douglas regales the cases he studied that led to the conception and ultimate success of criminal profiling and the unit known now as the Behavioral Analysis Unit of the Federal Bureau of Investigation (FBI). Delving into the minds of some of the most notorious criminals of his time, Douglas walks readers through the interviews and cases that led him to determine there is something deep within the psyche of criminals that compels them to do things a certain way (p. 62). This conclusion is what birthed the art of profiling and shaped the future of crime prevention.

John E. Douglas was born in New York and spent four years in the U.S. Air Force in the late 1960s. He went to Eastern New Mexico University to earn a BS degree in sociology/physical education/recreation. He received his master's degree in education, psychology/guidance, and counseling and an EdS degree in administration and supervision/adult education from the University of Wisconsin-Milwaukee. His PhD from Nova Southeastern University pertained to comparing techniques for teaching police officers how to classify homicides. Douglas is the author of multiple other non-fiction crime books including *Journey into Darkness*

(1997) and *The Anatomy of Motive* (1999). In the FBI, Douglas served as a sniper, an expert marksman on the M16, a SWAT team member, and later a hostage negotiator. He worked in the Behavioral Science Unit starting in 1977 and taught hostage negotiation and criminal profiling at Quantico and across the nation. Douglas created and managed the FBI's Criminal Profiling Program and was later promoted to unit chief of the Investigative Support Unit. Mark Olshaker frequently collaborates with Douglas in writing books about criminal and investigative psychology. In 1995 they formed Mindhunters, Inc. and later released this book, which was made into the Netflix series "Mindhunter" in 2017.

While Douglas' personal life experiences lend a timeline to *Mindhunter* so that it functions loosely as an autobiography, there are three more pertinent approaches Douglas implements: comparative, behavioral, and functional natures. Throughout the book, Douglas refers quite often to the former more limited approach to crime solving, prosecution, and interrogation techniques. He juxtaposes that former approach with one he helped develop. Following the death of the legendary first director of the FBI, J. Edgar Hoover, the Bureau shifted its focus from reacting to serial and violent crimes to preventing these crimes. This crime prevention approach utilized so-called "soft sciences"—as Hoover dubbed them—such as psychology. Foremost among those pushing for this change was Douglas and the developing Investigative Support Unit. He compares the previously accepted concepts like *modus operandi*, which is dynamic, meaning it is subject to change based on circumstances, to concepts he coined, such as the term *signature,* which is used to describe the unique compulsions of criminals that remain static throughout multiple crimes due to the perpetrator's need to fulfill him/herself (p. 268). In addition to these new ideas being used in theory, their acknowledged success led to their utility in court, both to prosecute criminals and to obtain search warrants (p. 262). Historically, this was unheard of, and these advancements were a huge step toward the validation of profiling. Using this comparative approach, the book capitalizes on the benefits of behavioral analysis.

Mindhunter, in its essence, is a compilation of ideas gained from interviews with infamous criminals including Charles Manson and Ted Bundy, plus gruesome cases such as the Unabomber and the Atlanta child murders. Essentially, because of the nature of his research, Douglas used the behavioral approach not only to develop profiling, but also to write *Mindhunter*. The statistics Douglas accumulates from the interviews, and from every crime scene and serial killer he tracks down, all lend to the behavioral approach analyzing patterns of behavior to develop reliable conclusions. As he walks through the areas of focus and analyzes the ways criminals are different, Douglas develops the key to his life's research, which he refers to as "a new weapon in the interpretation of certain types of violent crimes" (p. 14). The art of profiling lends predictability to serial crimes, and it is because there are now reliable ways to interpret ingrained characteristics of an "UNSUB" that previously unsolvable cases, such as Jack the Ripper, can essentially be solved by the book. This is the huge step in crime prevention that helped shape the future of interrogations, prosecution, attainment of search warrants, and answering the question, "why?"

