AMERICAN INTELLIGENCE JOURNAL

THE MAGAZINE FOR INTELLIGENCE PROFESSIONALS

MASINT and Other Technical Intelligence Priorities

NMIF

Vol. 36, No. 2, 2019

American Intelligence Journal

THE MAGAZINE FOR INTELLIGENCE PROFESSIONALS

Vol. 36, No. 2 *2019* ISSN 0883-072X

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.

AMERICAN INTELLIGENCE JOURNAL

Table of Contents

Table of Contents *(Continued)*

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 dedicated to Measurement and Signature Intelligence, and its various subdisciplines. MASINT is perhaps the least understood and most technical of the INTs, but also certainly one of the most challenging and interesting. Yet, it is one of the critical INTs needed to prevent strategic surprise, and thus has a very important role in intelligence and national security.

To understand the role of MASINT, it is helpful to review Department of Defense (DoD) Directives and Instructions. The Under Secretary of Defense for Intelligence, or USD(I), issues the DoD Directives to provide the roles and missions for the national agencies, services, and other intelligence components of the Department. The specific INTs are directed by DoD Instructions, and for MASINT the guidance is provided in DoDI 5105.58, MASINT. It provides the policy, responsibilities, and references for MASINT. Under "Responsibilities," it states that the Director, Defense Intelligence Agency, under the authority, direction, and control of the USD(I), shall:

- Serve as the DoD MASINT Manager.
- Establish, lead, and operate a unified, effective, and efficient defense intelligence community for MASINT activities.
- Manage DIA MASINT activities IAW DoDD 5240.01, including research and development and support of the transition of successful technology demonstrations into advanced development, fielding, and operations.
- Invest in MASINT R&D, training, technical demonstration activities, and acquisition consistent with guidance within resource limitations and in coordination with appropriate DoD components.
- Submit a nomination for National MASINT Committee (MASCOM) Chair for DNI or designee approval. Align personnel and provide administrative support to the MASCOM.
- Foster MASINT support to forensics, biometrics, and identity management.
- Support MASINT collection requirements and operations.

But what is MASINT? In the lead article "MASINT: An 'INT' for the 21st Century," LTG (Ret) Pat Hughes, former DIA Director, provides an overview of "INT" definitions and relationships, plus an extremely timely graphic portraying "All-Source INT." To further define MASINT, he lists the collected signatures of a wide variety of MASINT sensors, and the importance and samples of the signatures. To explain how MASINT attribution can solve the definition of an event, he walks the reader through a possible event, and how MASINT attribution defines and clarifies the event. He emphasizes the necessity to fully understand MASINT and especially when considering future threats. And, in wrapping up the overview of MASINT, he cites the requirement to fully develop the MASINT tools along with the need to motivate leaders further to use the toolset for getting the full benefit of MASINT collection, processing, exploitation, and dissemination.

Dr. John Sislin's article, "Underappreciated, Underrepresented: Thoughts on Teaching MASINT," describes the MASINT discipline in his outstanding description and guidance on how to teach this complex INT, and its more complex subdisciplines. He also delves into the "Myths of MASINT," and promptly dispels them. In so doing, he provides in more detail many aspects of the MASINT discipline, plus some of its sophisticated collection platforms, which leads to a clearer understanding of this intriguing intelligence entity.

To put MASINT in perspective, John Morris offers an incisive article, "MASINT: An 'INT' Still in Transition." He last wrote a couple of *AIJ* articles on this emerging discipline back in the 1990s while he was heading the nascent effort in DIA. He tracks its development through the Cold War period and lists programs that were developed around Cold War requirements. Then he addresses changes in MASINT dictated by the elusive "Peace Dividend," and the effects these changes had on MASINT organization and allocation of resources. The latest iteration of MASINT management is defined in the previously mentioned DoDI 5105.58 MASINT, in which the DIA Director is the DoD Manager, and appoints the Chair of the National MASINT Management Office. Consequently, MASINT execution is now federated, for the most part.

There are also two thinkpieces on various aspects of MASINT that are evolving. James Carlini's "Adapting and Adopting MASINT for Modern Military Operations" addresses cyberwarfare and its integration of sensors, especially MASINT sensors, to react quickly—even in seconds. He posits that "MASINT is the Future of Military Intelligence" and the necessity for a "Collage of Intelligence" to meet cyberwarfare timelines. His article is an excerpt from his forthcoming book, *Nanokrieg: Beyond Blitzkrieg*. Carlini has contributed several forward-looking pieces to *AIJ* over the last few years.

The other article is "Nanosecurity: Human Brain Electro-Optical Signals as MASINT," by Dr. Matthew Carlson and Dr. Ben Sawyer. They apply neuroscience focused on the inner workings of the mind. By taking a MASINT perspective on neural signatures along with projected technology developments, they surmise the possibility of remote interference in normal brain activity. The example is the "Havana Syndrome," which has symptoms usually associated with concussions or traumatic brain injury. The authors break down brain functions to discuss future neurosecurity vulnerabilities. Consequently, they believe MASINT is an excellent place to begin to detect the effects of these weapons, and how to guard against them.

MASINT is not just an intelligence discipline for defense applications, but can be used in a variety of missions. After Hurricane Katrina devastated New Orleans, the U.S. Coast Guard Commandant, Admiral Thad Allen, was selected to direct the federal response to the hurricane. ADM Allen was desperate to get more information on the destruction, geolocations of specific damage areas, and information to help guide the rescue and emergency planning. He turned to the Intelligence Community for help, and the then-NGA Director, Jim Clapper, put new capabilities into action. NGA teams were deployed to directly support the Coast Guard and the Federal Emergency Management Agency (FEMA). Hyperspectral imagery information was used to detect harmful effluents, plot their paths, and predict future flows. This helped significantly with the relief and rescue efforts, and made them more efficient, timely, and effective.

Another example of MASINT support emerged after the 9/11 attacks on New York City. While trying to determine the extent of the collapse of the World Trade Center's "Twin Towers," and the danger to adjacent buildings, LIDAR images were made of the impact areas. LIDAR, an acronym for Light Detection and Ranging, includes a remote-sensing method that uses light in the form of a pulsed laser to measure ranges (variable distances) to Earth. From the LIDAR images, it became easier to determine the damage, debris fields, and potential additional damage from the fallen towers.

The next volume of the *American Intelligence Journal* will be titled "Intelligence Community Leadership: The Next Generation." It will feature articles only by students on various aspects of intelligence. Of course, student articles have been published in the past, but this special volume will be devoted to those representing various universities across intelligence disciplines and subdisciplines. This initiative is another NMIF effort to advance the public awareness of the roles of intelligence professionals and the contributions they make to society, military intelligence organizations, intelligence disciplines, and advancement in analytical methods and techniques. Two other key roles the Foundation plays in support of intelligence careers are the NMIF Scholarship Program and the annual Awards Banquet. The scholarship funds qualify as charity donations, and virtually all the donated money goes to scholarship winners. This is because NMIF is an IRS Code 501(c)(3) charity.

In the spring, the NMIF Awards Banquet is hosted in full partnership with the national agencies, service intelligence organizations, and other intelligence and national security organizations. Nineteen awards are made during this celebration of outstanding intelligence practitioners. The winners are selected by their intelligence or national security parent organization, and recognized by their senior leaders during a truly memorable evening. The next Awards Banquet is now being planned. Intelligence and national security practitioners, as well as students, are warmly invited to attend.

John Clark

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

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

The Editor's Desk

Welcome to the first-ever issue of *AIJ*—at least the first on my watch going back to 2009—focusing on the little known and poorly appreciated discipline of Measurement and Signature Intelligence (MASINT). When the NMIF board of directors first urged me to put together an entire issue on MASINT, I was skeptical it was possible. From my earlier days as a collection manager for a combatant command, and from having attended DIA's Intelligence Collection Management Course nearly 35 years ago, I at least knew what MASINT was and its potential benefits. However, I also realized that some of its subdisciplines were extremely sensitive (and often highly classified), esoteric, and downright mysterious. In fact, I was worried that I would not be able to procure a sufficient number of unclassified manuscripts to fill a volume. Hence, I convinced the board to expand the breadth of the issue's reach to include Technical Intelligence (TECHINT) in general, figuring I could tap into the S&T intelligence community for material that was instructive and interesting but that did not restrict itself to the more specialized world of MASINT.

Fortunately, I think we achieved a double victory here. We were able to solicit five outstanding articles on MASINT or MASINT-related topics, ably summarized by President Clark, with another handful that qualify under the TECHINT rubric. One reason this issue is arriving in your hands several weeks after the end of 2019 (the cover date) is that we had to walk a bureaucratic tightrope in getting a couple of the manuscripts through the mandated pre-publication review process, which took much longer than anticipated. We knew that two articles in particular would attract attention at the highest levels of DIA—former Director Pat Hughes' piece and another written by his former Central MASINT Office chief, John Morris, who also had worked this "INT" at both NGA and CIA. These articles finally made it through, with Morris' modified somewhat, and we're delighted to feature them in this issue. I'm also pleased that one of my NIU colleagues, Dr. John Sislin, who teaches courses on collection and earlier delved into GEOINT and other INTs while serving as an NGA analyst, offers us a magnificent argument on how MASINT can be most effectively taught. John shows us this subject can be broached at the lowest possible classification levels and woven into classroom instruction on the other disciplines. He helps us "demystify" this INT that others too often try to avoid.

There is quite a bit of material in the unclassified news that can be used in courses on MASINT. For example, one revealing article I ran across in April 2019 in *Air Force Times* is titled "Patrick AFB's Secret Lab Watches for Nuclear Explosions Worldwide." It talks about the mission and role of the Air Force Technical Applications Center (AFTAC), which according to the article "detects and analyzes nuclear explosions detonated by foreign countries, utilizing a sprawling network of more than 3,600 sensors deployed around the globe." The Center "monitored the 1986 Chernobyl nuclear power plant accident in the former Soviet Union; verified North Korea's first nuclear test in 2006; and scrutinized Japan's 2011 Fukushima Daiichi nuclear power plant disaster." AFTAC has long been tasked with worldwide treaty monitoring and verification. The details on the methods are classified; the big picture is not. Another example stems from the 1990s when I was an attaché in Colombia and Peru. We were permitted to advise our host counterparts that the U.S. was capable of peering through triple-canopy jungle to detect emissions from microwave ovens used in remote labs that the narcotraffickers assumed were concealed. However, the exact methodology was classified and not shared.

Since I just mentioned both DIA and NIU, let me share a piece of news that some of you may already have heard. On October 1, 2020, after being under DIA's wing for 58 years (only one year younger than DIA itself), NIU will no longer be part of DIA. Made official by the most recent iteration of the National Defense Authorization Act, NIU will be moved directly under the Office of the Director of National Intelligence (ODNI). This change in executive agency was probably inevitable given the fact the University in recent years has seen both its student body and faculty become more "interagency" and its curriculum has evolved into something much broader than merely defense intelligence. Hence, we witnessed the series of name changes over the last four decades from Defense Intelligence School to Defense Intelligence College, to Joint Military Intelligence College, to National Defense Intelligence College, and finally to National Intelligence University in 2011. Only a couple of us still on the NIU faculty can boast that we have been affiliated with the school either as a student or faculty member at each of these name iterations. Change is constant, of course, as reflected by the changes in technology the IC is now experiencing at blinding speed. The newest component of NIU tries to keep track of those

changes, and that's the Anthony G. Oettinger School of Science and Technology Intelligence (SSTI), named for the longtime Harvard professor and chair of the Board of Visitors (BOV) and accredited to award the Master of Science and Technology Intelligence (MSTI) degree. The commencement speaker for the 2019 NIU graduation ceremony was BOV member Gilman Louie, the first CEO of In-Q-Tel. He observed, "We are entering a new era of disruption… We will see more change in the next 15 years than the last 50." He advised graduates to "never forget that intelligence is not a perfect science… It requires risk taking and expert judgment."

Although transferring to ODNI, NIU will still work closely with DIA and some of its faculty will likely continue as DIA employees. That is important for the subject at hand because DIA plays a central role in both MASINT, as President Clark outlined in his message, and TECHINT. In two separate items in the "This Week in DIA History" section of his weekly update to the workforce, the DIA Chief of Staff noted (paraphrased):

July 12, 2019 – DIA: Executive agent and functional manager for MASINT. Measurement and Signature Intelligence may be the least known and most technical intelligence collection discipline. MASINT utilizes science and technology to collect and analyze data, which helps characterize, identify, and locate the adversary in air, land, and sea. On July 17, 2009, the Principal Deputy Director of National Intelligence appointed the director of DIA as the MASINT functional manager for the U.S. Intelligence Community.

April 4, 2019 – DIA takes lead on the DoD technical intelligence mission. Shortly after DIA's creation in 1961, the Agency was tasked with development of necessary requirements for a unified DoD program for technical intelligence on foreign military forces. In April 1964, SECDEF Robert McNamara approved DoD Directive 5105.28, establishing DIA as the mission lead for intelligence collection and production requirements. A major undertaking, this placed DIA in the lead for gaining a grasp of foreign scientific and engineering advancements, capabilities and limitations of weapons systems, research and development, production methods and locations of weapons systems, acquisition and exploitation of these systems, and preparation/dissemination of findings.

Moving to TECHINT in general, the province of SSTI, there is little doubt that this is the path along which the IC is moving rapidly in the 21st century, despite the cautionary tone of the last two issues of *AIJ* which covered CI and HUMINT, respectively, in both of which the human factor is paramount. LTG Hughes aptly captured the trend in a presentation he gives to various civilian audiences titled "Complexity and the Convergent Forces of Change," curiously dated December 7, 2019 ("a date which will live in infamy" in terms of a malicious threat that went unwarned, or at least poorly warned, and unheeded). A couple of the general's bullets ring true: In a slide depicting "where we are now," he observes, "Technology has affected everything. Techno-change in techno-time is axiomatic." In a slide on "where we are going," he insists "techno-revolution proceeds unabated." BG Irene Zoppi of NSA, in her article about the future of warfare in an S&T-focused world, argues for a whole-of-government approach when it comes to investing in S&T and R&D. She discusses the ramifications of asymmetric conflict and projects that by 2030 the U.S. must have significantly increased its combat S&T superiority to maintain its dominant position in the world. In a preview of the theme for our next regular issue in 2020, while not forgetting the lessons of our first issue of 2019, frequent *AIJ* contributor Ray Faunt teams up with former Marine Corps Intelligence Activity (MCIA) commander Phil Gentile on "Artificial Intelligence within the Intelligence Community: The Need to Retain the Human Dimension" (as you will see later, AI will be the focus of a future issue). Next, Dr. Gus Otto, DIA's senior representative to NORAD/NORTHCOM and an NIU adjunct, talks about "Ethics and Morality in the U.S. Government and How the Intelligence Community Must Respond." Exploring situations which can challenge an intelligence officer's sense of what is right versus wrong, to include the "whistleblower's dilemma," Gus concludes that "passing the responsibility to the lawyers and chaplains has resulted, for too long, in the abdication of responsibility by leaders to create a climate and culture of ethical and moral behavior."

You have heard me say before that we try to include at least one article on China in each issue, given its critical importance and especially in terms of science and technology (which it likes to steal if it can get away with it). In this issue we feature an article on China's sanctions program related to the controversial U.S. deployment of the Terminal High Altitude Air Defense (THAAD) system to South Korea, written by recent Oxford graduate Caroline Chang. She expertly utilizes the THAAD sanctions by China as a case study to analyze trends in Chinese sanctions behavior overall and to understand the evolution of Beijing's retaliatory playbook. China's activities in the hi-tech world were the subject of an excellent seminar sponsored by NIU's Office of Research that I attended in January 2019. Charles Durant, Deputy Director for Counterintelligence at the Department of Energy, gave an unclassified overview of "The Targeting of U.S. Science and Technology by China." He reminded his audience that "China has a vigorous and voracious effort underway to improve its scientific and technological capabilities through the legal and illicit acquisition of U.S. intellectual property." According to Durant, Beijing is especially interested in DOE's multi-billion dollar complex of National Laboratories.

These Labs perform advanced basic science and applied research into "some of the most challenging national security and economic technology problems, and their work is of high interest to China's leadership, national security officials, companies, and researchers." In his unique article, Italian professor Giangiuseppe Pili compares being a chess player and serving as an intelligence analyst, something I had never thought about before. I met Dr. Pili at the 2019 annual conference of the International Association for Intelligence Education (IAFIE) in New York and heard his intriguing presentation on this link between two seemingly different worlds. I asked if he would distill his thinking into an *AIJ* article that could be understood by non-chess players like myself. As a former chess instructor and referee, and author of books on chess and philosophy, he is highly qualified.

We are proud to include the paper which won the 2019 NMIF Sherman Kent Award for intelligence writing. It was written by Jack Matthews, an Army Corps of Engineers official and graduate of the National War College. Jack provides an engaging study on the effects of disinformation on liberal democracies. Frequent *AIJ* contributor Dr. Bill Kelly of Auburn discusses the testy relationship (at least recently) between the U.S. President and the Intelligence Community. He argues this is a decades-long, naturally conflictive lash-up but measurably worse under the current administration. Kelly attributes this in part to the fact that Donald Trump is not a professional politician and has little experience working in a government bureaucracy. Next, Canadian attorney and researcher Andrew Fraser discusses another contentious issue, the Taliban in Afghanistan and the intricate, sometimes insidious role of neighbor Pakistan. He insists Pakistan is playing a ruthless "double game" with its pervasive influence over what goes on in Afghanistan and South Asia at large. NSA's Zach Young, a recent graduate of NIU's SSTI, advocates for a *National Intelligence Strategy* that takes information power into greater consideration. He argues the U.S. government must use every instrument at its disposal, and also lobbies for tighter integration between the *National Intelligence Strategy* and the President's *National Security Strategy*. Repeat *AIJ* contributor Rad Malkawi of Jordan discusses lessons learned by the U.S. military in an operational environment. He advocates for greater cultural knowledge and awareness in pre-deployment training, which he claims is too superficial and ignores the "I" in the "DIME" construct that DoD and IC students learn early on.

NMIF board member Col (Ret) Carla Bass, author of the award-winning book *Write to Influence!* (now in its 2nd edition), recently did a radio interview about the importance of good writing, which has been adapted into an article that should benefit our *AIJ* readers, many of whom are in positions where writing precisely and cogently is critical. Carla has taught more than ten writing workshops at NIU over the last year and a half. She routinely offers her writing and editing skills to help improve NMIF products. We are delighted to include two "In My View" articles in this volume, the sort of opinion pieces I don't receive as often as I'd like. Naval analyst Luke Holloman looks back at tactical intelligence failures from the Vietnam War to our current operations in Afghanistan and Iraq. He explains why assessments/estimates were often faulty, not for lack of tactical intelligence but more often than not due to weak organizational structure, compartmented information access, and what he calls "analytical complacency." Luke insists U.S. officials did not understand Vietnamese culture, which ties in nicely with Dr. Malkawi's conclusions. Retired Naval officer, NIU faculty member, and repeat *NIU* contributor David Belt, who teaches Middle East courses, argues that the assassination of Iranian General Soleimani was a mistake from a long-term perspective, a position with which I would guess many of our readers would disagree. That's what "In My View" essays are all about—projecting novel or provocative ideas while encouraging dissent and dialogue.

Finally, NMIF President John Clark briefly salutes a former President of NMIA—our longtime predecessor and then partner organization—Lt Col (Ret) Carol Bessette. This career Air Force officer was dedicated to defense intelligence and to NMIA. She helped steer the Association through rough waters during its early development. She will be missed by her family and those who were in and around NMIA in those formative days.

We still have a few more weeks to collect articles and book reviews for our first issue of 2020, which is being restricted to those by students only. As I said in my last column, we're doing this in part to demonstrate NMIF's mission of encouraging young people to develop an interest in seeking intelligence careers. NMIF is insistent upon funding a robust scholarship program assisting students in intelligence studies programs and, through a newly established Education Committee (staffed, amazingly enough, by some of our newest and youngest board members whose own student experience was not that long ago), is exploring ways to interact more intensely with students at a number of institutions. Therefore, an issue of *AIJ* showcasing the work of some of the best and brightest from that contingent—whether having previous experience working in the IC or not—makes eminent sense. Although we have a solid lineup of articles so far, there is still plenty of room for more. In particular, I could use some book reviews by students. If you've read a good book lately dealing with intelligence, national/international security, homeland security, or law enforcement, and it's been published in the last two years or so or is forthcoming soon (perhaps you have a proof copy), please let me know and, if there's not already a review of that book in the hopper, you may submit

it. I know that often students have to critique a book for a course, or perhaps they've investigated one for the literature review of their ongoing master's thesis or doctoral dissertation. Why not convert that effort into a review of the book that can get you a little additional exposure in the pages of *AIJ* and also add a line to your CV?

Starting with the student-only issue, here is the slate of *Journal* themes through the end of 2021:

- Spring 2020: "Intelligence Community Leadership: The Next Generation" (cutoff May 15).
- Fall 2020: "Artificial Intelligence: Ramifications for Collection and Analysis" (cutoff October 15).
- Spring 2021: "Countering Transnational Threats" (cutoff April 15).
- Fall 2021: "Law Enforcement Intelligence and Homeland Security" (cutoff October 15).

I look forward to hearing from prospective authors and reviewers, and especially students. In addition, I welcome feedback at any time on the value of this *Journal* to your studies and professional work. We are always anxious to hear your thoughts on past articles, books read, and themes we should consider for future issues.

Bill Spracher
Editor

MASINT:
An "INT" for the 21st Century

by LTG (USA, Ret) Patrick M. Hughes

A wisp of smoke, a burning bush, oily water, sand seas, and rolling thunder from the sky. Do these things mean the commandments are being handed down again?

Some people say it is not real. They claim MASINT is a dust bin for everything that some other "INT" does not include (or want).

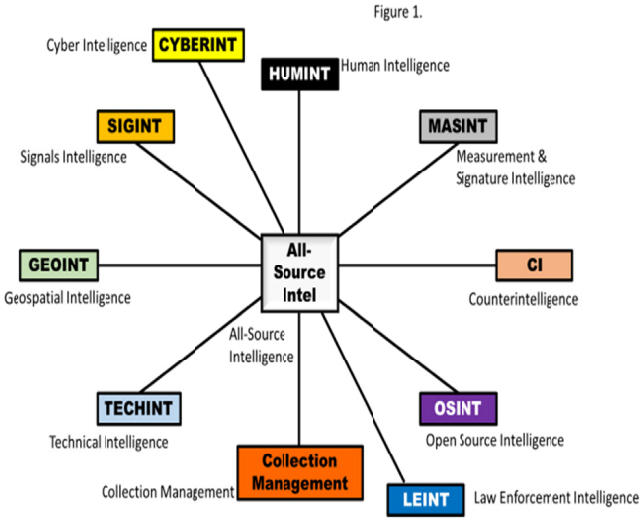
Some say it is not a "real" INT since it has no dedicated singular agency behind it. Indeed, they claim, it lacks the structure and distinctive identity of SIGINT and GEOINT and HUMINT (although these "INTs" have their own identity problems).

Besides that, they do not like the term "MASINT." Some people spell it as "MazeInt." My reply: Ridiculous! If Obe Wan Knobe had thoughts like this, where would the Power be? This view is inherently ultracrepidarian. To begin with, what is MASINT?

Measurement and Signature Intelligence (MASINT) is a scientific and technical (S&T) form of intelligence which seeks to collect, process, identify, analyze, and understand specific characteristics of signatures, and to provide descriptive technical measurement of those signatures. This includes certain appearances, reflections, emissions, chemical and biological make-up, dynamic activity, and all other specific "signatures" which identify and describe, in their raw form and in their analyzed form, what needs to be known to facilitate military and intelligence missions, and other applications in support of national requirements.

This intelligence discipline may be facilitated and in part achieved by all other intelligence functional disciplines, such as those shown in Figure 1 below. MASINT may also require unique sensors, sources, and methods which have been specifically designed and structured to collect and analyze signatures and to develop measurement which is not otherwise available across the family of intelligence disciplines.

Figure 1.



To help understand Figure 1, here are the included intelligence functions under each major discipline heading:

HUMINT (Human Intelligence) – includes all intelligence derived from human sources.

CYBERINT (Cyber Intelligence) – includes intelligence derived from and applicable to the Cyber domain.

SIGINT (Signals Intelligence) – includes communications intelligence (COMINT), electronic intelligence (ELINT), and several other forms of related intelligence.

MASINT (Measurement and Signature Intelligence) – includes signature intelligence and applicable measurement from any and all sources which have collectable signatures.

GEOINT (Geospatial intelligence) – includes images, renditions, maps, charts, geodesy, and related intelligence.

CI (Counterintelligence) – includes all efforts undertaken to protect information and to find and eliminate security threats.

TECHINT (Technical Intelligence) – represents every possible source of scientific and technical intelligence, including the analysis and exploitation of materials, equipment, and capability.

OSINT (Open Source Intelligence) – includes any information which may be derived from openly available sources.

LEINT (Law Enforcement Intelligence) – should also be included as an "INT." It is made up of all the other noted intelligence functions (disciplines) but, because of the nature of its application and the legal context in which it is achieved, it must be mentioned as a distinct form of intelligence.

Collection Management – is a vital part of any explanation and operation involving the deliberate collection and subsequent exploitation of all sources of intelligence.

All-Source Intelligence – includes combined information from any applicable sources which is synergistic and provides more complete and accurate information than would otherwise be available from any single source.

The functions and applications of specific sensors, sources, methods, and collection mechanisms, and the subsequent reporting, processing, analysis, synthesis, and delivery of intelligence product to appropriate recipients, are included in each intelligence discipline.

MASINT (Measurement and Signature Intelligence) is that intelligence derived from [the] many signatures and measurements found in the environments of interest that are not otherwise the province of other [more traditional] intelligence disciplines. Its utility is derived from the technical collection of appropriate attributes and the measurement, analysis, and production of useful products in direct response to mission needs.