Regarding the functionality of profiling enumerated in the book, Douglas comments comparatively little on the particulars of the process. Often, he merely states his conclusions with only brief hints to the indicators that led to the inferences. However, it is noted that profiling is an intricate skill honed by year after year spent encountering and studying the actions and minds of criminals both on a personal and objective level. It should also be stated that, considering the nature of the book, the intended audience, and the scope of a single investigation, it is likely necessary to curtail some quantity of details in the detective process as well as the investigations. Despite these matters, the authors manage quite well to strike a balance between outlining the functionality aspects of the process while at the same time setting a charged pace that is maintained throughout the book.

As previously mentioned, the book is basically a compilation of cases through which Douglas walks the readers. Obviously well-informed, his writing style is down to earth and blunt. He offers his opinions of the people around him at times but is mainly focused on providing a concise review of the cases he worked. There is nothing frivolous about the writing style, and it can make the reader feel as though he/she is reading on a need to know basis only. However, for the area of inquiry, this is an effective writing style. Because of the nature of the book, the limitations are quite clear. There will be some cases that go unsolved; there will be others that are solved. Even in those cases which are solved there can be some question as to the veracity of the conclusions. As a book written in first person addressing cases for which the details are not always readily accessible to the public, the perspective of the reader is directly linked to Douglas' meaning that his conclusions are almost invariably those of the reader. However, with a topic such as this, it is good to make the reader privy to Douglas' thought process and conclusions because it offers the best opportunity for the reader to get the most realistic feel for the situations.

The purpose of *Mindhunter* seems to be centered around the idea of giving the average citizen an inside look into the development and functions of criminal profiling. With the detailed cases, outlined interviews, and play-by-play crime solving, the book fulfills its purpose and even might exceed

expectations. Though the cases can sometimes be gruesome, violence is never detailed unnecessarily or gratuitously. The gory details of the crime scenes especially offer opportunities to observe links to the profile's conclusions. The personal touch Douglas includes of some life details and personal opinions adds ethos to the book and further separates it from the fictional renditions of this topic. As for evidence, the fact that the book itself is just a compilation of statistical analyses of criminals, Douglas' interpretations of their behavior, and their ultimate capture lends a vast amount of authority to the conclusiveness of the concepts. However, there could have been more attention afforded to the process of profiling. It would certainly be impossible to outline profiling techniques strictly within the limitations of one book, but deeper insight into the process might prove more impactful. That said, the book expressly proves its thesis regarding the effectiveness of the profiling with examples again and again of it working to apprehend the serial criminals of the 20th century.

This book will pique the reader's interest in profiling techniques and might even influence younger readers to expand career options. *Mindhunter* does a wonderful job revealing the reality of criminality in practice, placing due emphasis on the fact that anyone can be a victim. It will induce a desire to become more aware of the surrounding world and could provide critical knowledge to help jumpstart a career in law enforcement, if one decides on such a pursuit. *Mindhunter* by John Douglas, assisted by Mark Olshaker, introduces a vital perspective to anyone who is interested in becoming better equipped for life in a world in which crime is as certain as death and taxes.

• •

THE CULTURAL ROOTS OF STRATEGIC INTELLIGENCE.

Gino LaPaglia.
London, UK, Lexington Books, an imprint of Rowman and Littlefield Publishing. 2020.
264 pages.

Reviewed by Daniel P. Rich, a 2020 graduate of National Intelligence University who earned an MSSI degree and currently an analyst for the Department of Defense. He holds a bachelor's degree in Architecture and a master's in Geographic Design from Thomas Jefferson University in Philadelphia. Prior to government service, he was a defense contractor for a large firm supporting a DoD geospatial program.