MASINT is made up of at least the following: Heat, Light, Sound, Odor, Chemical, Magnetic, Biological, Acoustic, Movement, Emissions, Radiations, Vapors, Nuclear, Radiological, Nano, Micro, Standard, Electromagnetic, Reflections, Energy, Gravity, Theory, Waves, Tubes, Pulses, Resistance, Particles, Waste, Air, Strands, Coils, Helixes, Rays, Roaming, Coherence, Asymmetry, Volubility, Mass, Form, Weight, Cube, Size, Smoke, Aggravation, Oscillation, Temperature, Speed, Liquidity, Fluidity, Time, Tension, Strings, Compounds, Minerals, Elements, Hybrids, Seismic, Hydroacoustic, Hydrologic, Infrasound, Infrared, Ultraviolet, Radio Frequency, Radar, Materials, Geophysical, Electro-Optical, Laboratory Results, Physics, Mathematics, Geology, Physical Sciences, Multi, Hyper, Ultra, Sub-Pixel, Algorithms, Optimization, Mirrors, Minimization, Target Detection, Correlation, COSMEC, IDL, ENVI, HYPEX, USMS, CMMS Filter, FLIR, SWIR, Hypercube, Wavelets, Fractals, Models, Advanced Code, AI, Robotics, UGS, DUGS, UUS, BAS, DDC, Architectural Documentation, City Public Systems Information, Manufacturing Data, Telemetry, Linkage, Parametric, Calibration, SAR, TAGS, RCS, Vibration, Extraction, Compression, Metadata, PRISM, Fire Plume and, of course, the ever present X. [Editor's Note: Some practitioners include telemetry under SIGINT, and specifically under ELINT. What used to be called (at least when I was a young MI officer taking courses on intelligence collection) Telemetry Intelligence (TELINT) was later expanded into Foreign Instrumentation Signals Intelligence (FISINT), and both were categorized as SIGINT. I do not desire to start a debate here, instead merely suggesting that not all intelligence professionals describe MASINT in exactly the same way.]

The importance of this form of intelligence cannot be overstated, especially in the evolving complex global condition. For example, weapons with mass and complex effects (WMCE) such as nuclear, biological, chemical, radiological, advanced explosives, electromagnetic pulse and, in contemporary context, some elements of cyber warfare and information warfare, must be understood in as much detail and with as much clarity as possible. That is not to say that other intelligence disciplines cannot make very specific contributions in this regard, but without putting the information in its larger "measurement and signature" context the needs of leadership and decision-makers cannot possibly be met.

Imagine, if you will, that a report from many quarters arrives in our nation's capital, describing a large explosion with a mushroom cloud and vertical striations appearing nearby. Then reports come to us about great destruction and chaos. Communications are disrupted. Finally, this situation begins to develop from reporting in the media. This may happen within minutes. Without a specified approach, with assigned responsibilities, to all the forms of intelligence and their subsequent (and rapid) combination, analysis, and synthesis, the obvious questions are unlikely to be answered—at all—let alone accurately.

Question #1: Was the explosion nuclear?
Question #2: Who did it?
Question #3: How did they do it?
Question #4: What are its likely effects?
Question #5: What steps should we now take in its aftermath?

Perhaps the most pressing question that seems to crop up in nearly every context is: Who did it? Whatever "it" was, attribution is a key part of intelligence response. Among the many other functions of MASINT, some specific

characteristics will usually be associated with specific sources or origins. Think of it as nation-state forensics on steroids.

Parameters (an important applicable term) can, in part, be defined by expected and projected threat conditions the U.S. is likely to encounter, but they must also be developed from real-time collection and rapid analysis. This requires a dedicated and well-designed (planned) approach to the entire intelligence cycle. It also requires a single integrated (interoperable) database and tool set designed for MASINT information.

Technologically advanced adversaries, extraordinary denial of entry activities by our opponents to their homeland, war in cities and other complex environs, war in our homeland, asymmetric and asynchronous conditions, unrestricted (multi-domain) warfare, and domination and control of people in very diverse geopolitical conditions are all possible, and all are likely to be different, more technical and more culturally challenging, than anything encountered in the past.

The future will include counterterrorism, counterinsurgency, counter-crime with national security implications, and small incidents and events that do not rise to the level of warfare—for example, the safe and successful evacuation of non-combatants from threatened locales, and numerous other categories of missions and requirements we can anticipate.

These events will take place in every possible domain and every possible dimension. All of them will have technical signatures and related measurements that can be dealt with only in a coherent way if a single group of technically trained intelligence practitioners with the right connectivity and the right protocols have the authority (and the responsibility) to answer the questions our leadership poses.

One of the functions of the IC is to describe this set of future threat conditions, in some detail, so that U.S. government leaders have some idea of the conditions and circumstances with which they will be faced…and what they will need to accomplish their missions. In the case of some anticipated threats, the scientific and technical details available through the MASINT discipline are the key to any accurate description of what we are faced with.

Some forms of the MASINT challenge will be seen by the purist as so mundane as to be unworthy of much attention—unless, of course, you are an operator who has to enter a building through a doorway on 11th Avenue NE, which has an Adams Rite AR 3090©, take two flights of stairs, enter the third door on the right, just down the hall, which it turns out is directly adjoining the facility control system the building depends upon for its electricity, system controls, and maintenance. There you must find the air vent on the left (green vent slats in a green frame against a beige wall), in which you can roll a grenade to the control room and still survive the blast, if you know which way the baffles slant, for sure, and whether or not the vent run has any vertical rise before it exits into the control room. You may also wish to know what sort of secondary explosions or damage effects might occur and if they will affect you. What about structural damage—can you still get out of the building? Cameras? Of course, you need to know everything you can about them and their systemic operation.

Later you may wish to fly a cruise missile into the 14th floor—the window on the left (south) side center of the building, geolocation: 1622.4E1533.2N (from a mobile telephone emission), which is 5 feet (152.4 cm) wide and 8 feet (259.08 cm) tall, made of tinted 15-Mi and possibly reinforced (tempered) glass, with a reflectivity rating of 92%, made by a small window manufacturer in Copenhagen, with 12-inch aluminum framework support, flush, which has a 1½-foot (45.2 cm) vent along its bottom and opens at an angle when occupants desire fresh air. It is the 14th floor, not the 13th, because there is no 13th floor—culture does not support it—so make sure it is the 13th story, but the 14th floor. Timing: 1735 local time. Target has an appointment for afternoon cocktails at 1700 hours. MASINT can help.

Moreover, if you need to enter the locked door on the lower basement control room which is the counterpart to the one you blew up earlier, you may want to know—you may need to know—which way the door hinges are mounted and what sort of heat signature the door has, as seen through your SENVG [Spiral Enhanced Night Vision Goggle], assuming the building has not collapsed. You need MASINT.

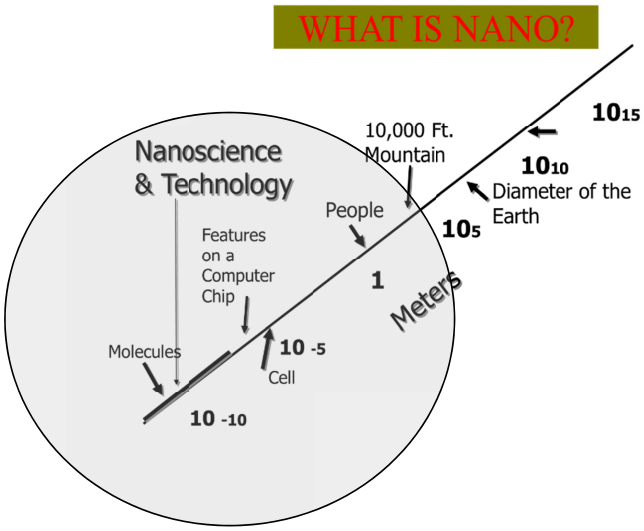
In case your mission includes determining where a terror group has its explosive device production facility, or whether or not a certain country which you have determined is the source of a bio-hazard has a plant related to the key component of—say ricin—which you must attack and destroy, then you may need MASINT help.

If you need to know which test stand is active, which tank is real, and which ship is the actual vessel on which the command group is embarked, or where exactly the enemy submarine may be in 14.9 seconds, or what the nomenclature and operational parameters of the anti-ship missile are, or what the exact range and likely fall-off of an air-to-air missile are, or when the clandestine satellite will fly by and be able to peer in on your activity, you may need MASINT.

The ability to develop this kind of intelligence will be anticipated by our potential opponents. This may include a build-up of long-term perception management and the

application of control, camouflage, cover, concealment, and denial and deception. The best way to see through the incidental presentation of a false signature or a misleading cue or a deceptive measurement is to have an all-source, all-method, all-science approach and to guard carefully our own abilities and methods. This is one reason why MASINT does not roll off the average "Intelligence" tongue—nor should it. We should protect all our capabilities, but the stuff of Measurement and Signature Intelligence is especially important, in part because some of it is so intimate.

We must come to grips with contemporary challenges in measurement too. Here are two simple examples. What, for example, occurs in the nanometer range that we need to know about?



Or, as another example, how do we measure something like computational power in floating-point operations per second (FLOPS), and what does it mean for military applications?

Prefixes in Order of Value from High to Low:

Yotta Y 1×10+24 1,000,000,000,000,000,000,000,000
Zetta Z 1×10+21 1,000,000,000,000,000,000,000
Exa E 1×10+18 1,000,000,000,000,000,000
Peta P 1×10+15 1,000,000,000,000,000
Tera T 1×10+12 1,000,000,000,000
Giga G 1×10+9 1,000,000,000
Mega M 1×10+6 1,000,000
kilo k 1×10+3 1,000
hecto h 1×10+2 100
deka da 1×10+1 10

MASINT is hard to fully "fathom" (pun intended). Nevertheless, it is a necessity for the modern age. That necessary "tag" will continue to be vital to our understanding of the operational environment and our enemies and their capabilities.

We need to put the right people—with the right training and background—in key positions, and develop a fully capable suite of MASINT tools and a support and communications infrastructure appropriate for this form of intelligence. We need to motivate young scientists and engineers (and wizards) to be interested in, and to serve in, this discipline. We also need the understanding and support of enlightened leaders, who will reinforce this intelligence discipline and use it to their advantage on behalf of our nation.

To do otherwise seems to me to be "illusionary."

LTG (USA, Ret) Patrick M. Hughes was the 12th Director of the Defense Intelligence Agency from 1996 to 1999. Prior to that, he was Director, J2, for the Joint Chiefs of Staff; CENTCOM J2; Commanding General of the Army Intelligence Agency; and Assistant Deputy Chief of Staff, Intelligence, on the Army Staff. From 2003 to 2005 he served as Assistant Secretary for Information Analysis in the newly established Department of Homeland Security. Now fully retired from the Army and government service, he heads his own consulting firm and travels often from his home in Florida to the Washington, DC, area to provide expert advice and assistance to the Intelligence Enterprise. He is a former President of the National Military Intelligence Association and served for many years afterward on the NMIA Board of Directors; he is now an NMIF Board Member Emeritus.

[Editor's Note: For more on LTG Hughes' tenure as the senior intelligence officer for DHS, see article by COL (USA, Ret) Michael M. Ferguson, "LTG Pat Hughes: The Renaissance Man of Intelligence and Homeland Security," *AIJ*, Vol. 35, No. 1, 2018, pages 65-73.]

Adapting and Adopting Measurement and Signature Intelligence for Modern Military Operations

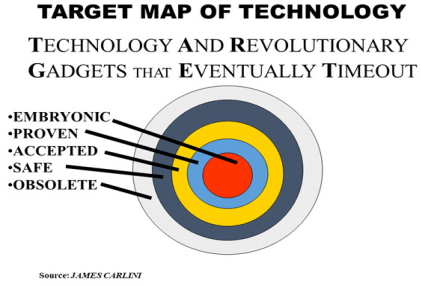
by James Carlini

[Author's Note: This article is an excerpt from my upcoming book, ***NANOKRIEG: Beyond Blitzkrieg***. It is a book series on redefining and rearranging the Military Infrastructure, Natural Destructive Strategies, Energy, and Tactics (**MINDSET**) needed to fight the Global War on Terrorism as well as any non-traditional conflicts in the 21st century.]

As discussed in a previous white paper by the author, NANOKRIEG: Beyond Blitzkrieg, the speed to conduct both attacks and counterattacks in war has been greatly accelerated. War has also been extended from the traditional (physical) battlefield into the electronic or cyber battlefields of Intelligent Infrastructure.

Like so many other technical and scientific subjects dependent on emerging technologies to support them, new intelligence-based weapons and countermeasures are only as good as the supporting technical devices, sensors, systems, and their applications by qualified staff and technicians. With these new tools, it is a complex job to keep track of and creatively apply new technologies for MASINT successfully. Tools start out as a system in an embryonic (emerging) stage and can mature quickly through four other stages of technology (proven, accepted, and safe stages to a status of obsolete technologies) (see Target Map of Technology below).

All technologies work their way through time from the embryonic (stage 1) to being proven (2) to being accepted (3) in a broader context across several industries, to becoming more common, everyday safe (4) technologies and then, eventually, they all become obsolete (5). Every technology runs through these five stages.



The successful application of MASINT creates a "Collage of Information and Intelligence" to utilize, which is more complex than a two-dimensional picture or chart and contains numerous unique identifiers to be analyzed and applied within a real-time decision framework. That multi-dimensional analyzation and synthesized application process needs to be as fast as possible if the information is to be usable within the accelerated, sub-second tempo of today's and tomorrow's real-time warfare.

> **"Quickness is the essence of the war."**
> **– *Sun Tzu***

How do we develop and maintain a real set of viable intelligence-gathering solutions as new technologies and weapons are constantly being developed as well as integrated by overlapping intelligence-gathering sensors and AI-based software? This article will answer that important question of the need for speed.

When it comes to fighting 21st century warfare, engaging traditional intelligence methods and battle-proven approaches from previous generations and conflicts is going to fail. Preparing officers and staffs to "fight with the last war's tools of strategies and tactics" will come up short (and late) against new weapons, integrated technologies, strategies, and tactics.

One of the big differences is today's battlefields have expanded from a traditional, physical platform to one where new dimensions of electronic battlefields are also employed. These new dimensions need to be thoroughly understood, analyzed, and defended. Cyberwarfare on cyber-platforms and Intelligent Infrastructure add to the complexity and open up more exposure to asymmetrical warfare (see Charts 1A and 1B on the following page).

Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) needs to adapt to include and oversee these new battlefield dimensions of warfare as well as engage in the latest capabilities of Intelligence, Surveillance, and Reconnaissance (ISR) across cyber battlefields (Intelligent Infrastructure) as well.

CHART 1A: THE EXPANSION OF THE BATTLEFIELD

TYPE OF WARFARE	DIMENSION	REQUIRED SENSORS	VELOCITY OF ATTACKS
TRADITIONAL WARFARE	PHYSICAL – LAND, AIR, SEA	UNDERGROUND, ABOVE GROUND, UNDERSEA & IN THE AIR	LIMITED
NANOKRIEG WARFARE	MULTIPLE DIMENSIONS OF BATTLEFIELDS (PHYSICAL, PLUS CYBERWARFARE, ELECTRONIC)	SAME AS ABOVE, PLUS ELECTRONIC/ INTERNET SENSORS & MONITORS	MUCH HIGHER ON THE ELECTRONIC BATTEFIELD

Source: James Carlini

CHART 1B: THE EXPANSION OF THE BATTLEFIELD

QUALITIES FOR SUCCESS IN SENSORS	WHY?
COVERT	*No Detection*
PASSIVE	*No signal emitting*
SPEED (PROCESSING)	*Fast analysis*
STEALTH	*No Detection*

Source: James Carlini

Another difference in today's battlefields is the tempo has accelerated. With electronic warfare, gathering intelligence of logistics for attacks and counterattacks has been changed from weeks and days to seconds and sub-seconds of time. The rapidity of attacks in cyberwarfare could be thousands of launches of various viruses, ransomware, and other denial-of-service attacks per second, and could definitely find its way into day-to-day operations.

One intelligence-gathering area showing promise in providing broader capabilities for battlefield analysis and faster decision-making is the area of MASINT. The Department of Defense recognized this discipline as a separate area of intelligence in 1986.

Creative analysis and approaches using new automated tools, intelligence-gathering sensors, and non-traditional methodologies as well as complex AI-based intelligence processing (Big Data) frameworks must be nurtured and applied. Any and all MASINT tools should be "joint forces" accessible and applicable, and not developed for single branch use only. (Clinging to outmoded strategies, like "This is the way we do it in the Army" or "This is the Navy way of doing things," is a waste of time as well as scarce and precious resources.)

MASINT: A COLLAGE OF INTELLIGENCE

MASINT, or Measurement and Signature Intelligence, is a relatively new discipline of detection, analysis, and defining conclusions based on the creative measurement of unique characteristics and by-products left by emissions, chemical signatures, radio-frequency emissions, seismic readings, and other emissive by-products an object leaves behind as a unique trail or identifier, like a fingerprint or footprint.

It has been said that MASINT is the future of Military Intelligence, but it can be viable only if we have military personnel who are sufficiently technical, creative, and innovative to understand thoroughly and apply these new "forensic"-type approaches as well as their supporting technologies beyond the traditional battlefield and expand it into cyberwarfare as well.

In this area, the diverse intelligence gathered and analyzed is only as good as the skills of the interpreter. The type of person who will do well in this area may not be the "traditionally" educated soldier. The persons working with MASINT will need to be creative, flexible, and adaptive, in addition to having technology skills.

In the Golden Age of Software in the United States (from the late 1960s to the early 1980s), there was a shortage of trained people and many companies recruited "trainable" people to become software developers, network engineers, and technical programmers. One of the best types of people to recruit was someone who had a music background because he/she was very used to working with and determining symbolic representation as well as understanding the framework of constructs and rules that dealt with interpreting the music. These individuals were also already exposed to team building and team dynamic skills. Those same types of skill sets are needed today when it comes to being creative and innovative when dealing with MASINT capabilities.

Integrated analyses to measure and detect various unique signatures of weapons, bombs, and other military ordnance must be made easy to apply as well as easy to synthesize and interpret rapidly. For the most part, the faster the total process can be fully executed, the more likely it can be applied to decision-making which, in many cases, has become real-time.

Multispectral measurements as well as unique, signature-tracking, intelligence-gathering approaches of passive and active emissive properties are used in new and complementary ways to create a "Collage of Information and Intelligence" that can be analyzed and acted upon. Instead of intelligence data contained in two-dimensional pictures, we are dealing with multi-phase mixtures (or collages) of information that are made up of various unique identity traits and emission trails gathered across a mix of terrestrial sensors and surveillance satellites.

It is already being said, "Multidisciplinary intelligence analysis will be crucial to meeting future intelligence needs." How well it succeeds in providing needed qualitative and quantitative intelligence will be "a function of both scientific ingenuity and management skill" as well as speed of execution.

What works one year could be technologically obsolete by the next year. New measurement approaches using various sensors and artificial intelligence (AI) for processing data analytics may change the whole way attacks and counterattacks are analyzed from their development throughout the framework of their stages of execution. [Editor's Note: The Fall 2020 issue of *AIJ* will explore the theme "Artificial Intelligence: Ramifications for Collection and Analysis." We are currently soliciting articles for that issue and expect to receive many, as AI is proliferating in virtually all aspects of modern society. I expect AI to play a pivotal role in the future of MASINT.]

There also can be no long-term "best practices" in this area because it is constantly changing and rapidly evolving with new facets of materials and diagnostic approaches being added and discarded on a regular basis. The best approach to keep up with these dynamic changes is to be creatively adept and understand that there needs to be continuous improvement in the intelligence-gathering techniques and state-of-the-art collection approaches because they could become obsolete by the following year.

Therefore, this process of identifying, collecting, and analyzing battlefield data to integrate into timely critical, usable information for strategic intelligence must also become significantly accelerated, in order to make informed decisions rapidly. This goes against what is currently being taught at the Naval Postgraduate School where one graduate course on "Intelligence for Homeland Security: Organizational and Policy Challenges" discusses the pros and cons of various intelligence-gathering approaches (including MASINT) and says that speed is not a prerequisite for success (see video at https://www.youtube.com/watch?v=SBdvDmgrTEk). On the contrary, in today's and tomorrow's wars, all are focused on speed of execution as well as speed of interpretation, decision-making, and counterattacks. Hence, in NANOKRIEG wars, speed is of the essence within the accelerated total framework of the war. All personnel working in this area need to be trained from a FACT-based approach for their skill sets. The skill sets need to be Flexibility, Adaptability, Creativity, and Technology-based.

SPEED IS OF THE ESSENCE

As more weapon systems become computerized and networked, speed is a prerequisite for success. The faster one can collect, analyze, process, and synthesize data into actionable information (intelligence) for decisions, the faster one can launch a successful attack or counter-attack.

The MASINT discipline currently under review includes a large set of both qualitative and quantitative characteristics which are still being added to. It is a relatively new area that originates back in 1986 when it was defined as an intelligence discipline. Its complexity and ongoing evolution raise the question as to how effective can it really be, unless there is real expertise in understanding and applying battlefield forensics? MASINT and Materials Intelligence can operate and overlap.

It has been said that MASINT "is the least understood of the disciplines and is perceived as a 'strategic' capability with limited 'tactical' support capabilities. However, MASINT has potential ability to provide real-time situation awareness and targeting not necessarily available from the more classic disciplines" (from http://www.au.af.mil/au/awc/awcgate/congress/ic21/ic21007.html).

If we review the phases of MASINT (see Chart 3), in the first "Stage of Process," Collection, the duration of this step (variable) could take days, hours, minutes or an immediate microsecond in time depending what we are looking at and observing. This stage may or may not be a candidate for any accelerated processing simply because the data we are collecting and/or sampling does not lend itself to any uniform accelerated collection approach. For example, changes in formation of ground forces, aircraft on a field, or ships in a harbor might be collected over a week or several days. The collection of the new additional forces and their changed locations cannot happen until it actually occurs. Something else, like a vapor trail from a ballistic rocket, may only have a 5- to 10-second real-time window from which to collect data to analyze, or from some electro-magnetic pulse to detect in a fraction of a second.

CHART 2: INVENTORY OF MASINT CHARACTERISTICS CURRENTLY ANALYZED

CHARACTERISTIC	DEFINITION
ACINT	Acoustic Intelligence (Non-Compressible Fluids)
ACOUSTINT	Acoustic Intelligence (Compressible Fluids)
CBINT	Chemical & Biological Intelligence
DEWINT	Directed Energy Weapons Intelligence
DMPINT	Event-Related Dynamic Measurement Photography
ELECTRO-OPTINT	Electro-Optical Intelligence
FISINT	Foreign Instrumentation Signals Intelligence
IRINT	Infrared Intelligence
LASINT	Laser Intelligence
MATINT	Materials Intelligence
NUCINT	Nuclear Intelligence
RADINT	Radar Intelligence
RF/EMPINT	Radio Frequency/Electro-Magnetic Pulse Intelligence
RINT	Unintentional Radiation Intelligence
MSI (Multi-Spectral Imagery)	Spectroscopic Intelligence
EDC	Effluent/Debris Collection
ADDITIONAL AREAS TO ADDRESS: (INTERRELATIONSHIPS)	
CYBINT	Cyber Intelligence from Cyberspace
DNINT	Digital Network Intelligence from Cyberspace
FININT	Financial Intelligence
OSINT	Open Source Intelligence
SIGINT	Signal Intelligence
TECHINT	Technological Intelligence

Sources: https://www.dsta.gov.sg/docs/default-source/dsta-about/dh2007_chapter_10.pdf?sfvrsn=2 and https://en.wikipedia.org/wiki/List_of_intelligence_gathering_disciplines#TECHINT.

CHART 3: BREAKDOWN OF MASINT STAGES

STAGE OF PROCESS	DURATION (Time)	PROCESSOR(S)
1) COLLECTION	VARIABLE	DEVICE/ SENSOR
2) ANALYSIS	SUBSECOND	SENSORS/COMPUTER
3) SYNTHESIS	SUBSECOND	COMPUTER
4) PRODUCTION	SUBSECOND	COMPUTER
5) DECISION	SUBSECOND	Human or System
6) APPLICATION/ ACTION	VARIABLE/ SUBSECOND	Human and/or System Decision

Source: James Carlini

When we look into the second through sixth duration (Time) phases (in "green" for the stages of Analysis, Synthesis, Production, Decision, and Application/Action), we need to be able to accelerate processing in these areas due to the technologies (hardware, software, and firmware) we may be able to deploy. It is in these areas (green) that we should segregate into specific sub-stages and look into developing better technologies to accelerate the total processing and amalgamation of data within that sub-stage into useful information (see Chart 3).

USING MASINT IN A REAL-LIFE SITUATION

Most should remember the movie "The Hunt for Red October." In that popular film, the sound of SONAR was used to track the Russian nuclear submarine until it went into a quiet mode using a newly developed caterpillar drive for "silent mode" propulsion. SONAR has come a long way since World War II, and the actual engine noises of a boat going through the water could be identified just by the sound signatures of the unique noises of its engines.

SONAR is considered a widely recognized and accepted example of a MASINT technology. The new technology was when the SONAR person started to track the non-organic engine noises coming out of the Red October made by a sound signature of the water being pushed out by a new caterpillar drive to propel the submarine in a quiet mode. That type of sound signature was new and first recognized as a seismic event by the computer and then used to track the sub (movie clip: https://www.youtube.com/watch?v=y7g6dKncO-I).

MASINT tries to obtain and analyze these new unique signatures and emissive trails based on collecting, measuring, and analyzing them and recording them to be used in a database as a comparison for future identification. This type of approach is being utilized in many different areas and applications across the electromagnetic spectrum as measurement devices and sensors continue to be developed, concentrated, and applied to many areas. The applications are limited only by the creativity of those employing the technologies and how they can use and integrate them for the new, unique, real-time "Collage of Collected Data, Information, and Intelligence."

In another example, let us say a bomb goes off in a building in New York City, and it is claimed to be the work of a specific terrorist group. The explosives used leave a residual chemical "signature" as well as a blast imprint as to the type of explosive used. Analysts involved in MASINT would take a detailed look at the explosion's aftermath, collect samples of debris and chemicals, as well as take some pictures of the area to determine the strength of the blast. They would also look to see if they could find any residual traces of chemicals and forensic remnants of the triggering device which could then also be analyzed to see what country of origin it was from or if it was some type of homemade triggering device.

Once all the forensic evidence and information are gathered, the type of explosive is examined and compared to a database of unique explosive "signatures" to see if it matches any previous bomb explosions and/or chemical characteristics.

- Was it C4? Was it dynamite?
- Were there any residual traces of specific chemicals or chemical compounds?

- Was it some homemade combination of explosive and/or combustible materials?
- Were other materials added (nails, ball bearings, incendiary devices)?
- Was it some sophisticated combination of materials that a specific country, military, or terrorist organization uses (U.S., Russia, China, Israel, Iraq, ISIS, Taliban, other)?
- Was there a homemade or sophisticated triggering device (country of origin?)?

All of these questions would be answered (see Chart 4).

If it does not match any previous bomb signature or "chemical footprint," it will probably be determined to be a new version or type of device that was first used in this specific event. All of the information collected at this specific event would be logged into the database and become more information for comparison after the next incident.

By having the database of information on chemical makeup of explosives, explosion footprint, other materials added, and country of origin/organization on triggering devices, we can determine whose work it is or determine if is someone totally new, or someone from previous attacks using an existing model or modified version of an existing explosive device. Other types of measurements can also include analyzing electromagnetic signatures of various metals.

The two sets of characteristics (Charts 5 & 6) are not mutually exclusive. If anything, they are overlapping. It is entirely possible that, as this newly recognized discipline emerges, a new and more widely accepted set of criteria will evolve. For example, the DIA list considers vibration. In the Center for MASINT Studies and Research list, mechanical vibrations, of different sorts, can be measured by geophysical acoustic, electro-optical laser, or radar sensors.

MASINT specialists themselves struggle with providing simple explanations of their field. One attempt calls it the "CSI" of the Intelligence Community, in imitation of the

CHART 4: BOMB EVENT COMPONENT ANALYSIS CHART

CHARACTERISTIC	DETAILS
CHEMICAL COMPOSITION	FROM EVENT SITE
TRIGGERING DEVICE	FROM EVENT SITE
BLAST FOOTPRINT	FROM EVENT SITE
OTHER MATERIALS PRESENT	FROM EVENT SITE
OTHER COMPARABLE SITES (SAME OR SIMILAR MATERIALS, CHARACTERISTICS	FROM DATABASE
ANY ORGANIZATION/ GROUP/ COUNTRY MATCHES	FROM DATABASE

Source: James Carlini

There are six major conceptual disciplines of MASINT: The Disciplines (see Chart 5), as defined by the Defense Intelligence Agency (DIA), which include (see Chart 6):

CHART 5: MASINT as Defined by the Center for MASINT Studies and Research

AREA/ DISCIPLINES ANALYZED
ELECTRO-OPTICAL
GEOPHYSICAL
MATERIALS
NUCLEAR
RADAR
RADIO FREQUENCY

CHART 6: MASINT as Defined by DIA

Emitted energy (e.g., nuclear, thermal, and electromagnetic)
Magnetic properties (e.g., magnetic flux and anomalies)
Material composition
Mechanical sound (e.g., engine, propeller, or machinery noise)
Motion (e.g., flight, vibration, or movement)
Nuclear, chemical, and biological features
Reflected (re-radiated) energy (e.g., radio frequency, light, and sound)

Source: http://www.wikiwand.com/en/Measurement_and_signature_intelligence.

CHART 7: TYPES OF SENSORS

AIRBORNE	CURRENT
ELECTRO-MAGNETIC	CURRENT
VAPOR EMISSIONS	CURRENT
UNDERGROUND (SEISMIC)	CURRENT
RF-CONTROLLED	CURRENT
UNDERWATER	CURRENT
CYBER/GRID	PROPOSED (for CYBERDEFENSES)
DATA CENTERS	PROPOSED (for CYBERDEFENSES)
CLOUD MONITORS	PROPOSED (for CYBERDEFENSES)
NETWORK MONITORS/ TRAFFIC MONITORS	PROPOSED (for CYBERDEFENSES)

former television series "CSI: Crime Scene Investigation." This emphasizes how *MASINT* depends on a great many sciences to interpret data. (Source: http://www.wikiwand.com/en/Measurement_and_signature_intelligence).

We need to add more coverage and types of sensors (see Chart 7) to the electronic side of warfare and not just the traditional side in order to have complete coverage of this new "collage of intelligence."

James Carlini is a visionary and strategist for mission-critical networks, technology, and intelligent infrastructure. He has been president of his own research firm since 1986. He is the author of LOCATION LOCATION CONNECTIVITY: Next-Generation Real Estate, Intelligent Infrastructure, Technology, and the Global Platform for Commerce *(published 2014). Carlini, who holds an MBA degree, is a former award-winning adjunct faculty member at Northwestern University in both the executive master's and undergraduate programs (1986-2006), developing and teaching courses in technology management, team dynamics, Six Sigma, network security, and international applications of technology. He also has served as an expert witness in civil and federal court on mission-critical networks and infrastructure. His original "Platform for Commerce" definition of infrastructure and its impact on economic growth was written in a 2009 white paper for the U.S. Department of Homeland Security, titled "Intelligent Infrastructure," and was later adopted and referred to in the U.S. Army Corps of Engineers handbook,* Infrastructure and the Operational Art *(2014) and its 2016 publication of* Infrastructure in Subpopulations. *He has written frequently for* AIJ *in the past. Carlini served in the Air National Guard and the U.S. Army Reserves for thirteen years (1972-1985).*

Global Battlefield 2030:
The Rise of Combat Science and Technology

by Dr. (BG, USAR) Irene M. Zoppi

Imagine that today is October 24, 2047. About nine billion people live, consume, and fight for the planet's resources. China is the leading economic superpower with maritime lordship over the unfrozen Arctic Ocean. Panama and Costa Rica boast Chinese-constructed mega-canals and Brazil Chinese-built railroad cargo networks from South America's coasts on the Pacific and Atlantic Oceans, which transport goods to/from Africa and Asia.[1] The United States is now the second economic superpower followed by India, Russia, and the United Kingdom, which control multi-monetary systems. For energy, technologies such as wind, solar, and nuclear fusion have replaced electrical power. Science and technology (S&T) drive the U.S. way of life and its defense. To this end, the military industry adapts to the rise of S&T to obtain the technologies that have transformed warfare. The new nature of war is cybernetic—a continually unpredictable global technological battlefield plagued with small conflicts involving hybrids of state and non-state adversaries.

The new nature of war is cybernetic—a continually unpredictable global technological battlefield plagued with small conflicts involving hybrids of state and non-state adversaries.

Over the next several decades, science and engineering[2] will accelerate their functional diversification beyond human imagination.[3] From unmanned flying drones' artilleries with laser-powered reconnaissance and surveillance systems to driverless bombs, we witness the use of virtual teams equipped with enemy recognition systems using artificial intelligence weaponry structures.[4] Other cyber-attacking robotic networks and 3D printer-made air, land, and sea armaments link to humanoids to serve as combat multipliers. Humanoids also can code/decode more rapidly than humans, which supports the claim that the cost of technology innovation outweighs global battlefield failure. In this article, I address prioritizing investment in Army S&T.

S&T modernization will rise, but at a high cost to the defense budget.

Prioritizing the next 10 to 30 years of the Army's investment in the cutting edge of S&T entails systematic force modernization, structure, readiness, and a rigorous budget.[5] Analytically projected upgrades require scientific alignment with the Army's S&T strategy and linked to the Army's S&T enterprise, therein connecting research and development (R&D) institutions, S&T laboratories for testing, and private-industry pipelines with endowed scientists and engineers. Thus, S&T modernization will rise, but at a high cost to the defense budget. Consequently, acquisition strategies require an overhaul with adaptation to the speed of S&T innovation. Wary debates of political and legal issues will necessitate up-to-date diplomacy on the part of senior leadership.

As the Army's fighting capabilities become marginalized due to the dearth of transformation, mid-term modernization will surge. Hence, mid-term private industry partnerships will revolutionize combat power technology in competition with emerging peer threats in the global landscape. As a result, the era of the "silver bullet" with unlimited resources is over. Force XXI modernization takes shape through a precedence format of near-term (10 years), mid-term (20 years), and long-term (30 years) development driven by S&T priorities. These priorities aim at reinvestment by leveraging innovative mechanisms and expanding financing options with projective action.

First, we should invest in S&T for military energy security. Innovation exists now; however, to incorporate self-sustainability, energy efficiency (e.g., green energy) and biodegradable, regenerative technologies will be costly. For this reason, power generation will be the most difficult technological hurdle. Overcoming stagnation to press forward toward conversion from, and replacement of, old technologies to new standards of eco-energy-efficient networks requires manufacturing independence,

which involves systematic and strategic coordination to "transition towards renewable and sustainable sources of energy controlled by 21st (XXI) century infrastructure."[6]

XXI innovation embraces the "whole of government" approach toward "joint partnerships" with comprehensive plans to accelerate military reform. The expectation of decision-making speed points to interagency coordination, accountability, and transparency.[7] To this end, petroleum-driven energy will be replaced by hydrogen fuel cells with idle transition when a vehicle is not in use. A modern mix of energy sources creates new pathways toward biogenetic/chemical/nuclear smart energy, wind turbines, solar panels, and electric and hybrid power with off-the-grid systems.[8] Therein, this requires the removal of old infrastructure, air-land-sea transportation, combat-ready equipment, and barracks/military housing and offices. Unfortunately, this effort is instrumental to the pre-existing structure, which must catch up with the available technology. Consequently, our current near-term military modernization policy uses the opportunistic method of acquisition—to "buy what is available and in the buying time."[9]

Second, investment in protection and survivability of human forces utilizing nanotechnology is key to retention and recruitment. At the Institute for Soldier Nanotechnologies (ISN),[10] S&T is testing body armor for ballistic protection made out of nanoengineering surfaces with magnetorheological and polyethylene glycol fluids. R&D of armored uniforms using microtechnology that supports individual soldier protection and survivability is required.[11] Ballistic rounds using both biodegradable technology and 3D-printing technology along with nanotechnology address high-level investment of human life. Although this is not new, it will revolutionize future trans-genetic smart uniforms (e.g., instant armor suit) in the next few centuries.

3D asymmetric vision with multi-satellite radio connection links intelligence units, human terrain teams, and multi-linguist elements to iCloud repositories for up-tempo C2.

Third, we must capitalize on XXI virtual teams (e.g., ghost troops)—unmanned, autonomous, agile, and adaptive to air, land, and sea employed with mounted and dismounted forces utilizing drone technology.[12] These systems provide a virtual (game-like) role that offers digitization of the battlefield. Unmanned ground/water/aerial vehicles (UGWAVs) contribute several combat applications from logistics transport to the delivery of multi-missiles, grenades, artillery, smoke, mines, chemicals, or simple reconnaissance, survey, intelligence, and surveillance.[13] For example, the Defense Advanced Research Projects Agency (DARPA) is the proponent for creating the way forward with systems having intuitive technology such as the Offensive Swarm Enabled Tactics (OFFSET). OFFSET uses UGWAVs in human-swarm teaming of 250 robots with small-unit infantry tactics.[14] Investing in virtual technology links human ingenuity to the defense industry by fostering telepresence prospects for generation XXI. Purposely, virtual tech entails first and second order of critical investment priorities.

The National Security Agency uses cryptologic systems to obtain real-time processing of data to support the warfighter, therein speeding battlefield decision-making and troop defense while preserving cybersecurity.

Fourth, R&D of advanced processing smart technologies with intuitive targeting, mobility, precision, and rapid maneuver is needed. XXI R&D[15] has advanced in the private sector with high-end patented technologies for the Intelligence Community (IC) that aim at national security informed by innovation. For example, 3D asymmetric vision with multi-satellite radio connection links intelligence units, human terrain teams, and multi-linguist elements to iCloud repositories for up-tempo C2. Mobility and precision, with rapid maneuver techs such as armed robotics[16] and hypersonic weapons,[17] also are under development. This investment links with the next priority that aims at cybersecurity.

Fifth, XXI S&T military strategy uses information technology,[18] which allows quantum computerization, cryptology, and cybersecurity to circle back to all the above-stated priorities. As new technology is in development, emerging threats such as cyber-espionage, cyber-hacking, and cyber-attacks[19] will become routine. Hence, electromagnetic transmission of classified/sensitive information over secure or unsecured networks will utilize the quantum nature of the photon.[20] The National Security Agency uses cryptologic systems to obtain real-time processing of data to support the warfighter, therein speeding battlefield decision-making and troop defense while preserving cybersecurity.[21]

Finally, companies such as SpaceX, Boeing, ViaSat, and others are partnering with OneWeb and Airbus for a multi-billion-dollar finance package bridging the S&T of orbitology with mega-satellite constellations.[22] Satellite ecosystems will convert to new biodegradable components with the regenerative capacity to sustain voice and data speed supremacy in the interconnected global system.

Global Battlefield 2030 aims at increasing combat S&T superiority.

Asymmetric war cannot be won without S&T. To this end, Global Battlefield 2030 aims at increasing combat S&T superiority. Therefore, senior military leaders will need to be ready to promote S&T for national security and defense against all known and unknown emerging XXI peer threats that disrupt our American way of life.

NOTES

[1] Irene M. Zoppi, "Global Trends 2030: Alternative Worlds," briefing slides, Reserve Officers Association-UPORFA Conference, Fort Buchanan, Puerto Rico, September 2016.
[2] Aerospace, biological, chemical, civil, computer, electrical, environmental, genetic, information, geo-technical, mechanical, nuclear/radiation, petroleum, robotic, software, structural 3-D, and language.
[3] Technology that has not even been developed yet.
[4] Often referred to as autonomous weapons systems with artificial intelligence.
[5] While maintaining current mission up-tempo and Ready Force X readiness foci.
[6] Richard Prevost, *Energy Industry*, Team Research Project (Washington, DC: Industrial College of the Armed Forces (now the Eisenhower School), Spring 2010).
[7] President Obama issued a Presidential Memorandum on August 31, 2011, and an Executive Order on March 22, 2012, to add more transparency, accountability, and certainty to the approval and review processes for major infrastructure projects for the U.S. Armed Forces.
[8] Paul Calhoun, "DARPA [Defense Advanced Research Projects Agency] Emerging Technologies," *Strategic Studies Quarterly* 10, no. 3 (Fall 2016): 91-113.
[9] Daniel Gouré, "Near-Term U.S. Army Modernization: Buying What Is Available and Buying Time, Lexington Institute, January 11, 2017. Accessed on October 21, 2017, http://www.lexingtoninstitute.org/near-term-u-s-army-modernization-buying-available-buying-time/.
[10] Founded in 2002, ISN is composed of scientists and engineers from MIT, Army, and industry partners working together to discover and field technologies that dramatically advance soldier protection and survivability capabilities, http://isnweb.mit.edu/what-is-isn.html.
[11] "Team Combines Modeling and Experimentation to Improve Microfluids," *ISN News* (February 2004), p. 5.
[12] Larry Friese, N.R. Jenzen-Jones, and Michael Smallwood, *Emerging Unmanned Threats: The Use of Commercially-Available UAVs by Armed Non-State Actors* (Perth, Australia: Armament Research Services, 2016).
[13] Michael Horowitz and Paul Scharre, *An Introduction to Autonomy in Weapon Systems* (Washington, DC: Ethical Autonomy Project, Center for a New American Security, 2015).
[14] What is DARPA? October 22, 2017, Website File, https://www.darpa.mil/news-events/2017-10-12 (accessed October 22, 2017).
[15] Samuel R. White, Jr., ed., *Futures Seminar, Volume Two: The United States Army in 2025 and Beyond: A Compendium of U.S. Army War College Student Papers* (Carlisle Barracks, PA: U.S. Army War College Press, 2015).
[16] Andrew Herr, "Will Humans Matter in the Wars of 2030?" *Joint Force Quarterly*, no. 77 (2nd Quarter 2015): 76-83.
[17] Richard P. Hallion and Curtis M. Bedke, *Hypersonic Weapons and US National Security: A 21st Century Breakthrough* (Arlington, VA: Mitchell Institute for Aerospace Studies, Air Force Association, 2016).
[18] For example, computer coding and decoding networks through robotics.
[19] For example, phones/pagers, transceivers/transmitters, and computerized systems.
[20] Cindy Hurst, "The Quantum Leap into Computing and Communication: A Chinese Perspective," *Joint Force Quarterly*, no. 77 (2nd Quarter, 2015): 44-50.
[21] Richard P. Hallion and Curtis M. Bedke, *Hypersonic Weapons and US National Security: A 21st Century Breakthrough* (Arlington, VA: Mitchell Institute for Aerospace Studies, Air Force Association, 2016).
[22] Jonathan Amos, "Satellite mega-constellation production begins," June 27, 2017, BBC News File, http://www.bbc.com/news/science-environment-40422011 (accessed October 22, 2017).

Brigadier General (USAR) Irene M. Zoppi serves as Director of the Army Reserve Engagement Cell for U.S. Army South in San Antonio, TX. She formerly was Deputy Commander for Support of the 200th Military Police Brigade at Fort Meade, MD. When not on Reserve duty with USARSO, she is Chief of Customer Outreach and Advocacy for the National Security Agency. Prior to her current assignment, she directed the NSA Academic Center of National Intelligence University, which is now collocated with NSA HQ at Fort Meade. She holds the distinction of being the first Puerto Rican female to accede to flag rank in the U.S. Army Reserve.

MASINT: An "INT" Still in Transition

by John L. Morris

FOREWORD

In June 2020, John Morris will complete 50 years of measurement and signature intelligence (MASINT) service and advocacy, from Radar and Infrared Analyst to MASINT Functional Manager for the nation. Along the way, he learned the trade well and has been a senior technical advisor to many decision-makers, e.g., the Directors of DIA, CIA, and NGA, as well as industry leaders.

Since this article is a narrative of the personal views and remembrances of the author, the intent is to keep it technically light while conveying the importance and value of this truly unique and interesting source of technical intelligence. Let us begin with two personal MASINT vignettes.

VIGNETTE #1

In the spring of 1998 I arrived at the Pentagon early one morning where I was to meet with the Director, Air Weather Service (AWS), a friend and colleague at the Air Staff, on an operational requirements topic. He had just gotten off the phone with the USEUCOM Director of Operations (J3), and he looked pretty worried. I offered to be a good listener, and it turned out to be fortuitous that we had planned to meet that day.

For several weeks U.S. air operations had been ongoing in Kosovo and their success depended first and foremost upon the accuracy of the 24-hour cloud cover predictions, provided by the Air Weather Service, and the J3 was very dissatisfied. U.S. bombers were returning to base without having delivered "bombs on target" due to unexpected cloud cover. After a short discussion about the problem, I reminded my friend of a new MASINT solution that might be helpful—an R&D sensor recently deployed for a different mission. After a short but persuasive appeal from him, I reluctantly agreed to release R&D products, without attribution to MASINT at his request, in order to support both U.S. and Allied bombing operations that were being planned jointly each morning. Working day and night for a few weeks, dedicated researchers at the National Air and Space Intelligence Center (NASIC) implemented a near-real-time processing capability and then disseminated automated weather products to AWS on a daily basis. These products were passed through AWS to EUCOM J3 very quickly; however, we never received feedback concerning their utility until after the war had concluded.

Months later, while attending a senior-level short course at Harvard University, I got a rare opportunity to get direct feedback from the EUCOM J3, who was also attending. Imagine my disappointment when I asked how useful he found the rapid MASINT support during Kosovo air operations, and he replied, "What MASINT support?" Momentarily confused, I asked how effective his weather support was. He noted that for several weeks into the war the weather support was totally ineffective; however, it dramatically improved a few short weeks after he made a telephone call to the AWS Director. Furthermore, he credited the near-real-time weather products with "significantly" shortening the air war in Kosovo and saving lives. Upon my return to CMO, I made sure that all future MASINT products would be appropriately identified.

VIGNETTE #2

While representing the Director of NGA on a visit to Australia in 2006, I stopped in for a courtesy call with the Director, Defence Imagery and Geospatial Organisation (DIGO), renamed in 2013 as the Australian Geospatial-Intelligence Organisation (AGO). He surprised me by telling me how much they "loved" and appreciated U.S. sponsorship for a MASINT R&D capability dating back to 1999. Since I had been the original program manager, I already knew that they liked it, but as these were strong words I asked him to clarify. He confided to me that a U.S. intelligence official had introduced them to one particularly relevant data set immediately after hostilities had erupted in East Timor in September 1999. That single data set, which had been overlaid onto a map of the island, was presented to the Australian Prime Minister. He studied it for a few moments and then exclaimed that he had no

idea the hostilities were so widespread throughout East Timor. Up to that point, he had been dependent upon local human reporting which was very unreliable due to disruptions in communications on and from East Timor. I will never know for sure, but it was inferred this was the deciding factor in the committal of forces to East Timor under a UN resolution. This was of particular interest to me since I was that U.S. intelligence official (Director of the Central MASINT Organization) who hand-delivered the data in 1999 after an urgent request from the Direct of Central Intelligence (through the DIA Director) to me.

INTRODUCTION

Measurement and signature intelligence (MASINT) is an intelligence source that was born out of necessity and a strong sense of national urgency shortly after World War II. Although the term "MASINT" was not coined until the mid-to-late 1970s, its roots and motivation were clear from the early days of the arms race with the former Soviet Union. Four Soviet events after World War II caught the attention of the world and focused U.S. intelligence priorities for the next five decades:

August 1949	Soviets exploded atomic bomb—the Cold War began.
November 1955	Soviets tested hydrogen bomb—more suitable for delivery by missile.
August 1957	Soviets demonstrated first successful test of an ICBM-capable missile.
October 1957	Soviets successfully orbited Sputnik—the Space Race began.

The above events galvanized the fledgling U.S. intelligence agencies: CIA, DIA, NSA, and the military services (especially the Air Force). It was clear that intelligence was needed to provide more technical details in order to define fully the Soviet capabilities for U.S. policymaking, decision-making, and defense planning.

WHAT IS MASINT?

First, for those who have tried to define MASINT as that which was left over after subtracting SIGINT and IMINT from the world of intelligence, let me share my tongue-in-cheek rebuttal which I offered at my retirement ceremony over 27 years ago at CIA HQ:

> IMINT provides information on what your enemy wants you to see;
> SIGINT provides information on what your enemy wants you to hear;
> but MASINT discovers the secrets that your enemy is hiding from you.

I will admit that I was a little touchy at that time about definitions which started with what MASINT "is not" rather than what MASINT "is." After giving it a little more thought, I would say that MASINT augmented other intelligence sources by providing additional (and often unique) technical insight into our enemy's weapons capabilities, their operational employment, and their vulnerabilities. After all, effective intelligence production is a collaborative process, not a competition.

WHY AND HOW DID MASINT HAPPEN?

MASINT grew out of an urgent need to understand the capabilities of our adversaries to build nuclear-tipped ballistic missiles after World War II and employ them against the U.S. and our allies. Our policymakers and defense community needed more technical fidelity than traditional intelligence sources could provide. DIA, CIA, and especially the USAF played leading roles in developing technical collection and analytic methodologies that later became known as MASINT. Air Force Systems Command (AFSC) developed the technical sensors, especially those employing radar and infrared technologies, and Air Defense Command (ADC) was given responsibility for fielding and operating them. The Foreign Technology Division (FTD, now NASIC) provided assessments on the Soviet threat and offered technical advice in the acquisition phase. After deployment, FTD analyzed the data from the new collection programs to provide refined threat information to DIA and CIA.

Thus, early on, FTD was identified as the "national agent" for performing data processing, analysis, and dissemination to DIA, CIA, NSA, and the military services having intelligence production charters from DIA. The Assistant Chief of Staff for Intelligence, USAF (referred to as the Air Staff in the Pentagon), was responsible for planning, programming, and budgeting for the Air Force Technical Sensor Program (TSP), which directly supported national intelligence requirements. The Air Staff and DIA formally tasked FTD to provide program management, collection planning, and acquisition support for the TSP, as well as data processing and analysis production for all elements of the defense and intelligence communities in support of national security requirements. Early on, DIA, Air Staff, and CIA seniors were the principal policy players in forming what later became known as MASINT. FTD played a key role in developing MASINT analytics and methodologies. FTD (strong in MASINT) and CIA (strong in SIGINT) exchanged analysts to enable more effective collaboration, integration, and coordination. FTD also sent liaison analysts to DIA and NSA, and established a formal rotation to the Intelligence Community (IC) Staff. I was the first such detailee in 1974.

MASINT began with an elite workforce of scientists and engineers using advanced laboratory computing capabilities to extract unique information from new collection technologies, such as radars, electro-optics (EO), infrared (IR), lasers, wideband radio frequency (RF), and seismic and particle samplers, to name just a few. MASINT data analysts at FTD provided single-sensor and integrated multi-sensor data analysis reporting on each missile event to our weapons assessment customers (who later became known as all source analysts) at FTD, DIA, CIA, NSA, and other DIA-chartered service scientific and technical intelligence (S&TI) centers.

New MASINT analysts were expected to arrive with a good working knowledge of, and the ability to apply the fundamentals of, chemical and physical first principles involved in rocket propulsion and ballistic missile flight. Although few arrived with all of the prerequisite skills, those assigned to both signature analysis and flight reconstruction especially needed them. They got a lot of practice, and were immediately assigned a training officer, or mentor.

When I first arrived at FTD direct from graduate school with an advanced degree in electrical engineering, I was quickly challenged by my new supervisor, an Air Force major, with a phased array radar data tape awaiting me at my desk. He advised that I was to determine the hypersonic ballistic coefficient of the newest Soviet ICBM reentry vehicle, which housed the nuclear warhead, from the radar data. Due to my blank stare, the major said quite simply, "Figure it out, lieutenant; you're an engineer." He did take pity and gave me a reference book to help in understanding flight dynamics. It was a translation of Germany's V-2 missile development program—design equations, structural design, Keplerian orbital mathematics showing trajectory trade space, reentry drag curves and, thankfully, a technical description of hypersonic ballistic coefficients (with a hint on how to calculate them). The book was a very large and thick compendium of blue-lined pages, published in Stuttgart, Germany, in 1953 (long before the modern copy process was invented). I still own and treasure that book today.

MASINT analysts became a close-knit group, but no one was afraid to go to the chalkboard to explain and defend his analysis among peers. Due to remote sensing phenomenology of the new technologies, an ever-expanding suite of collection sensors emerged: Radar—line of sight, bi-static, over the horizon, synthetic aperture (SAR), long-range imaging; EO/IR active and passive sensors—imaging/non-imaging, thermal, multispectral, hyperspectral, ultraspectral, radiometric, polarimetric, and others. We never stopped learning.

Due to the timelines needed for in-depth processing and analysis, policymakers and DOD weapons developers were our initial customers. Decades later, as computing techniques progressed, computer sizes decreased, and communication bandwidth increased, the warfighter emerged as a major user of MASINT.

HOW DID MASINT EVOLVE?

Soviet nuclear weapon testing and ballistic missile development generated critical requirements for technical intelligence capabilities to characterize this new threat and provide warning against attack. Therefore, motivation was very high. Soviet weapons testing was continuous during this development cycle. Ballistic missile testing, however, was even more prolific and widespread with testing throughout the Soviet Union. Hence, the opportunities for refining collection and exploitation capabilities abounded. Early on, missile technology derived from numerous captured German V-2s and was the foundation for Soviet strategic missile development, especially short- and medium-range ballistic missiles.