Have you ever wondered, "What is strategic intelligence?" More importantly, have you ever wondered where strategic intelligence comes from? Author Gino LaPaglia attempts to answer the latter in his book *The Cultural Roots of Strategic Intelligence* by examining the foundation and evolution of strategic intelligence within various world cultures throughout history (p. xi). Traditionally, when most of us hear the term "strategic intelligence" we think of the "Western," Cold War concept that emerges immediately after the Second World War (p. 1). However, LaPaglia does an incredible job of spinning this concept on its head by suggesting that world cultures throughout history have employed their own versions of strategic intelligence. This includes the Greeks, Romans, Judeo-Christians, Muslims, and Chinese, as well as various entities during the Medieval Renaissance, for the purposes of this book.

By drawing on past empirical evidence, LaPaglia demonstrates that strategic intelligence is a human-based concept that keeps us alive and thriving despite the overwhelming odds, inconsistencies, unfairness, and general randomness (depending on what one believes) that exist in our physical reality. Consistently LaPaglia uses the transliterative device "WWXD," or what "What Would 'X' Do?" in order to illustrate what each deity, person, or even fictional cartoon character must do in order to get by, survive, and succeed (pp. 24, 42, 73, 77, 110, 145). Furthermore, what of those who do persevere, overcome, and succeed? They are inevitably left with this thought, "Strategic Intelligence refuses to be boxed in: it always insists on hope…" (p. 121). And that's the moral of the story!

One might ask, however, "Who is this book actually for?" since the title seems to be inherently misleading about what the reader thought he/she was going to read regarding strategic intelligence. LaPaglia wrote his book for three audiences: "current and future practitioners of strategy in the public (national security) and private (business and competitive intelligence) sectors, academic theorists of strategy, and for the general public…" (p. xiii). Depending on which category one falls into/identifies with, it dramatically changes how one will relate to the book. For example, in the opinion of the reviewer, LaPaglia uses a certain type of prose that is suited to academics, historians, and learners of world cultures but is not conducive to the general layperson. While this prose is beneficial for those specific audiences, general readers will probably have a tough time understanding the examples LaPaglia draws out regarding strategic intelligence and how those concepts are rooted in each world culture's history (see below, Chapter 4 comment). However, the author surprises the reader with unusual yet insightful one-off references from 21st century pop culture which are cleverly rooted in a chapter's overall discussion of a particular world culture.

Here is just one example: Chapter 2 – Greco Roman Strategic Intelligence: "The problem of the contingent can be treated genealogically when we understand that it has been articulated under different but related and comparable metaphors in the culturally foundational stories of Eurasia, often in terms of journey, exile, aging, the vicissitudes of

fortuna, regime transition, seasonal change, astrological wandering, and death… I refer to the Looney Tunes characters upon which generations of Americans have been raised: Bugs Bunny and the hunter Elmer Fudd, Wile E. Coyote and Road Runner, Tweety and Sylvester, or Hanna and Barbera characters Tom and Jerry… The message? Get smart or get eaten, smashed, or shot…" (p. 26). These references dramatically help and keep the discussion relevant for those of us who have not spent our lives studying Greek, Roman, Judeo-Christian, Muslim, Chinese, or Medieval culture, history, or social constructs.

I enjoyed reading LaPaglia's *The Cultural Roots of Strategic Intelligence* if for nothing else than to marvel at the fact that all world cultures have some sort of strategic intelligence underpinning their existence, which is something I had not previously considered or was even aware of, and I would readily recommend this book to others. I especially enjoyed reading Chapter 4 – The Legacy of Judeo-Christian Strategic Intelligence, due to my extensive understanding of that particular culture and its application of intelligence throughout history. However, I had a difficult time understanding some of the finer points in both Chapter 2 – Greco-Roman Strategic Intelligence and Chapter 7 – The Endowment of Chinese Strategic Intelligence, due to my lack of knowledge of the subject matter. Readers who have immersed themselves and understand these various world cultures (especially in depth) will greatly appreciate LaPaglia's examination of their respective constructs of strategic intelligence.