The following is a brief history of the deployment of some of the MASINT technologies and events that contributed to where we are today. It is not meant to be complete, but it is representative:

Time Frame of Events and Activities

Late 1950s

Seismic and Sound Surveillance System (SOSUS) networks were under way.

Fixed-beam "fan" radars were deployed for missile surveillance.

Mid-1960s

Seismic and SOSUS network continued to expand.

Air sampling flights became operationally routine.

Over-the-horizon (OTH) radar was used for missile warning.

Missile warning mission sparked debate on radar vs. infrared for reliability.

Missile from space was detected with first IR experiments.

Precision single-beam tracking radars were deployed.

Late 1960s

RC-135 surveillance aircraft were operationally deployed.

Airborne phased array radar began operations but crashed within a year.

Advanced range instrumentation ships (ARIS) with single-beam tracking radars were deployed.

Early 1970s

Air Force launched the first operational Defense Support Program (DSP) early warning satellite.

- The DSP constellation operated by ADC from three different ground sites in Australia, West Germany, and Colorado.
- FTD developed and provided missile signatures and profiles that were used for target classification: ICBM vs. MRBM vs. IRBM vs. space launch.
- FTD also developed intelligence reporting from DSP during the first year.

Large aperture long-range imaging radar was developed for space object identification.

Digital airborne spectral EO deployed to characterize missile re-entries.

Ground-based air sampling was conducted.

OTH radar added ranging capability.

CIA/DIA/USAF established radar and optical intelligence (RADINT/OPTINT) Working Group (ROWG).

- IC-wide membership and participation emerged.
- FTD chaired the ROWG and provided analytic standards and documents.

In 1973 the DCI stood up the first IC Staff at CIA.

- Initial focus was on collection and processing assessment, analytics and production, and budget and programs. Integration was added later.
- Manning was by permanent CIA employees, detailees from industry as temporary government employees, and detailees from other government agencies. After being interviewed in late 1973, I was selected and reported as a detailee in early 1974.
- SIGINT, IMINT, and HUMINT committees were added shortly afterward to establish formal collection requirements and priorities.

Mid-1970s

The term "MASINT" was coined by DIA, Air Force, and CIA.

DIA established the Measurement and Signature Data Requirements (MASDR) system to document and prioritize collection requirements.

USAF (FTD) and CIA exchanged MASINT analysts and began to exchange data formally (and informally).

FTD seniors agreed to divide infrared exploitation internally.

- Banded IR went to MASINT.
- Spectral IR went to SIGINT.
- CIA and others followed the FTD alignment paradigm.

Ship-based phased array tracking radar was introduced.

LANDSAT satellite-based VIS/NIR/SWIR/TIR was deployed.

Special studies began on thermal IR and SAR.

Early 1980s

Airborne SAR experiments began.

Airborne thermal experiments began.

Airborne laser intelligence experiments began.

Ship-based X-band precision tracking radar was developed and deployed.

Mid-1980s

MASINT Sub-Committee was stood up initially under SIGINT in 1983.

MASINT proved itself and became permanent DCI Committee in 1986.

Laser Intelligence (LASINT) was realigned to MASINT.

NASIC developed detailed modeling and simulating for missiles and lasers.

LASINT vs. missile tracking "shootout" (CIA vs. USAF).

Airborne MSI experiments began.

NASIC formed end-to-end MASINT Directorate.

Late 1980s

Thermal and SAR began in earnest.

"Non-literal imagery" term was coined.

Early 1990s

We won the Cold War—Congress made plans for a "peace dividend."

- Major national MASINT program was cancelled.
- USAF Tech Sensor Program began to be dismantled.
- SOSUS fell into disrepair.
- MASINT was cut disproportionately.

DCI decentralized intelligence management and assigned it to stove-piped agencies.

Central MASINT Office (CMO) was chartered by DCI (DCI directive) and SECDEF (DOD instruction).

- Functional Manager for national and defense MASINT.
- Independent research budget to stimulate DoD/IC investments.
- Reported through DIA Director, but with DoD/IC manning and resources.
- MASINT Committee subordinated to CMO.
- Centrally managed, with decentralized execution due to lack of resources.

Mid-1990s

Congress began to take an interest in MASINT.

CMO expanded and accelerated hyperspectral exploitation development via dozens of formal agreements with academia, industry, and other agencies.

DCI established the Environmental Task Force (ETF) in mid-1990s at request of Senator (later Vice President) Al Gore.

- Explored the utility of intelligence and defense technologies to assist in observing the environment and assisting environmental scientists.
- Up to 60 U.S. environmental scientists were granted security clearances, briefed on IC technical collection capabilities, and allowed to identify experiments to address environmental issues. The IC capability owners then proposed IC-executed team projects to address the issues.
- Four MASINT experiments were approved and executed by NASIC.

Late 1990s

DCI-DOD redesignated CMO as Central MASINT Organization.

- Clarified authority inside DIA as a key component, DIA/CM.
- Strengthened CMO as national MASINT Functional Manager.
- Increased overall manning and funding almost five-fold.
- Ensured that CMO would be directly represented in all DOD & IC decision-making meetings, co-equal with other INT functional managers.

Strengthened MASINT "branding" to clarify roles with other INTs.

- Imagery-related MASINT, RF MASINT, SAR MASINT, EO MASINT.

DOE SNL developed and deployed Thermal Spectral Imager.

Thermal, MSI, and SAR exploitation began to mature but faced resistance.

Congressional interest continued as MASINT began to mature.

Term "Imagery-derived MASINT" (IDM) was officially coined.

CMO demonstrated utility of IDM.

Early 2000s

Terrorist attack on 9/11 was a turning point for MASINT.

IDM "came of age" in OEF and OIF.

IMINT DCI directive was updated; IDM was realigned to NIMA (now NGA).

NIMA Director established Senior MASINT Advisor as a direct report:

- Assist all senior leaders and managers to understand IDM.
- Facilitate effective integration of IDM into new GEOINT operations.
- Identify/train/mentor new leaders to sustain and advance AGI utility.

- Ensure NGA planned and maximized service component participation.

IDM was relabeled as Advanced Geospatial Intelligence (AGI) in early 2003.

- Defined as spatial, spectral, radiometric, polarimetric, phase history, temporal, and related calibration data for both stationary and moving targets.

DIA disestablished CMO and formed DIA/DT, which integrated remaining MASINT functionality with other collection operations to focus on defense and deemphasize national signatures.

Mid-2000s

MASINT and GEOINT were redefined by DNI to reflect organizational reassignments of IDM (now AGI).

AGI continued to be associated with the MASINT community, primarily due to influence of the military service components and commonality in technical application of observable phenomenology.

Late 2000s

NGA retired the term "AGI" and totally merged it into GEOINT.

Due to partnership with the National Air and Space Intelligence Center (NASIC, formerly FTD) for exploitation, spectral innovation has become known for rapid advances in operational applications.

DIA/DT resources were restructured into DIA/ST and refocused mostly to science and technology as applied to different classes of weapons systems.

DIA formally stood up a new MASINT management structure.

- DIA Director as MASINT Functional Manager and chairman of a MASINT Senior Executive Council, with IC-wide agency directors as members.

A new national MASINT management office was established under the DIA Director to assist and staff his national MASINT Functional Management responsibilities.

MASINT execution is now federated, for the most part.

ORGANIZATION AND MANAGEMENT

The sub-disciplines of MASINT were developed and evolved independently over several decades in the 1947-1970 time frame. Since budgets were very limited and these forward-thinking entrepreneurs were often competing with each other, governance and organization were challenges from the very first. All of the other national INTs had management and organizational structures through existing agencies and budget lines, but MASINT did not even have a name at that point. MASINT sub-disciplines each had their own advocates, but few had real budget support from the major agencies. Although DIA was the "founding" agency, its budget was almost totally operations and maintenance (O&M) funding. MASINT required research and development funding, procurement funding, and O&M funding.

Two things occurred to force some decisions in the early 1970s: (1) the Soviets were outbuilding the U.S. in technologically-evolving ICBMs, and (2) the Space Race was neck and neck. In 1973 newly-appointed DCI William Colby, although overburdened with the Watergate investigations in Congress, approved the stand-up of the first dedicated Intelligence Community (IC) Staff, chartered to provide structured oversight, coordination, and a foundation for informed decision-making for the entire IC. The motivation for organizing MASINT came from DIA, CIA, and the Air Staff, but the forum for accomplishing the task was the IC Staff.

During the 1970-1983 time frame, DIA, CIA, NSA, and the Air Staff signed formal individual and collective agreements, exchanged data and personnel, and began the process to formalize national MASINT. The DCI established a MASINT Subcommittee in 1983, with administrative support from the SIGINT Committee, as a trial organization. The trial was declared a success, and the MASINT Committee formally stood up as a full DCI committee in 1986, with a permanent staff and membership from all military services and IC agencies.

The MASINT Committee (MASCOM) was responsible for gathering formal user requirements into a national database, prioritizing the requirements, and giving direction to collection agencies in a federated construct. MASCOM also determined future collection and exploitation needs in support of the DCI's budget process and advocated for capabilities. This process continued until the DCI decided that it was no longer necessary to micromanage the IC. In late 1992, the DCI distributed the national single-INT committees to the respective functional agents: HUMINT went to CIA, SIGINT went to NSA, IMINT went to the Central Imagery Office (later to become part of NIMA), OSINT went to CIA, and MASINT

went to the Central MASINT Office (which was assigned to DIA). The Chairman of MASCOM became the Deputy Director of CMO.

In 1998 the DCI was apprised of the fact that CMO was woefully under-resourced to oversee and functionally manage an assemblage of national and defense budgets that was executed through at least four military services and six national-level defense agencies. At that point, the DCI strengthened and retitled CMO as the Central MASINT Organization, significantly increased manning and resources, and established more senior positions so that CMO could participate in various national decision-making forums on an equal basis with NSA (SIGINT), NIMA (IMINT), and CIA (HUMINT). In addition, the Director of CMO added a second hat as the director of DIA's newest key component, DIA/CM, and through that responsibility continued to report to the DIA Director. During this period, CMO demonstrated a number of new technologies that transitioned to the military services and other agencies. This was exemplified by the transition of imagery-derived MASINT (renamed AGI) to NGA during the 2003-2005 time frame. Since that transition, DIA has managed MASINT as a federated system, for the most part, executed by the military S&TI centers within the general defense intelligence program.

THE FUTURE FOR MASINT

First and foremost, the threats that challenge our nation are getting more complex and widespread. They require the most advanced technologies and agile approaches for solutions. MASINT has always been known as the most technical of the INTs and has a long history of rapid innovation. Once it demonstrates a breakout technology, then everyone wants it. Let us accept for a moment that is a very good transition plan for the following reasons:

(1) Acquisition procedures for research and development (R&D) allow for much shorter timelines to implement. An example is the R&D demonstration system referenced in the two vignettes, which was a 24-month acquisition program. Operational systems take at least three to four times longer for their acquisition.

(2) Pathfinders and demonstration programs are much less expensive because they are planned for shorter periods of performance and more risk is acceptable. Operational systems, on the other hand, require more redundancy and testing to reduce risk to an operational mission; however, the lengthened acquisition drives up costs even more due to the mismatch with the computer technology cycle of 18-24 months. After deployment, operational systems require expensive periodic upgrades and continue to have escalating annual O&M annual costs as the aging equipment goes out of inventory. This leaves little funding available to initiate other advanced technology programs.

(3) This type of transition plan lends itself well to the current federated execution process that the Defense Intelligence Agency has established with the military services and the other defense agencies.

From the history laid out in this article, one can see that MASINT, as an organizational construct, has been in transition for several decades. This will undoubtedly continue to evolve over time. Regardless of future organizational changes, however, **measurement and signature intelligence has proven to be a "go to" intelligence source for addressing the most challenging national security problems of the United States**. Anyone who chooses this career path will find it very rewarding and have a lot of fun along the way.

John L. Morris is currently the President and CEO of his own consulting firm. He has spent his career in various, and ever increasingly responsible, positions in MASINT across the national Intelligence Community. Starting his career at a well-known defense contract company, he was a test engineer. He subsequently graduated from Southern Methodist University with a Master of Science in Electrical Engineering and was commissioned a second lieutenant in the Air Force. He was posted to the Air Force Foreign Technology Division, now the National Air and Space Intelligence Center (NASIC) in Dayton, OH. He held multiple MASINT positions at NASIC, culminating in his promotion to MASINT Technical Director. Joining DIA in 1995, he became the Director, Central MASINT Organization (CMO), as well as the MASINT Functional Manager. In 2000 he moved to CIA as Deputy for MASINT, Imagery, and Space Activities. Next, he became the Technical Advisor for MASINT and OPIR (Overhead Persistent Infrared) to the Director of NGA. Retiring from the Senior Executive Service, John worked at another research company as its Chief Scientist and Vice President. He is a noted author and expert on all things MASINT, and continues to consult on various MASINT and technical intelligence issues within the IC and the national security community at large.

Underappreciated, Underrepresented: Thoughts on Teaching MASINT

by Dr. John D. Sislin

INTRODUCTION

The Mayan empire flourished during the 3rd to 10th centuries, in parts of Mexico and Central America. The Mayans built complex cities, with multiple and varied plazas and buildings. After the 10th century, the civilization declined and the jungle reclaimed the now-vacant cities, many completely disappearing from sight. In 2018 more than 60,000 structures were discovered in Guatemala, using Lidar (Light Detection and Ranging). This sensor, often mounted on an aircraft, remotely scans the ground using a laser and measures energy reflected off an object (e.g., the ground or man-made objects) to create a very high-resolution, three-dimensional representation of objects.[2] Well illustrated in this case was the Lidar sensor's ability to pierce dense foliage. An archaeologist participating in the study noted he had been standing within 150 feet of a fortification wall, identified by the Lidar sensor, and never saw it.[3] Lidar is one example of a sensor used to collect information as part of Measurement and Signature Intelligence, or MASINT. MASINT is an underutilized and underappreciated method of collecting intelligence; demystifying the subject could aid instructors, students, and researchers in exploring some of its valuable capabilities.

MASINT is one of five collection disciplines or "INTs," which include open source intelligence (OSINT), human intelligence (HUMINT), signals intelligence (SIGINT), and geospatial intelligence (GEOINT).[4] MASINT, which is managed by the Defense Intelligence Agency (DIA),[5] is defined as:

> Technically derived intelligence (excluding signals intelligence and traditional imagery intelligence) that, when collected, processed, and analyzed, results in intelligence that locates, tracks, identifies or describes the signatures (distinctive characteristics) of fixed or dynamic target sources. It includes the advanced data processing and exploitation of data from overhead and airborne imagery collection systems. MASINT data can be acquired from a variety of satellite, airborne, or shipborne platforms; remotely piloted vehicles; or mobile or fixed ground-based collection sites. Its sensors include, but are not limited to, radar, laser, optical, infrared, acoustic, nuclear, radiation, detection, spectroradiometric, and seismic systems, as well as gas, liquid, and solid materials sampling systems.[6]

A more concise definition is given by John L. Morris, former Director of the Central MASINT Office. MASINT is "technically derived intelligence that detects, locates, tracks, identifies, and describes the specific signatures of fixed and dynamic target sources."[7] [Editor's Note: See separate article in this volume by Mr. Morris, considered one of the IC's experts in this discipline.] Perhaps the foundation of MASINT, as expressed in its name, is measuring a characteristic of a target (e.g., radiation, vibration, etc.) and then comparing that known characteristic to a library of signatures, which allows for a target to be identified and further described. For example, a missile may be identified by comparing certain measurements with a database of missiles. Sensors, which are used to collect those measurements, are typically grouped into six sub-disciplines: radar, geophysical, material sampling, nuclear radiation, electro-optical, and radio frequency.[8] Those sensors are associated with a variety of platforms, including space-borne, airborne, ground-based, underwater, or underground platforms.

MASINT, as a discrete subject, is currently not commonly found within intelligence studies programs in the U.S., based on a review of such programs' course catalogues. GEOINT, HUMINT, OSINT, and SIGINT courses seem to be more common. However, many intelligence studies programs in the United States include a course on intelligence collection in general—collection being a major component, and a fundamental part, of the intelligence process. Adding more material on MASINT is possible.

MASINT may be an understudied subject for several reasons. Intelligence studies programs as a whole encompass many differences, which include serving diverse student populations, offering different credentials (from an intelligence studies minor or certificate to a PhD), and varying widely in terms of organizational resources.[9] Given MASINT is just one piece of intelligence collection, which is in turn one piece of intelligence studies, it is not surprising that it is not as common as intelligence analysis courses, for

instance. In addition, though, there may be a mistaken view that MASINT is difficult to teach: the materials are all classified, its value is more difficult to determine, it does not have the same currency as other INTs, it is technical and confusing, and it is undervalued by the Intelligence Community (IC) and therefore less important to the curricula. This article seeks to make the case that MASINT is not nearly as problematic a subject as these misperceptions suggest. MASINT is in fact relatively easy to incorporate into intelligence collection courses and can be used to examine a wide variety of themes and stimulate student discussion and learning.

This short essay is organized around and addresses five myths about MASINT that have hindered its inclusion in academic discussions of intelligence. Although the essay is unlikely to convince anyone to create a stand-alone course on MASINT, it may inspire instructors to consider adding more MASINT material to existing courses. For readers who are new to this discipline, the article offers a number of fundamental topics on MASINT (which could make up a lecture) including its definition, sub-disciplines, underlying sources of information, organization and management, applicability, strengths and weaknesses and, to a lesser degree, the future of MASINT collection.[10] For readers who are familiar with MASINT, they may share the author's surprise at the amount and variety of publicly available information on this INT and may perhaps be inspired to delve into the topic with more specificity and depth. Each INT brings its own strengths and weaknesses to the table and each INT is more or less appropriate for different targets. Including at least a short discussion of MASINT is appropriate to a well-rounded discussion of intelligence collection, within intelligence studies.

FIVE MYTHS

Myth #1: It is difficult to teach MASINT; all the good stuff is classified.

Much of the information about intelligence collection specifically, and intelligence studies generally, is classified. It is of course true that various programs, targets, sources, and methods are justifiably classified. Additionally, the more current the information, the more likely it is to remain classified. Armin Krishnan asserts for instance: "The U.S. Government does not—in some cases—even acknowledge the existence of certain collection systems and methods" and "there is great scarcity with respect to official information on current capabilities for technical collection and analysis."[11] The second argument is not new. Michael Handel wrote in the 1980s that new knowledge will be acquired through "historical case studies rather than on contemporary events."[12] Krishnan goes one step further and asserts, "A course on technical intelligence cannot rely exclusively on official documentation since most of it is classified and not available for use in an academic program."[13]

For several reasons, this pessimism is not always justified. First, some part of each of the INTs—even OSINT—is classified. People do not seem to be surprised that HUMINT takes protecting sources and methods very seriously, and students may resort to picking up examples of tradecraft, probably erroneously, from movies or spy novels. This does not prevent offering a course on HUMINT, however, which can discuss actual historical cases of espionage or themes, such as the ethics of spying. Some intelligence studies programs even have entire courses devoted to HUMINT, such as the Institute of World Politics and American Military University.[14]

Second, much material on MASINT, including programs and general missions, is publicly available. Those who study MASINT are fond of listing a variety of platforms to illustrate the range, in a positive sense, and the lack of coherence, in a negative one, of the collection discipline. Discussing the six sub-disciplines (radar, geophysical, material sampling, nuclear radiation, electro-optical, and radio frequency) thus often informs a large part of the discussion on MASINT. Fortunately, examples of the six sub-disciplines are fairly easy to locate. Sufficient variation among them facilitates instruction on both historical and contemporary sensors and platforms, as well as U.S. and foreign tools. These examples illustrate that it is actually surprisingly easy to discuss, compare, and apply this part of the MASINT discipline in the classroom. An important point is that just flinging platform examples at students is probably not that useful.[15] From the U.S. IC point of view, the reason for having a spectrum of platforms is to create a toolkit from which to choose the best platform to answer the intelligence question being addressed. From a teaching point of view, platforms can illustrate several themes and allow for a series of comparisons and subjects for class exercises, in which students reflect on how they might use some of these tools.

Each sub-discipline is explained in more detail below in a way that can be discussed in an academic setting:

Radar. Radar systems are an active collection method where an energy pulse, consisting of high-frequency radio waves, is transmitted from the radar and, if it strikes an object, some of the reflected energy may be received back by the radar and characterized.[16] Partly because radar is such a ubiquitous technology, there are many examples that an instructor could draw upon in a classroom discussion. It is also possible to compare and contrast different radar systems. Three examples illustrate just a few of the possibilities.

A first example of a radar system is the AN/FPS-108 Cobra Dane. Cobra Dane is a phased-array radar, located at Eareckson Air Station in Shemya, Alaska.[17] The radar, which is operated by the U.S. Air Force, achieved initial operating capability in 1977.[18] The large structure—the roughly circular face is 95 feet in diameter—has an operational range of about 2,000 miles.[19] It had a very specific initial mission—it was built to collect intelligence in support of verification of the strategic arms limitation treaties between the United States and the USSR, but this mission has broadened since the end of the Cold War. At various times, Cobra Dane missions have included collecting data on foreign ballistic missile events and conducting space surveillance.[20]

Contrasted with Cobra Dane is Cobra King, a ship-based, mobile platform, which is located on the USNS *Howard O. Lorenzen*. The radar system, consisting of S- and X-band phased radars, became operational in 2014.[21] The two radars, located toward the stern of the ship, work hand in hand: the "S-band radar is specifically used to search and acquire the target, and then hand it off to the X-band, which provides high resolution target characterization."[22] The system is also designed to support treaty monitoring activities, such as START. A main advantage of the ship is that it can sail to areas where it can carry out its mission. It also illustrates cooperation among the U.S. military services, in this case elements of the U.S. Navy (which operate the ship) and the U.S. Air Force (which operates the radar system).

A final international example is the Jindalee Operational Radar Network (JORN) in Australia. This system, comprising three over-the-horizon radar systems (OHTRs), is operated by the Australian Defence Forces.[23] Each OTHR includes a large, fixed transmitter and an array of also large receiver antennas. The first OTHR in the Network was installed in 1974, after which the two additional radars were built and the Network underwent a variety of upgrades. The Network serves a few purposes, as noted by the Australian Department of Defence Science and Technology Group: "24-hour military surveillance of the northern and western approaches to Australia, but [it] also serves a civilian purpose in assisting in detecting illegal entry, smuggling and unlicensed fishing."[24] OTHRs are designed to collect against targets that are located thousands of miles away, out of the line of sight between a radar and its target. JORN radars have an operational range of 1,000 to 3,000 km.[25] By bouncing high-frequency (HF) radio waves off the ionosphere, some of this energy may perchance strike a metal target, and some of the energy that strikes the target may return to the radars' receivers. In this way the target is detected. The JORN radars can detect large aircraft and ships; however, the Network can be affected by the condition of the ionosphere or environmental conditions (for example, it is more difficult to locate a ship in rough seas), as well as by the nature of the target.[26]

Geophysical. Geophysical MASINT focuses on collecting acoustic information (both audible and infrasound) transmitted through the air, ground, or water. Sound can be created by vibrating objects or pressure waves. In addition, this sub-discipline includes measuring variations in the strength or direction of the magnetic field, which can be done, for example, with a magnetometer. This can be a useful strategy for detecting submarines underwater, a method that dates back to just before—and was used by the military during—World War II.[27] A more modern problem is clandestine, underground nuclear testing.

As international treaties have restricted nuclear testing, the one method people feared noncompliant nations might try would be to hold an underground test. Fortunately, such tests resemble earthquakes, which are already monitored by seismic sensors. The trick is to discriminate between the two types of events, making the challenge more of identification than detection.[28] Two different organizations collect seismic data to detect nuclear explosions as part of treaty monitoring: the U.S. Air Force Technical Applications Center (AFTAC) and the Comprehensive Test Ban Treaty Organization (CTBTO). AFTAC monitors for nuclear detonations underground, undersea, in the atmosphere, or in space using more than 3,600 sensors, including some seismic monitoring sensors—as part of the U.S. Atomic Energy Detection Systems (USAEDS), whose purpose is to monitor for nuclear treaty compliance.[29] The CTBTO runs the International Monitoring System (IMS), which consists of 321 monitoring stations and 16 laboratories.[30] These two organizations cooperate, as noted by AFTAC: "In fact, AFTAC now contributes six of its U.S.-based USAEDS seismic monitoring stations to the IMS."[31] It would be interesting to focus classroom discussion on an international organization as a MASINT collector, as well as the challenges of sharing U.S. data, in general, with other actors.

An example of an acoustic system is known as the Unattended Transient Acoustic MASINT Sensor (UTAMS). The development of UTAMS emerged from a specific need by troops on the ground in Iraq. U.S. troops were coming under fire from rockets and mortars, as well as dealing with the threat of improvised explosive devices (IEDs). The U.S. Army Research Laboratory (ARL) created an acoustic sensor for detecting these weapons. Amazingly, the system, which employed commercial off-the-shelf technology (e.g., hearing aid microphones) was conceived and built in just over two months.[32] The UTAMS is interesting as a classroom example because it is a very tactical system, which also has been deployed on aerostats and towers. A domestic example of an acoustic sensor is ShotSpotter, used in many American cities for detecting and locating gunfire and alerting police when a verified gunshot is detected.[33]

An example of a hydroacoustic sensor system is the Integrated Undersea Surveillance System (IUSS). This system is quite well-known and documented, and has been in place for several decades, though with some interesting changes. According to the U.S. Navy, the mission of the IUSS reads in part: "To support antisubmarine warfare command and tactical forces by detecting, classifying, and providing timely reporting of information on submarines and other contacts of interest…"[34] A major component of IUSS is the SURTASS, or Surveillance Towed Array Sensor System, which is a mobile component towed behind a ship. The program originated in the 1970s, though the concept was already well established. As noted by the U.S. Navy, "SURTASS consists of a long Y-shaped acoustic array that is towed horizontally behind a surface surveillance ship."[35] However, when dealing with a very quiet submarine, the Navy may turn to a Low-Frequency Active (LFA) sonar system, which is "a system of up to 18 acoustic transmitters or projectors suspended vertically by cable beneath a Navy surveillance ship."[36] Students may have heard of the LFA system, if not by name, but from open source information regarding possible negative consequences of the active system upon marine life (e.g., whales). The second major component is the SOSUS, or the Sound Surveillance System, which was first put in place in 1954 as a fixed system. SOSUS consists of undersea arrays of hydrophones on the sea floor connected by cables to processing centers on land.[37] It is worth noting that this system, due to its age, has changed over the years. The system was largely built to deal with Soviet submarines. After the end of the Cold War, that mission changed. Today, a major focus of the IUSS is in the Pacific (currently consisting of five ships), and the system is much smaller than it was prior to the 1990s.[38]

Materials. The materials sub-discipline focuses on the collection of gases, liquids, or solids. These samples are analyzed to determine their composition (e.g., chemical). An important focus of this sub-discipline is on weapons of mass destruction (WMD) and searching for and detecting biological, chemical, or nuclear materials.[39]

One example of a platform within this sub-discipline to monitor for nuclear materials is the WC-135W Constant Phoenix aircraft. According to the U.S. Air Force, this "atmospheric collection aircraft supports national level consumers by collecting particulate and gaseous effluents and debris from accessible regions of the atmosphere in support of the Limited Nuclear Test Ban Treaty of 1963."[40] Atmospheric testing is now part of the treaty verification process, although the mission predates the Constant Phoenix to the earliest times of the nuclear era, in 1949, when an Air Force plane detected nuclear debris from the first Russian nuclear test.[41] There are currently two of these aircraft in the Air Force inventory, and their missions can extend beyond nuclear weapons detection; they were used for monitoring both the 1986 Chernobyl incident in Ukraine and the 2011 Fukushima nuclear plant accident in Japan. The plane's sensors are quite interesting. According to an AFTAC spokeswoman: "The WC-135 crew of special equipment operators operate a suite of collection devices that are housed in the main body of the aircraft. One is an external flow-through device called a U1B foil. Similar to how a traditional jukebox operates, filter paper is cycled through the foil into the airstream as the aircraft flies through an area where radioactive debris may be present. Simultaneously, large high-pressure spheres collect whole air samples through an onboard compressor system."[42] In the future, the Air Force intends to upgrade three tankers into Constant Phoenix aircraft and then retire the original planes for a net gain of one aircraft.[43]

As part of its enforcement strategy, CBP uses various pieces of radiological detection equipment to help secure U.S. borders.

In contrast to the two Constant Phoenix aircraft, a more plentiful ground system (with both fixed and mobile platforms) is used by U.S. Customs and Border Protection (CBP). As part of its enforcement strategy, CBP uses various pieces of radiological detection equipment to help secure U.S. borders.[44] As noted in a fact sheet on these technologies: "An integral part of the CBP comprehensive strategy to combat nuclear and radiological terrorism is the scanning of all arriving conveyances and containers with radiation detection equipment prior to release from the port of entry. CBP's nuclear and radiological detection equipment includes Radiation Portal Monitors (RPM), Radiation Isotope Identification Devices (RIID), and Personal Radiation Detectors (PRD) for 329 ports of entry nationwide."[45] This is a good, practical example because it focuses on Homeland Security as a MASINT application.[46]

Nuclear radiation. This sub-discipline focuses on nuclear radiation and phenomena "associated with nuclear weapons, processes, materials, devices, or facilities."[47] Unlike in the geophysical sub-discipline—which also focuses on nuclear material—here the focus is on detecting gamma rays, x-rays, and neutrons. The primary example of a MASINT system designed to collect nuclear radiation is the United States Nuclear Detonation (NUDET) Detection System, or USNDS. The purpose is to detect, locate and characterize nuclear detonations that occur in the atmosphere or space.[48] This is a joint undertaking involving the Department of Defense, through the U.S. Air Force, and the Department of Energy, through the National Nuclear Security Administration (NNSA). This is a space-based system that began in 1963 with the launch of Vela satellites. Currently, the United

States has sensors on GPS satellites, among others. The USNDS is meant to operate within the larger USAEDS, previously mentioned under the geophysical sub-discipline.

Electro-optical. The electro-optical sub-discipline includes sensors that examine the reflected or emitted energy from the optical portion (infrared, visible, and ultraviolet wavelengths) of the electromagnetic spectrum. There are three types of non-literal EO that can be collected: infrared (IR), laser, and spectral. These sensors have been mounted on both airborne and space-borne platforms. IR sensors collect emitted energy in the infrared part of the electromagnetic spectrum, or radiant heat coming from a target. Laser collection is an active method of remote sensing that makes use of pulses of laser light directed at a target. The time it takes for the pulse to return to the sensor provides information regarding the surface of the target. Lidar, discussed in the introduction, is one example.[49] Finally, spectral sensors take advantage of the fidelity of examining tiny slices of wavelengths of the electromagnetic spectrum. Sensors that examine a few clusters of such wavelengths, such as red, green, or blue frequencies, are termed multispectral, while sensors that capture tens, hundreds, or thousands of frequencies are known as hyperspectral.

Cobra Ball is an example of an IR collection (airborne) platform.[50] The aircraft, the RC-135, has a long service history, dating back to the 1960s. There are a number of variants of the aircraft, with different letter designations—RC-135S is the Cobra Ball program; other versions of the aircraft participate in SIGINT, or more specifically in ELINT, collection activities. The RC-135S originally operated out of Eareckson Air Station (formally known as Shemya Air Force Base) in Alaska, but in 1994 "all RC-135S aircraft and operations were transferred to the 55th Wing at Offutt AFB in Omaha, Nebraska."[51] There are currently three aircraft. According to the U.S. Air Force, Cobra Ball "flies Joint Chiefs of Staff-directed missions of national priority to collect optical and electronic data on ballistic targets. These data are critical to arms treaty compliance verification, and development of U.S. strategic defense and theater missile defense concepts."[52] For example, the aircraft have been used recently to monitor North Korean missile activities.[53] Classroom discussion can take a few different forms using this particular platform. First, this is a good example to talk about risk-taking. These aircraft fly in peacetime missions on the peripheries of countries, but are still challenged by other aircraft and there is the danger of loss of aircraft.[54] Second, this is an opportunity to discuss criteria for picking the best platform for the mission at hand. Third, one of the challenges with MASINT is that some platforms are essentially "one-offs," while others are long-standing. Cobra Ball fits on the latter end of that spectrum. Finally, it may be possible to discuss at least briefly the issue of the future of MASINT. The RC-135 aircraft are old. The Air Force needs to decide, in light of Cobra Ball's mission, whether some platform should replace the aircraft, and what that platform would look like in the future.[55]

Hyperspectral imagers may be mounted on both aircraft (manned and unmanned) such as the Airborne Visible/ Infrared Imaging Spectrometer (AVIRIS) flown on NASA's ER-2 jet, among other aircraft, and on satellites.[56] Two recent examples of sensors that can carry out hyperspectral imaging (HSI) are from India and China.[57] India's example is the Hyperspectral Imaging Satellite (HysIS), launched by the Indian Space Research Organisation (ISRO) on November 29, 2018.[58] China's satellites are the Jilin-1 and the Spectrum 01 and 02. (Jilin-1 is the name for a constellation of remote-sensing satellites that feature different types of sensors. The Spectrum satellites are part of this constellation.) The two Spectrum satellites were launched on January 21, 2019. According to the manufacturer, the commercial satellites have a resolution of 5m and collect on 26 spectral bands.[59] HSI systems are particularly well-suited for civilian applications such as environmental monitoring, agriculture, and land usage monitoring, among others.[60] HSI is an interesting category of sensors, from a development perspective. Governments may build different types of remote-sensing satellites for national security purposes. Companies, on the other hand, probably must find some way to profit from a new sensor. While panchromatic and multispectral imaging satellites are common in the commercial world, it is unclear if HSI will be seen by companies as a tool that can make money; companies may end up uninterested in this sensor.[61] In one of many examples of a comparison among the sub-disciplines, in the case of Cobra Ball it is the platform that is the issue for the future; here it is the sensor.

Radio frequency. Radio frequency energy can be emitted by most electronic products.[62] Some products, such as older electrical power tools, might emit RF energy incidentally or not by design. A second group of products, such as personal computers or printers, might emit RF energy unintentionally. Here, the RF energy is "leaking out" of the product. Finally, some products radiate RF energy intentionally. This category includes Wi-Fi transmitters or Bluetooth radio devices.[63] A challenge for the military, law enforcement, and the IC is detecting improvised explosive devices (IEDs). As Colin Stagner notes, a common approach to detecting IEDs is detecting chemical traces of explosives, but this is not a perfect solution. He suggests an alternate idea of detecting the initiator, such as a remote trigger (e.g., from a garage door opener) or proximity detector (motion sensor). He notes: "These initiators are electronic devices which generate and process high-frequency signals. Such signals can radiate from resonant features in the device's printed circuit board (PCB) and packaging, escaping into the environment as *unintended electromagnetic emissions* [italics in original]."[64] It is possible to detect unintentional electromagnetic emissions (UEEs); moreover, it is possible then to identify the device and its status using a comparison database of signatures.

A second example with IC implications is a product called Ghostbuster. Designed by university researchers, the product is designed to thwart eavesdropping within a wireless network by employing a passive wireless receiver to intercept information being transmitted wirelessly between, for example, a wireless camera and a router. The authors note that, even though the eavesdropper is not actively sending out any signal, the hardware that comprises the eavesdropper leaks RF signals—and those signals can be detected.[65]

To conclude this section with implications for teaching MASINT, it should be obvious that there are a variety of sensors in all six MASINT sub-disciplines available for classroom discussion or student research. Several themes that might be examined include different types of platforms (e.g., ground, air, or space); MASINT collectors (U.S., foreign nations, companies, international organizations, etc.); missions (treaty monitoring, homeland defense, environmental, etc.); changes in missions over time; strategic vice tactical missions; underlying scientific disciplines; underlying sources along the EM spectrum; future development, etc.

Myth #2: I'm already teaching other technical INTs, such as IMINT or SIGINT; why focus on MASINT?

Even though there are many examples of MASINT collection platforms, it is a reasonable question to ask, especially given limited resources: Why not just focus on other technical INTs, such as IMINT or SIGINT? With the rise of commercial imagery, IMINT, as well as GEOINT overall, is ubiquitous today—as anyone who has searched for real estate, an apartment, or a route map, or looked down from space using Google Earth to see if his/her car is parked in the driveway, can verify. SIGINT, or at least the communications intelligence (COMINT) part of it, is also well known by the public thanks to the past few years of revelations about the National Security Agency's (NSA) collection programs.[66] Ironically, companies which produce smart speakers seem more interested in listening in on our conversations than NSA, which seems to be more circumscribed by laws. Geospatial proponents will argue that the rise in imagery and geospatial applications makes IMINT or GEOINT more important today; those grappling with privacy versus security issues enjoy debating SIGINT.

It is certainly true that MASINT has some weaknesses worth discussing. Writing in 1998, Zachary Lum identified some technical hurdles that prevented MASINT from being useful. One was "disseminating the data and exploiting it in a timely manner…"[67] A second was volume, that is, overwhelming amounts of data. Another was lacking or incomplete signature databases.[68] Other challenges include getting access to the target and lack of persistence (i.e., adversaries can use denial and deception (D&D) to avoid times when sensors are sensing).[69] [Editor's Note: For a wealth of incisive articles on this subject, see *AIJ*, Vol. 32, No. 2, 2015, which explores the theme "Denial and Deception."]

MASINT, however, can make a unique contribution. One of the main advantages of MASINT is that it often produces objective data. The results of a soil sample are, assuming the machine is calibrated and working properly, accurate. Yes, it is possible that the collector gathered a soil sample in the wrong location or that an analyst infers the wrong meaning for the chemical composition of the soil, but what is collected is correct. It is arguably much easier to collect something that is either accidentally or intentionally inaccurate when it comes to OSINT or HUMINT, for instance. A second advantage is that MASINT is often collected via stand-off devices or remotely. This has the effect of minimizing the impact of D&D efforts. Finally, while some will critique MASINT as the "leftovers" of the technical intelligence collection method, excluding IMINT and SIGINT, this can also be considered a strength, as many of these collection methods and their processing and exploitation are unique.[70] Connie Lynn writes: "The greatest strength of MASINT is that the sensors have the potential to isolate very precise signatures and characteristics of objects or activities that can't be seen or detected by human senses."[71] As Aaron Chia Eng Seng, a lecturer at the Defence Science and Technology Agency's college in Singapore, sums up:

> Difficult tactical and intelligence problems often require information from several sources to provide a more complete assessment of the situation. MASINT contributes both unique and complementary information on a wide range of intelligence requirements, and is often the basis for cueing other collection disciplines. MASINT is considered highly dependable since it collects performance data and characteristics on targets that do not realise that they have created an indication of presence or activity. As a result, these signatures are often not protected by any countermeasures. Because it works in different parts of the electromagnetic spectrum, MASINT detects information patterns not previously exploited by individual sensors.[72]

When it comes to MASINT instruction, this issue of how MASINT stands against other technical forms of collection allows for a discussion of both the strengths and weaknesses of the discipline, but also for a comparison with the other INTs.

Myth #3: Granted MASINT was important during the Cold War for providing strategic intelligence on Soviet missiles and nuclear programs; it is not currently relevant to students.

Two arguments underlie this myth. The first is that MASINT became intimately tied to the hunt for Soviet strategic assets. That argument holds that MASINT's most useful applications do not fit the modern era of targeting, and that today MASINT is focused on the wrong sort of targets, and is thus less useful. A second, related argument is that in the past MASINT was an INT that often provided very accurate results—based on scientific principles—but this occurred at the expense of a timely answer. Today, timeliness is often seen as a critical component of intelligence that often seems to focus on current, fast-moving objectives. MASINT's former strength is thus a weakness.

In relation to the first argument, MASINT is not exclusively a Cold War tool. Prior to the Cold War, MASINT was geared to the battlefield, for example, with radio direction finding. Then during the Cold War, facing the hard target of the Soviet Union and such concerns as nuclear war, MASINT looked primarily to that target. As Zachary Lum notes, MASINT historically was seen as a group of intelligence collection techniques "used during the Cold War to gather extremely fine-grained threat data on foreign (primarily Soviet) strategic capabilities. The original MASINT mission, which continues today, was exclusively national intelligence, providing data to support treaty monitoring, proliferation management, technical exploitation and weapons assessment."[73]

Today, it is clear that the concerns of policymakers are a different mix than during the Cold War. The post-9/11 counterterrorism mission is an obvious example. In an interesting twist, however, two different conclusions emerged about whether MASINT matters today. One argument is that, with the passing of the Cold War, one loses a fair amount of incentive for MASINT collection. Examples include the IUSS and Constant Phoenix, which was almost cut. The underlying argument for this is that MASINT is a strategic INT, focused primarily on WMD, which is evident looking at all the examples above—most focus on nuclear or missiles.

However, the other side is also argued: Now that the Cold War is over, there are a lot more interesting, more mobile, sneakier targets out there and this is MASINT's time to shine. Other INTs like IMINT or SIGINT, it is argued, will not keep up. This view was offered by three different camps. First, it was the view coming out of Congress, where it was suggested that in the 21st century, as the proliferation of high-tech weapons, WMD, the growing sophistication of targets, and greater D&D occurred, MASINT was going to be essential. "In fact, some believe MASINT will be the most important 'technical INT of the future.'"[74] Some authors familiar with MASINT, such as those who were in the IC, supported this view. John Macartney writes that "throughout 1998 and 1999, senior U.S. intelligence officials were telling these public forums [e.g., Association of Former Intelligence Officers and National Military Intelligence Association luncheons and symposia] that MASINT was gaining in importance and would soon be *the* most valuable of all the collection disciplines [emphasis in original]."[75] Finally, academics writing about MASINT offered a similar observation. Krishnan, for example, posits: "Over the last ten years MASINT has emerged from being a minor contributor of intelligence to a major technical collection discipline, which already overlaps with and supplants the traditional SIGINT and IMINT disciplines."[76]

Turning to the second argument—timeliness—it is the case that, in the past, processing and exploitation took a long time. Today, with 24/7 news, and what seems like customers' short attention spans between crises, and how quickly crises can appear and spread, it seems like there is no time for methodical, scientific exploitation. However, neither of these two concerns—focus or timeliness—is quite correct.

The reality is that the other INTs, like IMINT, did not remain static and also evinced new capabilities for new missions. The view that MASINT would essentially step in and explode on the scene turned out to be wrong. However, the argument that we do not need MASINT today is also wrong. The answer is somewhere in the middle. One type of example is that existing MASINT platforms were put to similar uses elsewhere. For example, we mentioned above how the focus of acoustic MASINT has shifted from the Atlantic to the Pacific, or how Cobra Ball is in part focused on North Korea or sending Constant Phoenix to Japan in 2011. John Morris offers many current and useful examples of MASINT mission support areas, including support to military operations, defense acquisition and force modernization, proliferation of WMD and advanced conventional weapons, arms control and treaty monitoring, environmental issues, counterterrorism, and counternarcotics.[77]

Concerning timeliness, first of all, some MASINT systems in the past were very timely, such as the nuclear detection systems. It is rather pointless to require days to determine if a nuclear first-strike is under way. Second, more importantly, improvements in computer processing, storage, and digital transmission have allowed MASINT to accelerate dramatically the process of matching unknown signatures to a known signature in a database and report out that hit.

Systems like UTAMs are a good example, where the sensor can identify a threat and locate its origin in near real time. Likewise, the nuclear detection systems emplaced at U.S. ports of entry or at the borders also work nearly instantaneously.

In terms of teaching MASINT, the implication is simply that MASINT remains relevant today. MASINT has many current applications. If we think of MASINT before the Cold War as being focused on the battlefield, then a shift to strategic issues during the Cold War, then a shift back to the battlefield in the 1990s, followed by a new focus in part guided by counterterrorism, and perhaps in the near future moving back to strategic (per the new 2019 *National Intelligence Strategy*), the point is MASINT does not forget how to do earlier applications. MASINT is additive, which is a strength. This includes both strategic uses, such as foreign missiles, and more tactical applications like UTAMS, but also just a range of applications that goes beyond the traditional military ones.

Myth #4: MASINT is notorious for being misunderstood by the IC; how can students be expected to understand it?

A challenge in teaching MASINT is the subject's technical nature. Frankly, MASINT is technical. Understanding the science—in fact, the multiple science disciplines—behind MASINT is difficult for many people, including students, to grasp. Some illustrative quotes are: "…the technologies involved are so exotic and complex that most of us do not have enough scientific background to understand much about MASINT."[78] As John Morris and Robert Clark suggest: "The old joke about needing to be a rocket scientist to understand something was actually true about MASINT in that [Cold War] era."[79] Even the name was criticized for not having explanatory power as to what MASINT did, for example by the Critical Intelligence Problems Committee, which reviewed the IC's view of MASINT for the Director of Central Intelligence in 1986: "There is a virtually universal view within the Community that, even after a number of years after its usage, MASINT is a commonly misunderstood and uninformative acronym."[80] The overall view, held by the IC itself, was that people just do not get MASINT.[81] External reviews, such as IC21 by Congress, concurred: "MASINT, as a specific and unique discipline, is not well understood by both the IC and user communities."[82]

There are two major challenges in understanding MASINT. First, the underlying sources of information require a lot of knowledge to comprehend. Moreover, "MASINT is a science-intensive discipline that needs people/scientists well versed in the broad range of physical and electrical sciences."[83] Understanding how a nuclear reaction works and what rays, waves, and particles are emitted by a reaction is certainly an example. Second, how the sensors work can be complex. An important distinction between MASINT and some of the other INTs, especially HUMINT and OSINT, is that MASINT is non-literal.[84] At the conclusion of processing, one does not receive a picture, as in electro-optical GEOINT; a translated news article, as in OSINT; or a report from an asset, as in HUMINT. Instead, the results may be measurements of chemical composition or spectral reflectance.

MASINT is mostly grounded in the electromagnetic spectrum. MASINT encompasses a number of scientists, and reviews such as IC21 noted that one really needed PhDs to interpret it. They needed to keep their skills and knowledge current, and this was hard to do in the IC.

While the actual science is complicated and the analytic techniques probably classified, what one can stress is that MASINT is science. Processing and exploitation take advantage of the scientific method, and that is quite common and something to which students should be exposed. Even without a depth of knowledge about the science behind a particular MASINT sub-discipline, students can be exposed to the method and then to critiques of it.

Myth #5: The Intelligence Community does not value MASINT; why should anyone else?

One issue, alluded to elsewhere in the essay, is that MASINT is not a popular subject within the IC. Matthew Aid writes that, since the 1970s, "American intelligence officials have struggled with the nagging question of just what MASINT is."[85] Aid further posits that MASINT was essentially created as a budgetary expedient, rather than a coherent, thought-out collection discipline. To Aid, this is still true today. MASINT "remains a hodgepodge of dozens of unrelated technical intelligence collection programs and one-off purpose-made sensors…"[86] As one author called it, "for most of its existence, the overlooked runt of the litter…"[87]

This myth is partly true. MASINT is not optimally used within the IC and there is too much uncertainty and simply a lack of knowledge about what the discipline can do, as has already been suggested. One can identify a number of management issues. Although DIA is the functional manager, for many years MASINT was hard to find in the IC. Budget issues and a lack of resources were a second problem. As Zachary Lum colorfully wrote: "Whatever technological obstacles face the budding MASINT discipline pale in comparison, however, to the bureaucratic tar pit in which it is mired."[88] Basically (describing a period up to the 1990s), the Central MASINT Office (CMO) was outgunned by the other agencies, and had little control over MASINT and little visibility within the IC. While the CMO was upgraded within DIA in 1999, John Macartney writes, that change did not produce a similar rise in size or clout.[89] A third problem was that the diversity of the programs within MASINT caused problems. Aid argues that, almost since its inception, "managing these collection assets has proven to be nothing short of a nightmare for the US intelligence community."[90]

Admittedly, management is not a topic that at first glance may seem exciting to intelligence studies students, or even to many practitioners. Much of the internal operations of the MASINT enterprise are also unlikely to be in the public purview. However, there is enough discussion of the history of the organization of the INT to spark some interesting classroom debate.[91] The fact that the evolution of the organization perhaps was not perfect or optimal is worth discussing, as are considerations about whether there are better ways to organize an INT. For example, should MASINT be housed in a separate agency, like NGA for GEOINT or NSA for SIGINT? Alternately, should MASINT be broken up into many smaller technologically similar units and off-loaded to the managers of other INTs to be added to their portfolios? Or perhaps students have other ideas that are worth mulling over.

CONCLUSION

Material on MASINT is not hidden away, nor is it particularly mysterious. It is relevant and useful to intelligence collection today. Further, it is actually pretty easy at least to add a lecture, discussion, or assignment on MASINT to an intelligence collection course and to give students the opportunity to pursue research papers or presentations on various aspects of MASINT. In learning about the IC in general and intelligence collection specifically, it is important for students to have as full a picture of these topics as can reasonably be offered. Devoting some course time toward MASINT will aid students, and potential future IC employees, in appreciating this area of collection and how it can help solve some of the most important and pressing intelligence questions. The table below summarizes the fundamental areas that could comprise a MASINT lecture and their myths and realities.

Table. **Summary of MASINT Topics, Myths, and Realities**.

Topic	Myth	Reality
Definitions and Sub-Disciplines	*All the good stuff is classified.*	There is plenty of information, which is easily found in such sources as government and military websites and academic journals.
Applications	*MASINT was good for studying Soviet missiles and nuclear, but not useful after the Cold War.*	MASINT has a variety of applications. It moved from strategic to tactical.
Strengths and Weaknesses	*In spite of expectations, MASINT is not useful today.*	MASINT's strengths keep it relevant.
Underlying Sources of Information	*MASINT is too technical and esoteric.*	Actually the scientific method is applied in a similar fashion to many science questions today.
Organization and Management	*The IC just is not that interested in it.*	This is partially true, but it is possible to describe a fair amount of the history of the INT and how it has been managed.

Source: Created by the author.

NOTES

[1] Tom Clynes, "Exclusive: Laser Scans Reveal Maya 'Megalopolis' Below Guatemalan Jungle," NationalGeographic.com, February 1, 2018, at https://www.nationalgeographic.com/news/2018/02/maya-laser-lidar-guatemala-pacunam/. Accessed on October 29, 2019. Lidar is also written as LIDAR and LiDAR; U.S. government sources do not spell the acronym consistently. "Lidar" will be used routinely throughout the rest of this article.

[2] GIS Geography, "A Complete Guide to LiDAR: Light Detection and Ranging," GISGeography.com, at https://gisgeography.com/lidar-light-detection-and-ranging/, last updated on February 17, 2018. Accessed on November 3, 2019.

[3] Stephanie Pappas, "Thousands of Mysterious Maya Structures Discovered in Guatemala," *Live Science* [online], February 1, 2018, at https://www.livescience.com/61616-mysterious-maya-structures-discovered.html. Accessed on November 3, 2019.

[4] Mark M. Lowenthal and Robert M. Clark, "Introduction," in Mark M. Lowenthal and Robert M. Clark, eds., *The 5 Disciplines of Intelligence Collection* (Thousand Oaks, CA: CQ Press, 2016): 1. Some authors prefer imagery intelligence (IMINT) over GEOINT and some intelligence commentators dispute the number of INTs.

[5] U.S. Department of Defense. *Measurement and Signature Intelligence (MASINT)*, Instruction 5105.58, April 22, 2009, incorporating Change 1, effective May 18, 2018.

[6] U.S. Department of Defense, *Management of Measurement and Signature Intelligence (MASINT)*, Instruction 5105.58, February 9, 1993.

[7] John L. Morris, "MASINT," *American Intelligence Journal* 17, no. 1/2 (1996): 24.

[8] John L. Morris and Robert M. Clark, "Measurement and Signature Analysis," in Mark M. Lowenthal and Robert M. Clark, eds., *The 5 Disciplines of Intelligence Collection* (Thousand Oaks, CA: CQ Press, 2016): 176-191.

[9] William C. Spracher, "National Security Intelligence Professional Education: A Map of U.S. Civilian University Programs and Competencies" (EdD diss., The George Washington University, 2009); Michael S. Goodman, "Studying and Teaching About Intelligence: The Approach in the United Kingdom," *Studies in Intelligence* 50, no. 2 (2006): 57-65; and Stephen Coulthart and Matthew Crosston, "Terra Incognita: Mapping American Intelligence Education Curriculum," *Journal of Strategic Security* 8, no. 3 (2015): 46-68.

[10] This outline is a useful way to cover any INT. It is, for example, an organizing principle of the book edited by Lowenthal and Clark. See Mark M. Lowenthal and Robert M. Clark, "Introduction," in Mark M. Lowenthal and Robert M. Clark, eds., *The 5 Disciplines of Intelligence Collection* (Thousand Oaks, CA: CQ Press, 2016): 1.

[11] Armin Krishnan, "Teaching about 'Area 51'? How to Cover Secret Government Technology and Capabilities in Intelligence Studies Courses," *Journal of Strategic Security* 6, no. 3, Suppl. (2013): 187.