Of note, and this is not an endorsement, LaPaglia references, and draws heavily from, Walt Disney's "The Sword and the Stone" (1963) as a seminal concept of "what is strategic intelligence" in practice. Readers who are unfamiliar with this movie should attempt to watch it (or at least read a description of it) so that they will be better acquainted with LaPaglia's points of view. He remarks, "Although insensitivity and ignorance to the dynamics of change in the mutable present can easily lead to one's unanticipated and premature end, 'The Sword in the Stone' is authoritative cultural evidence that human hope lies in Strategic Intelligence" (p. 25).This reviewer actually had to re-watch the entire movie but only after realizing that LaPaglia draws from it for almost every chapter of his book. In retrospect, the reviewer probably would have gotten more out of the book if the author had suggested in the preface that readers should watch the movie first.

• •

THE MORALIST: WOODROW WILSON AND THE WORLD HE MADE.

Patricia O'Toole
New York, Simon and Schuster. 2018.
601 pages.

Reviewed by David A. Brock, a State Department Foreign Service Officer who has served overseas assignments in Russia, China, and India. He graduated with an MSSI degree from National Intelligence University in 2020. Prior to his State Department career, he taught English in both California and Mongolia.

Patricia O'Toole demonstrates an engaging writing style that draws in the readers and causes the 600-plus pages of *The Moralist: Woodrow Wilson and the World He Made* to slip by effortlessly. Her easy-to-read prose comes as no surprise as the former Columbia University professor is the author of several well-regarded biographies of luminaries from the late 19th and early 20th centuries, including a Booker Prize finalist. In this book she focuses almost exclusively on the years of Wilson's Presidency. She sketches out only the barest details of his childhood and his early life in order to focus on an almost day-by-day retelling of his Presidential years, and especially the post-World War I peace process. [Editor's Note: A perhaps interesting tidbit of information is that Wilson is the only U.S. head of state to have earned a doctorate, a PhD degree from Johns Hopkins University. He subsequently taught at Princeton University, which he later served as its president prior to being elected Governor of New Jersey.]

Woodrow Wilson's name has often come up in recent years in discussions related to racism and how historical figures should be remembered and celebrated. Most notably, in 2016 student protesters tried to convince Princeton University officials to remove Wilson's name from its renowned School of Public and International Affairs, an effort to account for his racist attitudes that was ultimately unsuccessful.[1] [Editor's Note: A renewed effort in late June 2020 after the police killing of George Floyd was, however, successful, and the Woodrow Wilson School is now known as the Princeton School.] *The Moralist* does not delve into Wilson's personal view of African-Americans or how his view of race relations was similar to or different from others of his era. The author's careful chronology notes many occasions in which Wilson faced civil rights questions and how his administration marginalized African-Americans, both in the U.S. Civil Service and in the war effort. However, none of these incidents receives an in-depth treatment from her. They are mostly dismissed with a quick suggestion that Wilson, a native of Virginia, feared disturbing the support of the Southern Democrats for his other priorities.

O'Toole draws a contrast between Wilson's increasing support for women's suffrage and his lack of support for civil rights for African-Americans (p. 325). She mentions that he had become convinced of the correctness of the campaign for women's suffrage but does not go on to draw a conclusion as to his personal beliefs regarding racial equality or inequality. In the introduction, she suggests Wilson knew that supporting the segregation of the Civil Service was morally wrong (p. 3), but the evidence in the book for this attitude is thin.