[12] Michael I. Handel, "The Study of Intelli*gence," Orbis* 26 (Winter 1983): 821.

[13] Krishnan, "Teaching about 'Area 51'?" 192. See also John D. Macartney, "John, How Should We Explain MASINT?" in *Intelligence and the National Security Strategist: Enduring Issues and Challenges*, Roger Z. George and Robert D. Kline, eds. (Lanham, MD: Rowman & Littlefield, 2005): 170-171. Macartney

explains that heavy classification is one reason why so little is known about MASINT.

[14] IWP 688: The Role and Importance of Human Intelligence, at https://www.iwp.edu/courses/the-role-and-importance-of-human-intelligence/; and INTL623 – Human Intelligence (HUMINT), at https://www.amu.apus.edu/course-schedule/details.html?c=INTL623.

[15] It has already been done. See, for example, Matthew Aid, "Measurement and Signature Analysis," in *Routledge Companion of Intelligence Studies*, Robert Dover, Michael S. Goodman, and Claudia Hillebrand, eds. (New York: Routledge, 2013): 120-122; and John L. Morris and Robert M. Clark, "Measurement and Signature Analysis," in Mark M. Lowenthal and Robert M. Clark, eds., *The 5 Disciplines of Intelligence Collection* (Thousand Oaks, CA: CQ Press, 2016): 159-208.

[16] Radars can also be passive sensors, listening for a signal's return.

[17] Phased-array radars are one type of radar. These radars emit a pulse of radio waves from an array of antennas, or radiating elements. These antennas are electronically steerable. For a basic overview, see Mark Hickle, "Phased Array Antennas," YouTube, February 13, 2015, at https://www.youtube.com/watch?v=vtPPAnvJS6c. Accessed on December 12, 2019.

[18] Lt Col Jennifer Jeffries, "COBRA DANE: A piece of history transitions to AFSPC," March 3, 2014, at https://www.peterson.af.mil/News/Commentaries/Display/Article/734515/cobra-dane-a-piece-of-history-transitions-to-afspc/. Accessed on November 13, 2019.

[19] Missile Defense Agency, "Cobra Dane" Fact Sheet 16-MDA-8777, June 2016.

[20] Air Force Space Command, U.S. Air Force, "COBRA DANE Radar," March 22, 2017, at https://www.afspc.af.mil/About-Us/Fact-Sheets/Display/Article/1126403/cobra-dane-radar/. Accessed on November 6, 2019. See also GAO, *Missile Defense: Air Force Report to Congress Included Information on the Capabilities, Operational Availability, and Funding Plan for Cobra Dane*, GAO-19-68 (Washington, DC: December 2018): 1.

[21] Susan A. Romano, "Air Force's new maritime radar becomes operational," August 11, 2014, at https://www.af.mil/News/Article-Display/Article/494036/air-forces-new-maritime-radar-becomes-operational/. Accessed on November 30, 2019.

[22] Dan Taylor, "USAF Missile Defense – From the Sea," *Air Force Magazine* 98, no. 1 (January 2015): 48.

[23] Examples of instructive sources on JORN include Alex Cameron, "The Jindalee Operational Radar Network: Its Architecture and Surveillance Capability," *Proceedings International Radar Conference* (1995): 692-697; Peterson Air Force Base, U.S. Air Force, "Jindalee Operational Radar Network," January 25, 2017, available at https://www.peterson.af.mil/About/Fact-Sheets/Display/Article/1059651/jindalee-operational-radar-network/. Accessed on November 6, 2019; and J. Allison, J. Caddy, and P. Yip, "Jindalee Operational Radar Network Phase 6: Over-the-Horizon Radar Developments," in *IEEE Potentials* 38, no. 4 (July-August 2019): 28-33.

[24] Defence Science and Technology Group, Department of Defence, Government of Australia, "JINDALEE OPERATIONAL RADAR NETWORK," n.d., available at https://www.dst.defence.gov.au/innovation/jindalee-operational-radar-network. Accessed on November 6, 2019.

[25] U.S. Air Force, "Jindalee Operational Radar Network."

[26] U.S. Air Force, "Jindalee Operational Radar Network."

[27] Thomas H. Maugh II, "Victor Vacquier Sr. dies at 101; geophysicist was a master of magnetics," *The Los Angeles Times*, January 24, 2009, at https://www.latimes.com/science/la-me-vacquier24-2009jan24-story.html. Accessed on December 16, 2019.

[28] The detection challenge reappears with very small nuclear tests. See, for example, Paul G. Richards and Won-Young Kim, "Advances in Monitoring Nuclear Weapon Testing," *Scientific American* 300, Issue 3 (March 2009): 70-77.

[29] Air Force Technical Applications Center, "Air Force Technical Applications Center," September 5, 2019, at https://www.16af.af.mil/About-Us/Fact-Sheets/Display/Article/1963049/air-force-technical-applications-center/. Accessed on December 7, 2019. Finally, see also the CBTBO's "Verification Regime" website at https://www.ctbto.org/verification-regime/. Accessed on December 8, 2019. Here one can look at profiles of individual seismic stations, among a solid history and description of the IMS.

[30] U.S. Department of State, "CTBT: International Monitoring System," n.d., at https://2009-2017.state.gov/t/avc/rls/212176.htm. Accessed on December 8, 2019. A map showing the locations of the IMS sensors is at https://www.ctbto.org/map/. Accessed on December 8, 2019.

[31] Air Force Technical Applications Center, "Air Force Technical Applications Center," September 5, 2019.

[32] Stephen Tenney, Brian Mays, David Hillis, Duong Tran-Luu, Jeffrey Houser, and Christian Reiff, *Acoustic Mortar Localization System – Results from OIF*, U.S. Army Research Laboratory, December 2004.

[33] See ShotSpotter, "ShotSpotter Technology," n.d., at https://www.shotspotter.com/technology/. Accessed on December 11, 2019.

[34] U.S. Navy, IUSS Mission, n.d., at https://www.public.navy.mil/subfor/cus/Pages/Mission.aspx. Accessed on December 7, 2019.

[35] U.S. Navy, "Surface SURTASS LFA Sonar," n.d., at http://www.surtass-lfa-eis.com/systems-description/. Accessed on December 7, 2019.

[36] U.S. Navy, "Surface SURTASS LFA Sonar."

[37] Edward C. Whitman, "SOSUS: The 'Secret Weapon' of Undersea Surveillance," *Undersea Warfare* 7, no. 2 (Winter 2005), at https://www.public.navy.mil/subfor/underseawarfaremagazine/Issues/Archives/issue_25/sosus.htm. Accessed on December 30, 2019.

[38] Statement of Admiral (USN) Harry B. Harris, Jr., Commander, U.S. Pacific Command, before the Senate Armed Services Committee on U.S. Pacific Command Posture, April 27, 2017, p. 16, at https://www.armed-services.senate.gov/imo/media/doc/Harris_04-27-17.pdf. Accessed on December 16, 2019. Steven Stashwick, "US Navy Upgrading Undersea Sub-Detecting Sensor Network," *The Diplomat*, November 4, 2016, at https://thediplomat.com/2016/11/us-navy-upgrading-undersea-sub-detecting-sensor-network/. Accessed on December 16, 2019.

[39] See, for example, Institute of Medicine, *Chemical and Biological Terrorism: Research and Development to Improve Civilian Medical Response* (Washington, DC: The National Academies Press, 1999); National Research Council, *Existing and Potential Standoff Explosives Detection Techniques* (Washington, DC: The National Academies Press, 2004); Kim E. Sapsford, Christopher Bradburne, James B. Delehanty, and Igor L. Medintz, "Sensors for detecting biological agents," *Materials Today* 11, Issue 3 (2008): 38-49; George M. Murray and Glen E. Southard, "Sensors for

chemical weapons detection," *IEEE Instrumentation & Measurement Magazine* 5, no. 4 (December 2002): 12-21; and Robert Bogue, "Detecting explosives and chemical weapons: A review of recent developments," *Sensor Review*, 35 no. 3 (2015): 237-243.

[40] U.S. Air Force, "WC-135 Constant Phoenix," May 27, 2005, at https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104494/wc-135-constant-phoenix/. Accessed on December 2, 2019. The LTBT bans nuclear tests in areas other than underground; underground tests must not produce debris that would be outside the responsible state's territory. See U.S. Department of State, Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space, and Under Water, at https://2009-2017.state.gov/t/avc/trty/199116.htm. Accessed on December 3, 2019.

[41] U.S. Air Force, "WC-135 Constant Phoenix," May 27, 2005.

[42] Susan A. Romano, "Nuclear air sampling aircraft on display at Patrick AFB," March 5, 2019, at https://www.16af.af.mil/News/Legacy/Article/1774336/nuclear-air-sampling-aircraft-on-display-at-patrick-afb/. Accessed on December 3, 2019.

[43] Valerie Insinna, "Air Force to start transforming tankers into WC-135 'nuke sniffers' in FY19," *DefenseNews*, April 25, 2018, at https://www.defensenews.com/smr/nuclear-triad/2018/04/25/air-force-to-start-transforming-tankers-into-wc-135-nuke-sniffers-this-year/. Accessed on December 3, 2019.

[44] U.S. Department of Homeland Security, Privacy Impact Assessment for the Radiation Detection Systems, DHS/CBP/PIA-031, July 11, 2016, at: https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-rds-july2016.pdf. Accessed on December 3, 2019. Although this document is primarily focused on the collection of Personally Identifiable Information (PII) during enforcement, it offers useful descriptions and photos of the equipment.

[45] U.S. Customs and Border Protection, "Non-Intrusive Inspection (NII) Technology," fact sheet, n.d., at https://www.cbp.gov/sites/default/files/documents/nii_factsheet_2.pdf. Accessed on December 3, 2019.

[46] See https://www.dhs.gov/news/2014/07/29/written-testimony-dndo-house-homeland-security-subcommittee-cybersecurity.

[47] John L. Morris and Robert M. Clark, "Measurement and Signature Analysis," in Mark M. Lowenthal and Robert M. Clark, eds., *The 5 Disciplines of Intelligence Collection* (Thousand Oaks, CA: CQ Press, 2016): 189.

[48] John Leacock, "Neutron Propagation in Atmosphere," presentation dated October 15, 2014, at https://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-14-27966. Accessed on December 16, 2019.

[49] For a short overview of Lidar, see Connie Lynn, "Making the Most of MASINT and Advanced Geospatial Intelligence," Master of Military Studies research paper, USMC Command and Staff College (October 4, 2012): 16-19.

[50] U.S. Air Force, "RC-135S COBRA BALL," February 16, 2012.

[51] U.S. Air Force, "RC-135S COBRA BALL," February 16, 2012.

[52] U.S. Air Force, "RC-135S COBRA BALL," February 16, 2012.

[53] Elizabeth Shim, "Report: U.S. deploys second Cobra Ball surveillance plane to Japan," UPI [online], June 9, 2019, at https://www.upi.com/Top_News/World-News/2019/06/09/Report-US-deploys-second-Cobra-Ball-surveillance-plane-to-Japan/7001559831981/. Accessed on December 2, 2019.

[54] See, for instance, Robert S. Hopkins, III, "Air Force Manned Reconnaissance at a Crossroads," *War on the Rocks*, April 16, 2019, at https://warontherocks.com/2019/04/air-force-manned-reconnaissance-at-a-crossroads/. Accessed on December 2, 2019.

[55] See, for example, then-Secretary of the Air Force Heather Wilson's response to a letter dated June 29, 2018, from Senator Deb Fischer et al. regarding status of the fleet at https://www.airforcemag.com/PDF/DRArchive/Documents/2019/secaf-response-to-ne-delegation-letter.pdf. Accessed on December 30, 2019. The letter is available at https://www.fischer.senate.gov/public/index.cfm/2018/6/ne-congressional-delegation-seeks-answers-from-air-force-on-planes-at-offutt. Accessed on December 30, 2019.

[56] For a short overview of AVIRIS and HSI, see Connie Lynn, "Making the Most of MASINT and Advanced Geospatial Intelligence," Master of Military Studies research paper, USMC Command and Staff College (October 4, 2012): 1. For an interesting example of an electro-optical sensor focused on nuclear detection, see the Bhangmeter, which is a sensor designed to detect the double flash of light from a nuclear explosion. See Eileen Patterson, "The Double Flash Meets the Bhangmeter," *National Security Science* (July 2015): 12, at https://www.lanl.gov/discover/publications/national-security-science/index.php. Accesssed on December 15, 2019.

[57] Several other hyperspectral sensors on satellites are identified by Julie Transon, Raphaël d'Andrimont, Alexandre Maugnard, and Pierre Defourny, "Survey of Hyperspectral Earth Observation Applications from Space in the Sentinel-2 Context," *Remote Sensing* 10 (2018): 1-32.

[58] Department of Space, Indian Space Research Organisation, "PSLV-C43/HysIS Mission," November 29, 2018, available at https://www.isro.gov.in/launcher/pslv-c43-hysis-mission. Accessed on November 5, 2019.

[59] Chang Guang Satellite Technology Co, "Jilin-1 Spectrum 01 – 02 Satellite," n.d. Available at http://www.charmingglobe.com/EWeb/product_view.aspx?id=676. Accessed on December 3, 2019.

[60] For applications of HSI see, for instance, John D. Macartney, "John, How Should We Explain MASINT?"

[61] See, for example, Adam Keith, "Is hyperspectral the next Earth observation frontier?" *SpaceNews*, March 30, 2019, at https://spacenews.com/op-ed-is-hyperspectral-the-next-earth-observation-frontier/. Accessed on November 5, 2019.

[62] Federal Communications Commission, "Equipment Authorization – RF Device," at https://www.fcc.gov/oet/ea/rfdevice. Accessed on December 30, 2019.

[63] Federal Communications Commission, "Equipment Authorization – RF Device," at https://www.fcc.gov/oet/ea/rfdevice. Accessed on December 30, 2019.

[64] Colin Stagner, "Detecting and locating electronic devices using their unintended electromagnetic
Emissions" (PhD diss., Missouri University of Science and Technology, 2013), Doctoral Dissertations, 2152, 2, at https://scholarsmine.mst.edu/doctoral_dissertations/2152. Accessed on December 3, 2019.

[65] Anadi Chaman, Jiaming Wang, Jiachen Sun, Haitham Hassanieh, and Romit Roy Choudhury, 2018, Ghostbuster: Detecting the Presence of Hidden Eavesdroppers. In The 24th Annual International Conference on Mobile Computing and Networking (MobiCom '18), October 29-November 2, 2018, New Delhi, India. ACM, New York, NY, USA, 15 pages, available at https://doi.org/10.1145/3241539.3241580.

[66] SIGINT is comprised of three sub-disciplines: COMINT, noted above; electronic intelligence (ELINT); and foreign instrumentation signals intelligence (FISINT).
[67] Zachary Lum, "The Measure of MASINT," *Journal of Electronic Defense* 21 (August 1998): 47.
[68] Zachary Lum, "The Measure of MASINT," *Journal of Electronic Defense* 21 (August 1998): 47. Macartney, among others, also notes that collection, and construction of libraries of signatures, is a crucial task.
[69] Robert K. Ackerman, "Low-Technology Foes Require High-Technology Detection," *Signal* (October 2002): 24.
[70] See, for one example, Matthew M. Aid, "Measurement and Signature Analysis," in Robert Dover, Michael S. Goodman, and Claudia Hillebrand, eds., *Routledge Companion of Intelligence Studies* (New York: Routledge, 2013).
[71] Connie Lynn, "Making the Most of MASINT and Advanced Geospatial Intelligence," Master of Military Studies research paper, USMC Command and Staff College (October 4, 2012): 1.
[72] Aaron Chia Eng Seng, "MASINT: The Intelligence of the Future," *DSTA Horizons 2007*, 119, at https://dsta.gov.sg/who-we-are/publications/dsta-horizons/dsta-horizons-2007. Accessed on December 11, 2019.
[73] Zachary Lum, "The Measure of MASINT," *Journal of Electronic Defense* 21 (August 1998): 44. See also John L. Morris and Robert M. Clark, "Measurement and Signature Analysis," in Mark M. Lowenthal and Robert M. Clark, eds., *The 5 Disciplines of Intelligence Collection* (Thousand Oaks, CA: CQ Press, 2016): 159; and John D. Macartney, "John, How Should We Explain MASINT?" in *Intelligence and the National Security Strategist: Enduring Issues and Challenges*, Roger Z. George and Robert D. Kline, eds. (Lanham, MD: Rowman & Littlefield, 2005), who makes a similar argument.
[74] U.S. Congress, House, Permanent Select Committee on Intelligence, *IC21: The Intelligence Community in the 21st Century*, 104th Congress, June 5, 1996, Chapter 7.
[75] John D. Macartney, "John, How Should We Explain MASINT?" 171.
[76] Krishnan, "Teaching about 'Area 51'?" 190.
[77] John L. Morris, "MASINT," *American Intelligence Journal* 17, no. 1/2 *(*1996): 25, Figure 3.
[78] John D. Macartney, "John, How Should We Explain MASINT?" 170-171.
[79] John L. Morris and Robert M. Clark, "Measurement and Signature Analysis," in Mark M. Lowenthal and Robert M. Clark, eds., *The 5 Disciplines of Intelligence Collection* (Thousand Oaks, CA: CQ Press, 2016): 160.
[80] Critical Intelligence Problems Committee, "CIPC Review of the Community's Organization of MASINT," memorandum prepared for the DCI, DCI/ICS 86-3708, January 31, 1986, declassified on February 15, 2011, at CIA-RDP88G01116R0002001140007-8.
[81] U.S. Department of Defense, Office of the Inspector General, Evaluation Report on Measurement and Signature Intelligence, Washington, DC: Department of Defense, June 30, 1997.
[82] U.S. Congress, House, Permanent Select Committee on Intelligence, *IC21: The Intelligence Community in the 21st Century*, 104th Congress, June 5, 1996, Chapter 7.
[83] U.S. Congress, House, Permanent Select Committee on Intelligence, *IC21: The Intelligence Community in the 21st Century*, 104th Congress, June 5, 1996, Chapter 7.
[84] John L. Morris and Robert M. Clark, "Measurement and Signature Analysis," in Mark M. Lowenthal and Robert M. Clark, eds., *The 5 Disciplines of Intelligence Collection* (Thousand Oaks, CA: CQ Press, 2016): 161. Others also make this point, e.g., Lum, 44.
[85] Matthew M. Aid, "Measurement and Signature Analysis," in Robert Dover, Michael S. Goodman, and Claudia Hillebrand, eds., *Routledge Companion of Intelligence Studies* (New York: Routledge, 2013): 115.
[86] Matthew M. Aid, "Measurement and Signature Analysis," in Robert Dover, Michael S. Goodman, and Claudia Hillebrand, eds., *Routledge Companion of Intelligence Studies* (New York: Routledge, 2013): 115.
[87] Zachary Lum, "The Measure of MASINT," *Journal of Electronic Defense* 21 (August 1998): 43.
[88] Zachary Lum, "The Measure of MASINT," *Journal of Electronic Defense* 21 (August 1998): 48.
[89] John D. Macartney, "John, How Should We Explain MASINT?"
[90] Matthew M. Aid, "Measurement and Signature Analysis," in Robert Dover, Michael S. Goodman, and Claudia Hillebrand, eds., *Routledge Companion of Intelligence Studies* (New York: Routledge, 2013): 119.
[91] Reviews of the organizational history of MASINT are found in such readings as John L. Morris and Robert M. Clark, "Measurement and Signature Analysis," in Mark M. Lowenthal and Robert M. Clark, eds., *The 5 Disciplines of Intelligence Collection* (Thousand Oaks, CA: CQ Press, 2016): 172-176; Matthew M. Aid, "Measurement and Signature Analysis," in Robert Dover, Michael S. Goodman, and Claudia Hillebrand, eds., *Routledge Companion of Intelligence Studies* (New York: Routledge, 2013): 119-120; U.S. Congress, House, Permanent Select Committee on Intelligence, *IC21: The Intelligence Community in the 21st Century*, 104th Congress, June 5, 1996, Chapter 7; John L. Morris, "MASINT," *American Intelligence Journal* 17. no. 1/2, 1996, 26; and U.S. Department of Defense, *Management of Measurement and Signature Intelligence (MASINT)*, Instruction 5105.58, February 9, 1993.

Dr. John D. Sislin received his PhD in political science from Indiana University. His dissertation on the use of U.S. arms sales to influence recipient nations was supported by a fellowship from the U.S. Arms Control and Disarmament Agency. Among other positions, Dr. Sislin was a program officer at the National Research Council of the National Academy of Sciences prior to entering government service. He is a former imagery analyst at the National Geospatial-Intelligence Agency and currently is a faculty member in the Department of Collection, Analysis, and Counterintelligence, College of Strategic Intelligence, at the National Intelligence University. He recently served as chair of NIU's Institutional Review Board, which examines all master's thesis proposals for appropriate research on human subjects. John divides his time teaching and researching between intelligence analysis and intelligence collection. He has written several book reviews for AIJ *in the past and is a valued contributor.*

Neurosecurity: Human Brain Electro-optical Signals as MASINT

by Dr. Matthew Canham and Dr. Ben D. Sawyer

INTRODUCTION

Applied neuroscience presently allows not only the scientific discovery-oriented probing of the inner workings of the mind, but increasingly the probing of individual minds toward gathering intelligence. Significant advances in neuroimaging, leveraging both active and passive electro-optical energy, can reveal specifics of information held in the mind even without cooperation (e.g., Lange et al., 2018; Sawyer et al., 2016a). The processes of the brain increasingly join many other energetic sources from which quantitative and qualitative data analysis may extract identifying features and other useful intelligence (Sawyer & Canham, 2019). Indeed, it is increasingly appropriate to discuss the human brain as a system which can be read from, written to, and the operations of which may therefore be collected for analysis or influenced (Sawyer & Canham, 2019). Indeed, we argue here that we are witnessing the end of the era in which human thought is generally accepted as an entirely private process, the starting point of an unquestionably remarkable transition. The collection of unintended emissions and byproducts toward intelligence fits well into the mold of Measurement and Signals Intelligence, and indeed Measurement and Signature Intelligence (both MASINT, Macartney, 2001), and so we believe this community within the Intelligence Community is well-suited to discuss these new realities of neurosecurity, as it helped shape many formative discussions surrounding cybersecurity. A MASINT perspective on biological, neural signatures comes with the need to discuss current capabilities, projected technological arc, practicalities, and potential abuses.

While these authors currently have no knowledge of remote monitoring of brain activity, multiple commercial entities are working toward this technology (Strickland, 2017) in various forms. Simultaneously, evidence of remote interference in normal brain functioning is in the news. Most recently, between December 2016 and October 2017, at least 21 employees stationed at the U.S. Embassy in Havana, Cuba, reported experiencing a constellation of symptoms usually associated with a concussion or traumatic brain injury (TBI). Eighteen of these employees reported a sudden onset of symptoms coinciding with an intense chirping or ringing sound similar to the Indies short-tailed cricket. Symptoms reported by employees included difficulty hearing, dizziness, headaches, cognitive difficulties, difficulties with balance, and intense brain pressure (Kirk, 2019). A clinical evaluation by researchers at the University of Pennsylvania found structural differences between exposed employees and healthy controls (Verma et al., 2019). While the clinical implications of this are currently unclear, it seems plausible that these employees were exposed to something that altered their neurological structures and cognitive functioning. The mystery continued to deepen in 2018 when an embassy employee stationed in Guangzhou, China, reported similar symptoms. While we stress that there is still considerable mystery surrounding these events, it does seem likely that these symptoms were (1) induced and (2) likely not the direct goal of whatever process produced the phenomenon. Initial examination of the victims suggests remote microwave energy, long known to affect temporal lobe function (Dyer, 2018). These phenomena provide potential evidence of the intentional targeting of neural architecture, potentially as an attack, potentially as a side effect to some other goal.

Less circumspect evidence also exists. Capability to monitor neural activity exists given direct physical proximity, and remote neural monitoring may be feasible. Recent advances have seen remote detection of other biosignals once considered only measurable from direct physical proximity. For example, NASA's Finding Individuals for Disaster and Emergency Response (FINDER) system uses low-power microwaves to detect heartbeats at great physical range (Liu et al., 2014). Core body temperature is now routinely monitored in crowds to identify individuals with infections (Ng, Kawb, & Chang, 2004). Moreover, two categories of neuroimaging technology are emerging with the promise to make remote brain access a near-term reality. Industry groups like Facebook and Open Water are working to advance near-infrared and holographic techniques for monitoring neural blood flow patterns in real time (Open Water, 2018).

Meanwhile, Neuralink, Kernel, and others are working to connect the electrical activity of the brain to intermediary electrodes, and then to the Internet. The success of either of these technologies, neuroimaging at range or Internet-connected electroencephalography, will open a new universe of possibilities for the realms of MASINT, SIGINT, and HUMINT alike.

CURRENT STATE OF THE ART

Before diving into the world of neuroimaging, we offer a brief introduction into what is currently known about how the brain functions. We begin with the neuron, the basic building block of the neural network that is our brain. A basic decision-making system, it takes in input from upstream neurons through receptors known as dendrites and, once a certain threshold of these signals is met, "fires" an action potential which travels down the long synapse to the synaptic gap which separates one neuron from another. Here, chemical signals take over, propagating further action potentials downstream to other neurons in spreading cascades of activity and activation. The process is a foundation for complex patterns of information being aggregated and processed. For example, while the earliest neurons to process visual information might only detect the presence or absence of an edge, neurons further downstream in visual cortex will aggregate the presence of an edge in a specific orientation or relative position and recognize this as the letter "K." Further downstream, neurons will respond more vigorously to the letter "K" when it is placed at the beginning of a word as opposed to the middle or end. In this way, information is aggregated and processed into meaningful coherence.

While there is still debate surrounding the validity of brain area specialization, and growing evidence for "network" approaches to understanding activity, at a coarse level, brain regions appear to be functionally specialized for different activities. Understanding this differential specialization allows for a limited, but growing, degree of reverse engineering of brain processes. A great deal of cognitive processing occurs in the neocortex, the outermost layer of the brain. Here, four "lobes," anatomical brain regions, have been linked by research to functional specializations (see Figure 1, Miller & Cummings, 2017). The occipital lobe, or visual cortex, is where much of visual processing takes place. The parietal lobe handles spatial awareness and somatosensory processes which feed the brain's sense of bodily positioning and stimulation. For example, tickling the hands or feet with a feather would activate somatosensory processing, which would occur primarily in the frontal parietal lobe. The temporal lobe also sits just forward of the occipital lobe and below the parietal lobe, usually just above one's ear. The temporal lobe (aka the auditory cortex) processes sound and often handles long-term memory processing as well. Finally, the frontal lobe is responsible for fine motor functioning, and actions known as executive functions: deliberate decision-making, inhibitory control, attention, and working memory. If you are intensely concentrating on a task, then there is a high likelihood that you are recruiting much of your frontal lobe's prefrontal cortex. This final example is especially significant from a MASINT perspective: it has been suggested that when deliberately trying to deceive someone, the deceiver relies on his/her frontal lobe to a greater degree than does someone who is not attempting to be deceptive **(**Zeki et al., 2004**)**. There is greater activation in the prefrontal cortex because the individual must inhibit the true version events and must hold two versions active simultaneously **(**Ofen et al., 2016**)**. Although there is still much debate on the validity of this assertion, as an example it illustrates how neural processing might be utilized in an intelligence-gathering capacity.