The failure to delve into Wilson's personal view on racial equality is particularly surprising because the first chapter, titled "Son of the South," makes it appear that this might be a main theme of the book. In this chapter O'Toole notes that Wilson's father, a Presbyterian minister, was involved in the founding of a Confederate Presbyterian Church after the national Presbyterian Church came out against slavery. Wilson's father, as Clerk of the Confederate Presbyterian Church, had been one of the signatories of a foundational church document that declared "we are profoundly persuaded that the African race in the midst of us can never be elevated in the scale of being."[2] Growing up with his father, whom Wilson called "the finest of all teachers" (p. 3), and with others in the southern Presbyterian educational establishment, undoubtedly would have exposed Wilson to similar ideas of racial inequality. Unfortunately, the book never deeply examines whether Wilson rejected these ideas as a young man, if he did so at a later point, or if his acquiescence to segregation as President was rather the resurgence of a long-held belief that he had suppressed while living his adulthood among the more progressive ideas of the northern educational establishment. One insight into Wilson's views on race appears when he opposes the attempt of the Japanese delegation to have racial equality written into the Preamble of the League of Nations. O'Toole points primarily to political expediency for Wilson's opposition to this idea (pp. 368-369). This explanation seems inadequate, however, as O'Toole also extensively demonstrates that Wilson pushed for many things in the League of Nations that he knew would not be politically palatable to political factions in the United States.

The lack of clarity regarding Wilson's true view of race relations is emblematic of a major tendency in O'Toole's book to refer continually to Wilson's moral convictions, but then not to engage as to where he acquired these convictions. That said, she does point out that Wilson's convictions were not absolute and that he felt it was important for a leader to be able to change his mind (p. 220). She also points out, however, that Wilson shied away from engagement with his critics (p. 242). This picture of a moralist, whose source of conviction is unclear, who sometimes changes his mind, and who does not react well to criticism, seems much closer to describing a person whose only true belief is that he is always right. Despite his upbringing in the South, Wilson's ongoing frustration with Southern Democrats makes clear that he feels little kinship with their worldview. However, the book provides little insight into what shaped Wilson's own worldview, which led to such a strong belief that he was correct. There is a brief mention of Wilson's interaction with Presbyterian missionaries to China during his time at Princeton and how this may have shaped some of his views on China (p. 86) and also how Supreme Court Justice Louis Brandeis influenced Wilson's ideas on economic justice (p. 54). Aside from these short interactions, however, there is very little insight as to whether other religious figures, books, philosophers, or historians shaped the way Wilson looked at various parts of the world.

While the book is frustratingly thin on the origins of Wilson's beliefs, it is richly detailed on how they played out in the Versailles peace conference and the founding of the League of Nations. The book goes into great detail on how Wilson's views and personality came to dominate the process, even though in the end not all of his ideas were adopted. *The Moralist* documents the other conference participants' view of Wilson's conviction of his absolute certitude as having been both a roadblock as well as something that could be manipulated for their own goals. O'Toole seems to suggest that this manipulation was possible due to Wilson's complete sidelining of the rest of the American delegation, including his own Secretary of State who could have better prepared him for the give-and-take expected from the other countries. Her fluid prose and excellent sourcing in this context turn what would seem like a rather dry, extended diplomatic negotiation into the display of an intriguing clash of personalities and principles.

Woodrow Wilson was undoubtedly one of the key personalities of the 20th century. Readers interested in the mechanics of his Presidency and exactly what went into the development of the League of Nations—and the United States' subsequent failure to join it—will enjoy this richly detailed history. Readers who are hoping to gain a greater understanding of Wilson's personal convictions and how his legacy should be considered in regard to civil rights will likely come away somewhat disappointed.

[Editor's Note: Those wishing to erase the name "Wilson" due to the late President's views on race would be strongly challenged in the nation's capital, where such icons as the Woodrow Wilson Bridge across the Potomac River (part of the I-95 corridor) and the Woodrow Wilson International Center for Scholars, a U.S. government think tank, are widely recognized as part of the landscape. There is even a Woodrow Wilson High School that has debated a name change. Expunging the legacy of slave-owners, supporters of slavery, and segregationists among the Founding Fathers and their later disciples would become even more problematic if protesters decided George Washington's and Thomas Jefferson's names

needed to be erased from history too. They have already attempted unsuccessfully to pull down the statue of Andrew Jackson near the White House!]

NOTES

[1] Joel Rose, "Despite Protests, Princeton to Keep Wilson's Name on School Buildings," *NPR*, April 5, 2016, https://www.npr.org/2016/04/05/473063746/despite-protests-princeton-to-keep-woodrow-wilsons-name-on-school-buildings.

[2] "Address of General Assembly of the Presbyterian Church of the Confederate States of America to all the Churches of Jesus Christ throughout the World," adopted in Augusta, Georgia, December 1861, Hathi Trust Digital Library, https://catalog.hathitrust.org/Record/010944332

• •

COVER NAME: DR. RANTZAU.

Nikolaus Ritter (translated by Katherine R. Wallace).
Lexington, The University Press of Kentucky, 2019.
243 pages.

Reviewed by MAJ (USA) Jeanette Chavez, who spent the last ten years of her career serving as a Chemical officer before becoming a graduate student at National Intelligence University. After graduating with an MSSI degree in July 2020, she is remaining in the National Capital Region and continuing her career as a Strategic Intelligence officer. She also holds an MA degree in International Relations from Webster University and a BA in History from UCLA.

Cover Name: Dr. Rantzau recounts the experiences of Nikolaus Ritter during World War II when he served as Chief of Air Intelligence in the *Abwehr,* the German military intelligence section. Tasked with establishing an espionage network to gather intelligence on British and U.S. aerospace developments, Ritter's memoir provides keen insight into the clandestine world of German military intelligence. Having completed a short military career during World War I, Ritter lived in the United States for 10 years before returning to Germany in 1935. His mastery of the English language and perceptive personality allowed Ritter to build an extensive network of agents throughout Europe, the U.S., and North Africa.

The most striking aspect of *Cover Name: Dr. Rantzau* is its extensive level of detail. The recollection of true names, cover names, locations, and dates allows for a chronological presentation of Ritter's experiences. Such detail is no small feat given Ritter's extensive travel throughout Europe under the cover names of Dr. Rantzau, Dr. Reinhard, Dr. Jansen, and Dr. Renken. In assuming multiple cover names, Ritter successfully hid his true identity and protected his agent network from collapsing in the event it was compromised. Readers are thus left with a proper sense of Ritter's astute nature and foresight capabilities. The level of detail provided also allows for the revelations of minute details which would otherwise be confined to Ritter's memories. Subversive tactics, such as the forgery of documents and the reliance on field agents for weather reports, are fascinating details which could otherwise be overlooked in today's age of technological advancements and reliance.

At the same time, the strength of this book is also its chief weakness. The level of detail provided gives the impression of a diary but it lacks the infusion of personal sentiment. Agents are presented as little more than a list of physical attributes and the personality traits gathered upon first impressions. As a result, readers are left with an inability to connect with the characters in this memoir. Due to the chronological presentation of events and the very nature of espionage, readers may find themselves referencing earlier material to reconnect with characters. Additionally, Ritter's extensive focus on facts and details comes at the expense of his personal thoughts. Moreover, while he provides some details about his private life, the few sentences on this topic at the end of a few chapters equates such information to little more value than a footnote. As a result, the memoir is often times a series of facts which leave the reader with little room for an emotional connection.

Overall, *Cover Name: Dr. Rantzau* provides an informative and succinct account of life as a German intelligence officer, a subject typically lost in the annals of time and classified records. The story of Ritter's work during World War II highlights one of a patriot intent on performing his military duties in service to his nation. Insights or criticisms of the inner workings of the military or German political leadership are to be found elsewhere. Instead, readers are presented with a personal recollection of events, albeit at the expense of personal feelings. Today's readers, including current intelligence personnel, will find this to be an informative and succinct account which handsomely contributes to the historical literature.

Submit a book for review!

Please send copies to:
American Intelligence Journal
256 Morris Creek Road
Cullen, Virginia 23934

National Military Intelligence Foundation
PO Box 683
Charlotte Court House, Virginia 23923