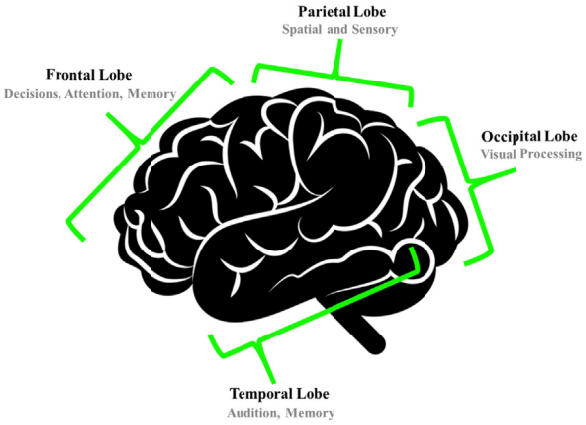


Figure 1: The neocortex or surface of the brain, disproportionately responsible for cognitive processing, is currently conceptualized as divided into functional regions. As with technical and social systems, useful MASINT consideration of these areas is in terms of intelligence and potential influence. Increasingly, it is possible to collect electro-optical energy emitted by the brain and, leveraging temporal and spatial dimensions, decode meaning and so acquire useful intelligence. Influence is also possible, and devices which project electrical force into the brain can disrupt or modify brain processes.

Detectable Signals – A discussion about neuro-imagining should first make the distinction between structural and functional imaging. Structural imaging provides a highly detailed static image of the neuro-

anatomical structures of an individual. When the researchers from the University of Pennsylvania examined the embassy employees and found differences in whole brain white matter, this difference was found through the analysis of static structural images (Verma et al., 2019). In contrast, functional imagery tends to be coarser but provides a dynamic series of snapshots that provide insight into the neural activity of an individual. While both techniques have relevance to MASINT applications, functional imaging will be the topic of focus here. Within the universe of functional imaging there are currently two types of signals, blood flow and electrical activity, that are detected to derive neural functioning.

Blood Flow Signals – When neurons are active, these cells consume sugar and oxygen and therefore require replenishment. This replenishment transpires through a process known as hemodynamic response. Termed a blood-oxygen-level-dependent (BOLD) signal, this difference between oxygenated and deoxygenated blood is detectable through various means such as magnetic manipulation or using infrared spectrum light. Examining this signal using magnetism usually involves a technology known as functional Magnetic Resonance Imaging (fMRI). fMRI technology witnessed an upshot in usage within brain research beginning in the early 1990s because it was considerably less intrusive than comparable imaging technologies available at the time. A major drawback in fMRI as a MASINT technique is the need to immobilize a subject and capture imagery over a long time period (from 45 minutes to a few hours), while secured to a table and loaded into a magnetic resonance tube. Movement during imaging is highly detrimental, meaning that only extremely compliant individuals can be imaged. Finally, high tesla (a measurement of magnetism strength) equipment capable of high spatial and temporal resolution imaging is extremely expensive and often requires a dedicated staff, making this technology largely confined to use within a dedicated laboratory. These inconveniences notwithstanding, several researchers have proposed methods of employing fMRI as a means of deception detection (Ganis et al., 2003; Kozel et al., 2005; Monteleone et al., 2009; Ganis et al., 2011). Continuing advances in the miniaturization of this technology suggest this could eventually be an approach moved out of the laboratory and into the field (see, for example, Cooley et al., 2015).

Other emerging techniques such as functional Near Infrared Spectroscopy (fNIRS) offer a window into more near-term workable solutions. Cheap, low-power, and portable, fNIRS utilizes the near infrared spectrum light to detect the BOLD signal. In the 700-900nm spectral range, bodily tissues are mostly transparent, allowing maximal detectability of the relative difference between oxygenated and deoxygenated hemoglobin. fNIRS utilizes a combination of infrared light emitters and receivers to parse out the BOLD signal through differences in infrared light intensity. These differences in light intensity can then be interpreted to detect and localize BOLD signals from specific brain regions to infer localized activity. One of the major advantages of fNIRS over fMRI from a MASINT perspective is the ease of use, and portability of these devices. Indeed, the technology is routinely held up as an excellent match for the demands of brain machine interface and field research (respective reviews are Naseer & Hong, 2015 and Quaresima and Ferrari, 2019). It is currently unclear what the ultimate detectable range using the infrared spectrum will be, but at present these signals are detected using a sensor cap worn by the subject which directly contacts the skin. This portability and ease of use would potentially allow for modern deployment in the debriefing of HUMINT assets by handlers or operational psychologists.

Electrical Activity Signals – While neuroimaging techniques dependent upon blood flow offer high spatial resolution and the capability of localizing neural activity, they lack the capability of detecting activity with a high temporal resolution because there is an inherent lag in the reuptake of oxygenated hemoglobin into active neural regions. This delay means that events which happen very quickly, such as visual recognition, can be missed by techniques reliant on BOLD signal. In these situations, techniques that detect electrical activity offer an advantage over those that detect signals related to blood flow. Electrical detection techniques have very high temporal resolution (on the order of milliseconds), but because electrical fields are distorted by the scalp, they lack the spatial resolution that blood flow-based imaging techniques have. Therefore, researchers often combine these techniques when studying neuro phenomena.

Techniques measuring electrical activity include deep brain electrodes, Electrocorticography (ECoG), and Electroencephalography (EEG), listed from most to least invasive. Brain-contact techniques utilize small probes (approximately 5 ìm thick) to directly connect to neurons to detect activity (Muthuswamy, 2012), and involve opening the skull to access the cortex. ECoG is somewhat less invasive, involving electrodes that rest upon the dura, a thin sheet of enervated tissue which contains the cerebrospinal fluid and the brain. Non-invasive techniques such as EEG detect voltage potential fluctuations deriving from the action potential activity within the neurons of the brain. Such measured "potentials" can be measured longitudinally over time, or measured relative to specific events, an approach which can identify specific patterns of brain activity known as event-related potentials (ERP). This connection between

outside events and brain activity is an excellent strategy to reverse engineer (to a limited degree) the brain activity as it relates to a specific stimulus. One of the most studied ERPs, the "P300" wave, is a distinctive positive fluctuation that occurs approximately 300 milliseconds after visual recognition of a stimulus. The P300 has therefore been proposed as a deception detection technique in "guilty knowledge tests." A subject wearing an EEG would, in such a test, be presented with visual stimuli in succession, and an amplified P300 of what occurred directly after any image recognized, and without the awareness or conscious control of the subject. Many other potentially useful ERPs exist, in the context of MASINT, and include error-related negativity (ERN, see Sawyer et al., 2016b), the P3 (see Rosenfeld et al., 1991), and ERN composite signals such as the multifaceted electroencephalographic response (MERMER, see Farwell & Smith, 2001), to name but a few. Indeed, while the present literature is focused upon individual signatures and their functional meeting, the overarching message here from a MASINT perspective is that electrical signals collected incidentally from brain activity can be used to provide actionable intelligence.

Directing Input into the Brain – Thus far our discussion has centered around reading activity from the brain, but electromagnetic energy can also be effectively used to input information into the brain. A delicate system, the brain can be influenced or disrupted by relatively small amounts of kinetic or electrical energy, and indeed is susceptible to informational patterns (Sawyer et al., 2016a; Sawyer & Hancock, 2018) Transcranial Magnetic Stimulation (TMS) is one such technology, and uses magnetic energy directed toward the neocortex either to excite or to suppress the underlying neural region. For example, an individual who has their visual cortex (occipital lobe, see Figure 1) may experience loss or aberration of vision. TMS has been used for decades in both clinical and research contexts. Recent applications of this technology are striking: for example, a research group at the University of Washington (Jiang et al., 2019) employed TMS as part of an "artificial telepathy" apparatus. In this experiment, two subjects (the senders) watched the orientation of Tetris-like pieces and focused on whether the piece should be rotated to align its placement. A third subject (the receiver), located in a different room and unable to see the pieces, was tasked with deciding whether to rotate the piece. The receiver performed well above chance (~81% accuracy) in deciding whether the piece needed to be rotated, based completely upon the signal he received from the senders. This suggests that beyond collecting actionable intelligence, there are presently ever-increasing opportunities for near engineering, potentially for influence or projecting force.

BRAIN MACHINE INTERFACES INTRODUCE NEW ATTACK SURFACES

Significant progress has been made in recent years in the development of both invasive and non-invasive Brain-Machine Interfaces (BMIs), allowing operators to communicate directly with machinery (computers, robotics, cars, artificial limbs, etc.) using only their thoughts (Roelfsema et al., 2018). A quick patent search reveals that over 3,800 patents were filed for such technology in 2018 (Google Patents, 2019). The intimate connection between the operator's brain and the controlled device opens an entirely new dimension of attack surfaces to be exploited by cyber threat actors. Information security primarily rests upon three pillars: Confidentiality (preventing unauthorized disclosure of information), Integrity (preventing unauthorized modification of information), and Availability (maintaining access to information), the so-called CIA Triangle (Wiley, 2008). Within the context of neuro-security a breach of Confidentiality could potentially allow unprecedented access to an individual's most private data, his/her thoughts. A breach of Integrity would mean that an attacker could inject commands into a neuro-device, or alternatively send false feedback to the brain from the device. A failure of Availability would prevent a user from being able to control the device or receive data from it. The failures of any of these pillars might seem to be purely within the realm of science fiction; however, proof of concept attacks have already been demonstrated for each.

Reaching into the uncooperative individual's mind to retrieve, or influence, information is increasingly a reality. Lange et al. (2018) were able to recover partial Personal Identification Numbers (PINs) from subjects' EEG (electroencephalogram) signal. Other research (Roelfsema et al., 2018) has demonstrated the ability to infer the words or concepts that an individual is thinking of, from EEG signals. Without the proper security, individuals using BMIs relying on similar signal processing would be subject to having their private thoughts exposed. Perhaps more disconcerting than breaching Confidentiality is a breach of Integrity; such a breach was demonstrated by Cusack et al., 2017 in a highly controlled environment. In this study, researchers conducted a Man-In-The-Middle attack against a BMI and a toy car and were able to intercept thought-based commands from the user's BMI and inject modified commands. In this case they substituted the command "turn left" with "turn right." If such an attack were launched against an artificial limb or a wheelchair (both of which can now be controlled with similar technology), an attacker could easily cause death or serious physical injury either the user or those around them. In a similar vein, Cusack et al. (2017) describe a simple modification to their integrity-focused attack of flooding the BMI connection with meaningless packets to disrupt the control channel and thereby deny the operator

access to the controlled device. This type of attack, properly timed, could lead to equally destructive results if the downstream device is the artificial limb or wheelchair mentioned above.

FUTURE DIRECTIONS AND NEUROSECURITY CONCERNS

The current state of the art in neuroimaging requires that sensors be placed in very close proximity to a subject's cranium, a state of affairs that many other energetic MASINT sources once shared. Could technology be someday (or presently) capable of detecting neural signals from a distance? While the signal detection difficulties of such a system are great, it is within the realm of possibility. Even such a technology with very limited range would have serious implications for the Intelligence Community, and open the door to covert neuro-surveillance. A few inches might allow an apparatus to be embedded in surfaces, such as seating. A few meters would allow for neuro-surveillance of an interview at a border crossing. More range comes with more interesting, and concerning, implications.

What about individuals who choose to use technology to project their neural information outward? Neuralink, and other industry actors, have this possibility as a direct piece of their value proposition. The idea of computer network-connected brains mirrors that of other computer network-connected sensors: surveillance becomes implicit in return for convenience. Indeed, it may be useful to consider the fact that surveillance capabilities of a covert microphone and a present generation household smart speaker are functionally very little. Covert or overt monitoring of neural activity holds many parallel possibilities, and Biafra mentioned remote neuroimaging is joined by technologies which will intentionally transmit neural information over the Internet, or other networks. It is extremely likely that industry and state actors, in the absence of legislative restraint, will find reason and avenues to collect and leverage such data. The rights of individuals to their own personal neural information, when transported through computer networks, is likely in the process of being decided presently by society and the courts, as rights to personal electronic information are a likely precedent.

Input, as discussed above, is another fascinating dimension of networked neural implants. The ideas are not radical, and indeed Apple and Nucleus, manufacturer of cochlear implants, recently made iOS the operating system connecting to more human implants than any other. These technologies join other apps which can be used to connect to a variety of human implants. In cochlear implants, for example, the intended mode of input is digital audio signals: it is better to listen to your phone call when beamed directly to your implant them through a microphone facing the phone speaker. However, these devices offer opportunities for MASINT, and for influence. Indeed, just as personal information and computer networks can be used for both surveillance and influence, it may be possible to manipulate overtly or covertly a target through an active neural, sensory nerves, or peripheral nervous system connection.

Consider a concerted effort to expose a subject to positive or negative stimulation in response to specific actions. Such a campaign would certainly result in some level of conditioning. We can, for example, imagine creating incentives not to enter a geo-fenced location, or not to leave one. Threat actors with the goal of rendering a target ineffective in their current occupation might leverage a cochlear implant to arrange for painful, annoying, disturbing, or other negative stimulus to be inflicted whenever the target entered their office. They could also simply degrade the quality of the function of the device. Because cochlear implants connect to the Internet through iPhones, this could be accomplished through the malicious employment of code. Note that such an attack would leverage intelligence about use location from the phone, and use the same phone to send negative stimuli to the target through the cochlear implants. Of course, cochlear implants in the United States presently all have removable external units, and could simply be removed. Submitting to deafness in order to remove the stimuli a denial in its own right, it is worth considering that such a scheme would work on other implants, each with its own uncomfortable set of possibilities.

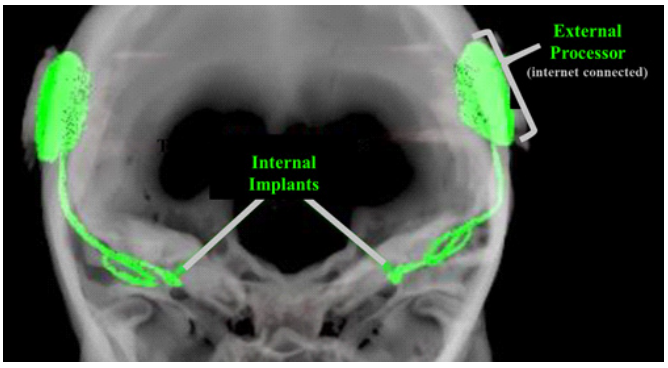


Figure 2: Modern cochlear implants are now compatible with Apple's iOS, which has therefore become a new and widely available attack surface for individuals with this type of sensory nerve-connected prosthesis. Neurosecurity questions exist regarding which central, sensory, or peripheral nervous system-connected devices will soon also be Internet-connected, and whether these have input or output capabilities.

The implications of direct and potential remote neuroimaging are, course, not limited to intelligence, nor to influence, nor to negative outcomes. Neuroimaging, especially remotely,

might prove a particularly robust new form of biometrics, through the recording of an individual's neural responses to specific stimuli, using amenable ERPs, for example. The possibilities for industry, health, and human computer interface are monumental. Interpersonal communication might be revolutionized, or at least improved. However, we believe that this hopeful narrative must be tempered with understanding of the implications to individual and aggregate security. Major questions exist, and at present there are no answers.

OPEN QUESTIONS AND CONCERNS SURROUNDING NEUROIMAGING AS A MASINT SOURCE

In sum, applied neuroscience techniques previously reserved for experts probing scientific questions are now increasingly amenable to MASINT. There are presently multiple scenarios in which intelligence can be gathered through passive monitoring of the electro-optical signals concurrent with brain activity (blood flow and neural discharge patterns), and in the near future such access may become available at greater physical distance. These opportunities are joined by rapid advancements in understanding of the functional organization and temporal signaling of the brain, coupled with rapid advancement in occupational power and machine learning technique quite familiar to the MASINT community. The result is the beginning of an era in which neural information, and the machinations of the human brain, are joining many other systems previously made amenable to MASINT information-gathering approaches. Indeed, the impacts of these combined advances are undoubtedly fueling scattered conversation and innovation in the public and classified spheres of many countries. While some outcomes will be undeniably positive, we feel that there are strong signs that a more focused conversation needs to be held.

Recently, several U.S. embassy workers stationed at Guangzhou, China, have reported symptoms like those reported by U.S. embassy workers stationed in Cuba. Again, there is much controversy surrounding these reports. One widely held assumption is that these are in fact the result of some type of "neuro-attack." Perplexing problems now arise. How could such an attack be detected? Every time your brain forms a new memory (which happens constantly), your brain changes in subtle and poorly understood ways. This constant change makes baselining incredibly challenging, and there remains some question as to whether this is even possible. Moreover, it seems likely that an "input"-based technology, as may be the cause, would be infinitely more detectable than a technology monitoring output. It seems evident that neuroimaging technology holds great potential for MASINT, and for this reason alone there is the likelihood that state-sponsored intelligence services will attempt to employ this technology as an intelligence-gathering technique. The high likelihood of this experimentation, and the relatively feasible nature of creating such a technology, should compel more research to be conducted on a variety of related neurosecurity topics.

It seems evident that neuroimaging technology holds great potential for MASINT, and for this reason alone there is the likelihood that state-sponsored intelligence services will attempt to employ this technology as an intelligence-gathering technique.

Beyond the fundamental question of whether neural tissue is amenable to gathering intelligence, or a likely target for projecting force, fundamental forensic questions which should be addressed by such a line of research are as follows:

How do we ensure neurosecurity? Just as cybersecurity was once poorly understood, so now is neurosecurity. We must understand which approaches are real threats, what their limitations are, and develop understanding as to how our own state, industry, and greater public population can be protected. We must also begin a dialogue in scientific, legislative, and public spheres to address how best to integrate these coming realities into our society. How do we safeguard freedom and security when the information between our ears is no longer inherently our own?

How do we detect attacks? In terms of information-gathering attacks, neurosecurity is likely to suffer from many of the same challenges as cybersecurity; by definition, a well-executed attack need leave no trace (see Hancock, Hancock & Sawyer, 2015). In terms of influence, the more difficult question is one of trust. What is possible in terms of influence, and how can we detect it? Indeed, this is the challenge of cyber-compromised computer systems which serve new masters, or have their cycles turned toward threat actor goals. How do we know when an individual has been attacked? One of the greatest challenges in the "Havana Syndrome" has been establishing whether something in fact occurred. Subjectively, patient reports align very closely (sudden onset, hearing a high-pitched chirping or ringing, difficulty concentrating and maintaining balance), but there is thus far no way to establish exposure conclusively.

Is it possible to develop a baseline? In cybersecurity, understanding of the original state of the system is vital for understanding whether an intrusion has occurred, and how the system is compromised. If a method for detecting a

neuroattack is developed, it will likely involve establishing an analogous neural baselining. The clinical evaluation of Havana Syndrome victims by researchers at the University of Pennsylvania found structural differences between exposed employees and healthy controls. Specifically, structural imaging indicated significantly decreased levels of whole brain white matter, differences in regional gray and white matter volumes, cerebellar microstructural integrity, and functional connectivity in the visuospatial and auditory subnetworks (Verma et al., 2019). While this study found differences between the exposed population and healthy controls, it was unable to demonstrate differences within patients before and after the time of exposure because there was no baseline created prior to their deployment. Another limitation of this study was that it focused on the structural aspects of the patients' neural architectures, but not their cognitive functioning. Baselining to detect a neuro-attack will likely necessitate a cognitive functioning component, perhaps involving rapid response to various stimuli. Developing a baseline of cognitive functioning will likely utilize neuroimaging, for example EEG to measure patient responses to stimuli over time. One of the greatest challenges to this will be understanding whether such baselining is even possible. The brain is incredibly plastic and changes constantly. In fact, every new memory formed causes changes within the brain. An unanswered question is what does "normal" change look like compared to "abnormal" change, and can these differences be detected? If they can be detected, is EEG the right technique, and are EEG responses to stimuli consistent over time? The few answers that presently exist come from vastly different domains in the neurosecurity threat to come.

CONCLUSION: TOWARD A MASINT UNDERSTANDING OF THE BRAIN

MASINT has existed for long enough that the community has witnessed many energetic signals moving from non-useful to pivotal. We here predict that the energetic emissions of the human brain will follow that pattern. Understanding the time frame of that change is difficult. It may take the entirety of our coming careers. It may have already happened. The cause of the Havana Syndrome remains a mystery at the time of this writing. It is also unclear whether Havana Syndrome is specifically the result of a neuro-weapon, or something entirely different. It does, however, provide the opportunity for a timely thought experiment, as the world will witness the effects of neuro-weapons in the foreseeable future. It is critical that tools and techniques be developed to detect the effects of these weapons, and to guard against them. We believe that the framework of MASINT, and the broader Intelligence Community which has such implicit interest in these ongoing developments, is an excellent place to begin this critical work.

References

Cooley, C. Z., Stockmann, J. P., Armstrong, B. D., Sarracanie, M., Lev, M. H., Rosen, M. S., & Wald, L. L. (2015). Two dimensional imaging in a lightweight portable MRI scanner without gradient coils. *Magnetic Resonance in Medicine*, *73*(2), 872-883.

Cusack, B., Sundararajan, K., & Khaleghparast, R. (2017). Neurosecurity for brainware devices.

Dyer, O. (2018). Microwave weapon caused syndrome in diplomats in Cuba, US medical team believes. *Bmj*, 362, k3848-k3848.

Farwell, L. A., & Smith, S. S. (2001). Using brain MERMER testing to detect knowledge despite efforts to conceal. *Journal of Forensic Science*, 46(1), 135-143.

Ganis, G., Kosslyn, S. M., Stose, S., Thompson, W. L., & Yurgelun-Todd, D. A. (2003). Neural correlates of different types of deception: An fMRI investigation. Cerebral cortex, 13(8), 830-836.

Ganis, G., Rosenfeld, J. P., Meixner, J., Kievit, R. A., & Schendan, H. E. (2011). Lying in the scanner: covert countermeasures disrupt deception detection by functional magnetic resonance imaging. *Neuroimage*, 55(1), 312-319.

Google Patents, (2019). Retrieved from https://patents.google.com.

Hancock, P. A., Hancock, G. and Sawyer, B. D., 2015, Cybernomics and the implications of cyber-deception. *The Ergonomist*, 537, 12-14.

Jiang, L., Stocco, A., Losey, D. M., Abernethy, J. A., Prat, C. S., & Rao, R. P. (2019). BrainNet: a multi-person brain-to-brain interface for direct collaboration between brains. *Scientific Reports*, 9(1), 6115.

Kozel, F. A., Johnson, K. A., Mu, Q., Grenesko, E. L., Laken, S. J., & George, M. S. (2005). Detecting deception using functional magnetic resonance imaging. *Biological Psychiatry*, 58(8), 605-613.

Lange, J., Massart, C., Mouraux, A., & Standaert, F. X. (2018). Side-channel attacks against the human brain: The PIN code case study (extended version). *Brain Informatics*, 5(2), 12.

Liu, L., Liu, Z., Xie, H., Barrowes, B., & Bagtzoglou, A. C. (2014). Numerical simulation of UWB impulse radar vital sign detection at an earthquake disaster site. *Ad Hoc Networks*, 13, 34-41.

Macartney, J. D. (2001). John, how should we explain MASINT? *Intelligence and the National Security Strategist: Enduring Issues and Challenges*, 170-171.

Miller, B. L., & Cummings, J. L. (eds.). (2017). *The human frontal lobes: Functions and disorders*. Guilford Publications.

Monteleone, G. T., Phan, K. L., Nusbaum, H. C., Fitzgerald, D., Irick, J. S., Fienberg, S. E., & Cacioppo, J. T. (2009). Detection of deception using fMRI: better than chance, but well below perfection. *Social Neuroscience*, 4(6), 528-538.

Muthuswamy, J., Sridharan, A., & Okandan, M. (2016). MEMS Neural Probes. *Encyclopedia of Nanotechnology*, 1993-2009.

Naseer, N., & Hong, K. S. (2015). fNIRS-based brain-computer interfaces: a review. *Frontiers in Human Neuroscience*, 9, 3.

Ng, E. Y., Kawb, G. J. L., & Chang, W. M. (2004). Analysis of IR thermal imager for mass blind fever screening. *Microvascular Research*, 68(2), 104-109.

Ofen, N., Whitfield-Gabrieli, S., Chai, X. J., Schwarzlose, R. F., & Gabrieli, J. D. (2016). Neural correlates of deception: Lying about past events and personal beliefs. Social cognitive and affective neuroscience, 12(1), 116-127.

Open Water (2018). At https://www.openwater.cc/technology. Poulsen K. (29 March 2008). Hackers assault epilepsy patients via computer. Retrieved 23 September 2019 from https://www.wired.com/2008/03/hackers-assault-epilepsy-patients-via-computer/.

Quaresima, V., & Ferrari, M. (2019). Functional near-infrared spectroscopy (fNIRS) for assessing cerebral cortex function during human behavior in natural/social situations: a concise review. *Organizational Research Methods*, 22(1), 46-68.

Roelfsema, P. R., Denys, D., & Klink, P. C. (2018). Mind reading and writing: the future of neurotechnology. *Trends in cognitive sciences*.

Rosenfeld, J. P., Angell, A., Johnson, M., & Qian, J. H. (1991). An ERP based, control question lie detector analog: Algorithms for discriminating effects within individuals' average waveforms. *Psychophysiology*, 28(3), 319-335.

Sawyer, B. D., & Canham, M., (2019) Neurosecurity: Infosec meets Brain-machine Interface. *B-Sides Las Vegas 2019*. Video at https://t.co/dGIJD9UIH4?amp=1.

Sawyer, B. D., Finomore, V. S., Funke, G., Warm, J. S., Matthews, G and Hancock, P. A., 2016a, Cyber vigilance: The human factor. *American Intelligence Journal*, 32(2), 157-165.

Sawyer, B. D., Karwowski, W., Xanthopoulos, P. and Hancock, P. A., (2016b), Detection of error-related negativity in complex visual stimuli: A new neuroergonomic arrow in the practitioner's quiver. *Ergonomics*, 1-7.

Strickland, E. (2017). Silicon valley's latest craze: Brain tech [News]. *IEEE Spectrum*, 54(7), 8-9.

Tosini, G., Ferguson, I., & Tsubota, K. (2016). Effects of blue light on the circadian system and eye physiology. *Molecular Vision*, 22, 61-68.

Wiley, J. (2008). Security Engineering: A Guide to Building Dependable Distributed Systems. 2nd edition, 239-274.

Yazdani, P. (2017). *Assessing seizure susceptibility using visual psychophysical tests* (doctoral dissertation, Newcastle University).

Dr. Matthew Canham, a psychologist and neuroscientist, is Research Professor of Cybersecurity for the Institute of Simulation and Training at the University of Central Florida in Orlando. His PhD degree in Cognition, Perception, and Cognitive Neuroscience is from the University of California, Santa Barbara. His research focuses on the human aspects of privacy and cybersecurity. Previously, Dr. Canham was a Supervisory Special Agent with the FBI, where he served in the field performing investigations of cyber-breaches, intellectual property theft, and other federal violations. Later, as manager of the Emerging Technologies Program with the Operational Technology Division based in Quantico, VA, he co-authored the FBI briefing for the incoming U.S. Presidential Cabinet on "Technology Based Threats to Law Enforcement in the 21st Century" and provided subject matter expertise to the FBI's Cyber Behavioral Analysis.

Dr. Ben D. Sawyer is Assistant Professor within Industrial Engineering and Management Systems at the University of Central Florida, and Director of the Laboratory for Autonomy-Brain Exchange (LabX). His PhD degree in Applied Experimental Psychology and MS in Industrial Engineering are from the University of Central Florida. At the Massachusetts Institute of Technology, he leveraged biosignals, big data, and machine learning to engineer models of human performance and behavior for the use of machine counterparts. At the Air Force Research Laboratory 711th Human Performance Wing's Applied Neuroscience and BATMAN Divisions, he built mathematical models of human performance for special operations, including cyber operations. His present research, and laboratory, seek to accelerate information transfer between human and autonomy. Dr. Sawyer's design recommendations are leveraged by Fortune 500 companies. His work has been covered by Forbes*, Reuters, Fast Company, and the BBC, and published in leading scientific journals.*

Artificial Intelligence within the Intelligence Community: The Need to Retain the Human Dimension

by LTC (USAR, Ret) Raymond A. Faunt and Col (USMC, Ret) Philip D. Gentile

SCENE-SETTER

On July 20, 1969, Apollo 11 pilots Neal Armstrong and Buzz Aldrin detached their Lunar Model (LM) from the Command Module and began their descent to the surface of the moon.[1] During a period of tremendous political and social upheaval in the United States, on this night it seemed everyone in the country was united, as millions of Americans (and millions of others around the world) listened and watched on radio and television.[2] Both men, not only exceptionally brave and steely-eyed, were brilliant and instinctive pilots who had flown numerous combat missions during the Korean War.[3] Unlike Korea, there was no chance of rescue during this mission; if they crashed or the LM malfunctioned, Armstrong and Aldrin would perish.[4] The LM was a modern marvel, a work of art and science. Most impressive was the actual Apollo Guidance Computer (AGC, what we would now consider a form of artificial intelligence (AI)), which would guide the LM to the surface of the moon.[5] The AGC worked its magic, while Aldrin provided verbal readings from the panel. As they neared the surface, Armstrong turned his attention away from his panel of gauges and looked out his window. What he saw was potentially disastrous; the landing site was covered with debris.[6]

View on the left is the actual 16-millimeter film from Aldrin's window. The view on the right is the reconstructed view of part of the debris field and craters that Armstrong would have seen from his window. His choice to go long on his landing probably saved the mission. AI got Apollo 11 to the moon; Armstrong had to make the decision where to land.

If Armstrong had chosen to follow his ACG blindly, and land the LM at the exact geocoordinates, there was a chance the LM would have crashed on the moon. Instinctively, Armstrong took manual control and began to transverse the surface horizontally looking for a better site.[7] As Armstrong burned precious fuel, he was seconds away from aborting his mission. Finding a cleared landing zone, with approximately 30 seconds of fuel remaining, Armstrong put the LM on the surface and informed Mission Control, "The Eagle has landed."[8] A few seconds later, Mission Control informed Armstrong that he had "a bunch of guys about to turn blue down here."[9] Armstrong and Aldrin had shown the world the ice water in their veins, and put together a winning drive in the closing seconds.

What would have happened if Armstrong had blindly followed his AI? More than likely the LM would have crashed on the moon, or the mission would have been aborted. Quantitatively, the AGC guided Armstrong to the proper location, but Armstrong refused to let AI make a qualitative assessment of his landing zone. He utilized his instincts, training, and experience (his informed mind) for decision-making. Obviously Armstrong was in the act of balancing the quantitative of AI with the qualitative of his experience, training, and judgment. Over the course of the last few years, the U.S. Intelligence Community (IC) has been exploring the pros and cons of AI. With many upsides, AI (if you will pardon the pun) is light years ahead of Apollo 11's AGC.[10] As impressive as AI is, the authors of this work posit that IC professionals must continue to utilize the human dimension of their instincts, training, and experience for decision- making. In the end, history has revealed that the human dimension is often the sweet spot for balancing the qualitative and the quantitative.

HISTORY REFLECTED IN "THE TERMINATOR"

Over the course of the last four years, AI has created tectonic tremors for change within both the federal government and the private sector. The IC has begun in-depth AI research and experimentation and, by all accounts, the promise of AI could be far more spectacular than ever was predicted.[11] Arguments for AI's

progressive advancement are hard to refute; like all technological advances, from the bow and arrow to smart munitions, change is coming via the promise of first-generation AI. In the movie "The Terminator," Arnold Schwarzenegger's character has the ability to rationalize and make innumerable decisions in his efforts to destroy Sarah Connor and her son.[12] Terminator is an example of highly perfected AI in the form of lethal robot technology that can make qualitative and quantitative assessments; the Terminator is AI on steroids (no pun intended regarding Arnold).[13] As history would show us, however, Sarah Connor discovers a way to defeat this technology. Was Terminator's defeat at the hands of Connor due to programmed biases coupled with a lack of balance between the qualitative and the quantitative?

Terminator: Lethal robot technology guided by high-functioning AI.

History is replete with examples of primitive Third World Sarah Connors defeating technologically superior countries. The United States' experience in Vietnam and the Soviet Union's efforts in Afghanistan are primary case studies on this point.[14] These crude Third World armies developed inventive strategies coupled with mitigating tactics, techniques, and procedures to defeat two of the most technologically superior nations the world has ever seen.[15] Quantitatively, the Mujahideen, North Vietnamese, and Viet Cong did not have a chance against the USSR or the U.S. What the U.S. and the USSR failed to recognize was the nationalistic ardor (or total qualitative dedication to the cause of independence, something that is almost impossible to quantify) of the fighting men and women who represented those rag-tag armies.[16] Technological superiority does not ensure victory and always there are ways to defeat technology due to built-in limiting biases and mechanical qualitative/quantitative weaknesses.

Mujahideen irregulars in an overwatch position. The Russian Army unleashed its full arsenal of modern technology against the Mujahideen and, in the end, left Afghanistan defeated.

Minimally equipped and technologically inferior Viet Cong irregulars. The Viet Cong's spirit and willingness to see the cause through to the end, no matter the cost, far outweighed its technological inadequacies.

AI: ENDLESS QUESTIONS

For the IC, the programmatic infusion of AI into the mix provides unlimited strategic and tactical possibilities for the end user. Where does this all leave the U.S. IC when it comes to AI? The questions are innumerable, from the tactical all the way to the strategic: Just how much power do we give to AI? Using history as a guardrail, it would border on the criminally negligent not to cast a suspicious eye on AI and ask direct questions. The ultimate question is: What are the limits of AI, and how much power do we give it? Would AI provide a false sense of security, when in fact the sentinel on the fence line is just as effective? How much do we allow AI to make decisions for us? Will AI inundate us with so much intelligence data that our ability to make rational decisions is overwhelmed? With the advent of AI, will our cognitive rationality begin a slow and steady decline? Will we be on the verge of a Forbin Project?[17]

> Forbin is the designer of an incredibly sophisticated computer that will run all of America's nuclear defenses. Shortly after being turned on, it detects the existence of Guardian, the Soviet counterpart, previously unknown to U.S. planners. Both computers insist that they be linked, and after taking safeguards to preserve confidential material, each side agrees to allow it. As soon as the link is established the two become a new Super-computer and threaten the world with the immediate launch of nuclear weapons if they are detached. Colossus begins to give its plans for the management of the world under its guidance. Forbin and the other scientists form a technological resistance to Colossus which must operate underground.[18]

Some believe the dumbing down of mankind is a very real possibility:

> In the long term, an important question is what will happen if the quest for strong AI succeeds and an AI system becomes better than humans at all cognitive tasks. As pointed out by I.J. Good in 1965, designing smarter AI systems is itself a cognitive task. Such a system could potentially undergo recursive self-improvement, triggering an intelligence explosion leaving human intellect far behind. By inventing revolutionary new technologies, such a superintelligence might help us eradicate war, disease, and poverty, and so the creation of strong AI might be the biggest event in human history. Some experts have expressed concern, though, that it might also be the last, unless we learn to align the goals of the AI with ours before it becomes superintelligent.[19]

For the IC, the programmatic infusion of AI into the mix provides unlimited strategic and tactical possibilities for the end user.

Can we eliminate biases within AI and ensure it provides the best possible answers? This brings to mind the crucial question: Where do programmatic designers of AI strike the balance between the qualitative and quantitative nature of the data that AI provides to the end user? In the end, could AI give us the intelligence edge that puts us light years ahead of those who would wish our nation harm? Or could an improper programmatic weighting of factors of the qualitative and quantitative data, coupled with biases, leave us vulnerable?

AI: STRIKING THE BALANCE BETWEEN QUANTITATIVE AND QUALITATIVE WHILE MITIGATING BIASES

Social media companies are experiencing the initial teething stages that are associated with any new technology; specifically the continuous monitoring mission (to detect bad actors) has been assigned to AI.[20] In an effort to regulate content, AI is being used as a sentinel.[21] Many of these companies are working through rules-based content identification coupled with policy-based restrictions.[22] Because of this, these companies have a monumental job in constantly tweaking the rules in order to cull out the "bad stuff" they do not want posted.[23] Their application of a quantitative approach is showing flaws: First, application of mechanical policy rules to data is not smooth and all-encompassing. Currently, companies are in a continuing reactive cycle (versus proactive) while continually seeking to make/adjust their rules in order to identify malicious material, treat it and, if required, block or revoke user privileges. Second, defining what is allowable is subjective (what some find offensive, some find not offensive; therefore, who decides?) and not mechanical, although online bad actors are treated as mainly a mechanical problem. The ultimate point is that the quantitative side by itself is not effective, or reflective of what is "right." Nevertheless, with AI we most often rely on the quantitative for "right." In and of itself, that is what shows the limitations of AI and how it may possibly be tricked or defeated. Depending on the company, and the individuals within those companies who will design and build the AI, there could be problems because their own biases have entered into the mix during the design of the system.[24]

The need to balance properly the qualitative to quantitative is paramount, especially when it comes to relying on information for intelligence purposes.

Increasingly, the idea of truth is being examined and we are seeing that bias and judgment (and abuse thereof) are alive and well today, as they were in past decades. The idea that data is agnostic of politics, or biases, and speaks only truth, is just not a credible assumption. A key takeaway is that qualitative thinking or qualitative expertise has its faults and biases; however, qualitative thinking is able to scrutinize the problem in a different, experienced-based light, adding important yet different perspectives to addressing a problem. The need to balance properly the qualitative to quantitative is paramount, especially when it comes to relying on information for intelligence purposes.

AI UPSIDE AND HUMAN DIMENSION

This should not give the reader the idea that all AI will turn into the Terminator or is fraught with interminable hazards. The problem resides more in its programming, monitoring, and proper usage. AI has more than proven its worth in hundreds of scenarios. Still, the need to maintain a human element of control and judgment is paramount. Yet, even the human element can commit fatal errors. There are dozens of examples of friendly fire instances where the AI contained within an attack munition did exactly what it was supposed to do, but human error/judgment caused the tragedy. During a more recent experiment, it was found that "AI was on par with human experts when it comes to making medical diagnoses based on images…"[25] Therefore, the question must be asked: Can AI stand by as a sentinel to prevent errors in human judgment, and where do we find this type of programmatic balance? As previously stated, AI upsides are innumerable, but especially within the Intelligence Community we cannot surrender our judgment to AI. In a fact-based society (especially when facts are relative to a key stroke and click), the IC must temper its desire to surrender to AI without maintaining the human dimension.

There is value with AI in technology-on-technology scenarios, such as a nuclear defense missile shield. Once the nuclear warhead is launched (detected through technological/AI-type means), AI will take over and guide our friendly missile toward the threat missile and shoot it down. However, human judgment is required to make that final call to launch the defensive missile. Within the fact-based virtual environment of today's world, it remains for the human element to weigh and sift the nuanced issues that AI is unable to analyze qualitatively. Is human judgment infallible? As previously stated, no, it is not, but the human dimension cannot be removed from the decision-making process. The authors would submit that AI can provide, but only in clearly defined scenarios should it decide. The ability to properly measure and define size and weights of missiles, tanks, boats, and planes can reside within AI and is of tremendous benefit. The U.S. drone program (an AI-type program overseen by a human dimension) has enabled the U.S. to remove enemy combatants from the terrorist mix, whereas in decades long past we had to wait dozens of years to capture a wanted terrorist. Ultimately, the IC must decide what it is willing to allow AI to do.

In a fact-based society (especially when facts are relative to a key stroke and click), the IC must temper its desire to surrender to AI without maintaining the human dimension.

In 2005, Israeli satellites detected a building deep in the desert of Syria.[26] An analyst immediately became suspicious—a building in the middle of the desert—why?[27] After comprehensive efforts to assess the building technologically, the Israelis came up with no answers; above all, the building was not constructed in the correct fashion to be a nuclear facility.[28] After conducting comprehensive all source intelligence collection and analysis (to include human intelligence operations in draining a Syrian scientist's computer in Vienna and sending the Sayaret Matkal to collect soil samples from near the suspect building), it was determined the Syrians were building a nuclear facility.[29] The Israelis promptly took military action and destroyed the building via an airstrike.[30] The human dimension provided the facts for the moral justification to take armed action. The question that should arise from this is what would have happened if this satellite was programmed to notify an analyst only in the case of remote buildings being designed in the common fashion for nuclear facilities? If an analyst relied on the AI to notify him, more than likely Syria would be well on its way to possessing a nuclear capability.

SUMMARY AND CONCLUSION

In summation, the authors would submit that, while AI presents unlimited if not unparalleled benefits to the IC, we must not allow it to make ultimate decisions for us. Stripping out the human element, or making the IC

process devoid of the human dimension, could possibly lead to a loss of cognitive processes or, much worse, lead us down the path of the Forbin Project. When it comes to our nation's national security, we should look for and, if necessary, adopt every technological advantage that ensures our strategic superiority. As the world becomes more lethal, and with the proliferation of nuclear-armed nations, our very survival depends on our ability to one-up our opponents. The authors would submit the ultimate one-up is the active and engaged human dimension that processes nuances of the ever-changing, asymmetrical, network-centric world.

NOTES

[1] Craig Nelson, *Rocket Men: The Epic Story of the First Men on the Moon* (New York; Viking, 2009), 236-276. Kenneth T. Walsh, "1968: The Year that Changed America Forever," *U.S. News and World Report*, December 31, 2017, https://www.usnews.com/news/national-news/articles/2017-12-31/1968-the-year-that-changed-america-forever.

[2] Chris Gibbons, "The Pilot Who Saved Apollo 11," *Orlando Sentinel*, July 20, 2019, http://www.orlandosentinel.com/opinion/guest-commentary/os-op-apollo-11-armstrong-20190720-qyoot6lxrvgqnoyvuvfu2btrnu-story.html.

[3] Nelson, 49-54, 44-46.

[4] James R. Hansen, *First Man: The Life of Neil A. Armstrong* (New York: Simon and Schuster, 2005), 200.

[5] David G. Hoag, *Apollo Navigation, Guidance, and Control Systems: A Progress Report* (Cambridge: Massachusetts Institute of Technology, 1969), 1-2.

[6] Nelson, 236-276.

[7] Ibid.

[8] NASA, "The Eagle Has Landed," Mission Pages, https://www.nasa.gov/mission_pages/apollo/apollo11.html. Space Log, "Transcripts Phase 6 on the Moon," https://apollo11.spacelog.org/page/04:06:46:06/. After landing, Armstrong explained why he had taken over manual control, saying, "Hey, Houston, that may have seemed like a very long final phase. The AUTO targeting was taking us right into a football field size—football field sized crater, with a large number of big boulders and rocks for about…one or two crater diameters around it, and it required a…in P66 and flying manually over the rock field to find a reasonably good area."

[9] Space Log, "Transcripts Phase 6 on the Moon," https://apollo11.spacelog.org/page/04:06:46:06/.

[10] Jackson Barnett, "AI Is Breathing New Life into the Intelligence Community," *Fed Scoop*, August 21, 2019, https://www.fedscoop.com/artificial-intelligence-in-the-spying/.

[11] James Manyika and Jacques Bughin, "The Promise and Challenge of the Age of Artificial Intelligence," McKinsey Global Institute, October 2018, https://www.mckinsey.com/featured-insights/artificial-intelligence/the-promise-and-challenge-of-the-age-of-artificial-intelligence.

[12] IMDb, "The Terminator," https://www.imdb.com/title/tt0088247/.

[13] Ibid.

[14] Mohammad Yousaf and Mark Adkin, *Afghanistan Bear Trap: Defeat of a Superpower* (Havertown, PA: Casemate, 1992), 25, 42, 48-49, 207-219. Bruce Riedel, "Comparing the U.S. and Soviet Experiences in Afghanistan," *West Point Combatting Terrorism Center*, May 2009, Volume 2, Issue 5.

[15] Max Boot, *Invisible Armies: An Epic History of Guerrilla Warfare from Ancient Times to the Present* (New York: Liveright Publishing, 2013), 413. Steven M. Walt, "I Knew the Cold War: This Is No Cold War," *Foreign Policy*, March 12, 2018, https://foreignpolicy.com/2018/03/12/i-knew-the-cold-war-this-is-no-cold-war/.

[16] Jack A. Goldstone, "Introduction: The Comparative and Historical Study of Revolutions," *Revolutions: Theatrical, Comparative, and Historical Studies*, 2nd ed., Jack A. Goldstone, ed. (New York: Harcourt Brace College Publishers, 1994), 1-17. Boot, 413-426, 485.

[17] "Collossus: The Forbin Project," https://www.imdb.com/title/tt0064177/.

[18] Ibid.

[19] Future of Life, "Benefits & Risks of Artificial Intelligence," October 1, 2019, https://futureoflife.org/background/benefits-risks-of-artificial-intelligence/?cn-reloaded=1.

[20] Rion Graham, "Using AI to Fight Against Bad Actors in Social Media," *Analytics Insight*, June 1, 2018, https://www.analyticsinsight.net/using-ai-to-fight-against-bad-actors-in-social-media/. "Facebook Teams Up with Police to Stop Streaming of Terror Attacks," *The Guardian*, September 17, 2019, https://www.theguardian.com/technology/2019/sep/17/facebook-teams-up-with-police-to-stop-live-streaming-of-terror-attacks. Senate Committee on Intelligence, United States Senate, Russian Active Measures Campaigns and Interference in the 2016 Election, October 8, 2019, https://www.warner.senate.gov/public/_cache/files/0/d/0dc0e6fe-4d52-49b0-9e92-a15224a74a29/C2ABC2CD38BA3C5207D7FA5352D53EC2.report-volume2.pdf.

[21] Rion Graham, "Using AI to Fight against Bad Actors in Social Media," *Analytics Insight*, June 1, 2018, https://www.analyticsinsight.net/using-ai-to-fight-against-bad-actors-in-social-media/.

[22] United States Patent Office, "Automated Adjustment of Content Composition Rules Based on Evaluation of User Feedback Obtained Through Haptic Interface," November 13, 2018, https://patentimages.storage.googleapis.com/91/72/82/c9bd538698207c/US10126818.pdf.

[23] Taylor Lorenz, "Instagram Has a Massive Harassment Problem," *The Atlantic,* October 15, 2018, https://www.theatlantic.com/technology/archive/2018/10/instagram-has-massive-harassment-problem/572890/.

[24] John Villasenor, "Artificial Intelligence and Bias: Four Key Challenges," Brookings Institution, January 3, 2019, https://www.brookings.edu/blog/techtank/2019/01/03/artificial-intelligence-and-bias-four-key-challenges/.

[25] "AI Equal with Human Experts in Medical Diagnosis, Study Finds," *The Guardian*, September 9, 2019, https://www.theguardian.com/technology/2019/sep/24/ai-equal-with-human-experts-in-medical-diagnosis-study-finds.

[26] Judah Ari Gross, "Ending a Decade of Silence, Israel Confirms It Blew Up Assad's Nuclear Reactor," *The Times of Israel*, March 21, 2018, https://www.timesofisrael.com/ending-a-decade-of-silence-israel-reveals-it-blew-up-assads-nuclear-reactor/.

[27] Yaakov Katz, *Shadow Strike: Inside Israel's Secret Mission to Eliminate Syrian Nuclear Power* (New York: St. Martin's Press, 2019), 33-34.

[28] Ibid., 34, 44-45.
[29] Ibid., 15-43, 159-166.
[30] Ibid., 182-188.

LTC (USAR, Ret) Raymond J. Faunt is a retired infantry officer in the Army Reserves and also served as an enlisted man in the U.S. Marine Corps Reserves. He currently works as a contract Senior Policy Advisor within the Intelligence Community. He served 28 years (17 on active duty) in command and staff assignments within the light, mechanized, special operations, and intelligence communities. An Operation IRAQI FREEDOM veteran, he has educated and trained military personnel from the Caucasus region. He is a graduate of the Air War College through distance education. He has earned five master's degrees and three graduate certificates. Most notably he holds an MSSI (with a concentration in Foreign Denial and Deception) from the National Intelligence University, an MA in Strategic Studies (with a concentration in Counterterrorism) from National Defense University, and an MA in National Security and Strategic Studies (with a concentration in Insurgency and Terrorism) from the Naval War College. Ray is a frequent and valued contributor to AIJ.

Col (USMC, Ret) Philip D. Gentile is a 30-year career Marine Corps intelligence officer with extensive experience spanning the tactical, operational, service, and joint intelligence levels. He has commanded a platoon, a company, and an intelligence battalion, and culminated his command time as the Commanding Officer of the Marine Corps Intelligence Activity in Quantico, VA. His principal staff assignments include Chief of Staff to the Director of Marine Corps Intelligence; Senior Military Assistant to the Undersecretary of Defense for Intelligence; Deputy G2, Multinational Forces West in Al Anbar, Iraq; G2, 1st Marine Division; and S2, 26th Marine Expeditionary Unit, Special Operations Capable. He is a graduate of DIA's Postgraduate Intelligence Program and earned master's degrees from both the Marine Corps Command and Staff College and Johns Hopkins University's School of Advanced International Studies.

Ethics and Morality in the U.S. Government and How the Intelligence Community Must Respond

by Dr. Gus A. Otto

[Author's Note: The views & opinions expressed in this article are those of the author and do not reflect the official policy or position of any agency of the U.S. government.]

OVERVIEW

Ethical by accident.
Moral despite the accidents.
Lucky most of the time . . . and we can't keep counting on it!

This is how I describe the U.S. government (USG) and its Intelligence Community (IC) day to day. Furthermore, in this day and age, without correction we will continue to keep hobbling along. Worse, we risk dilution and even real catastrophe if we continue to accept the status quo. Why? Because we are better than that for starters. It is not malicious—I know. It is because we know we can do better, and we need to stop being lazy and put the work in. We cannot wait for the next dilemma to strike, and then wrestle with it only after failure. We must act now to prepare ourselves for the inevitable dilemmas we will all face at the individual, organizational, and institutional levels.

This is how I start most conversations with my bosses, peers, and colleagues and those who the hierarchy calls "subordinates." Most agree. They then surrender because they feel like they are fighting an enigmatic struggle against the unattainable. When we get together to share a drink, break bread, or relish a brief pause in the unyielding grind of the day, we just do not have the energy to do more. Therefore, this article is intended to provoke, to solicit response, and maybe compel the "System Lords" to help. Passing the responsibility to the lawyers and chaplains has resulted, for too long, in the abdication of responsibility by leaders to create a climate and culture of ethical and moral behavior.

For nine years, after I started many of my classes in the Professional Military Education (PME) arena, I played a trick on my students. Many were senior military officers, including generals, and senior civilians, plus the occasional executive. After introductions and some rapport building, I got serious. I asked how many had read the U.S. Constitution. A few reluctant hands went up. I asked how many had read it lately. Fewer hands raised. Then the bomb . . . I asked who had taken an oath to the U.S. Constitution. A couple of "spring-butts" raised their hands before the logic bomb detonated in their minds. Others' wit restrained their hands, though not their grimace. Throughout the rest of our time together, we sought to weave ethical and moral behavior into our discussions. To this day, former students, old colleagues, and the occasional senior ask me how to move toward a more ethical and moral world, guided by shared values found in the U.S. Constitution. There are no easy answers and, unless we address them, we will continue to muddle through. I prefer to muddle less.

DEFINITIONS

For this discussion, we need more than an obligatory definition; we need a common point of departure. *Merriam-Webster* defines "ethical" in a couple of ways, including "involving or expressing moral approval or disapproval . . . conforming to accepted standards of conduct . . . ," and then goes on to offer broader ways to define it including a "kid's definition . . . involving questions of right and wrong" and finally the "legal definition . . . conforming to accepted professional standards of conduct."[1] Each of these is meaningful and relevant to the rest of this article. *Merriam-Webster* similarly defines "moral" in many ways to include "expressing or teaching a conception of right behavior . . . sanctioned by or operative on one's conscience or ethical judgment . . . moral practices or teachings: modes of conduct."[2] For the purposes of this article, I propose a standard where we keep these definitions, and restrict the ethical to the organizational or institutional and the moral to the individual domains.

Finally, there is the law. Some argue the law comes about when there is a consensus, yet not always a clear majority, or acknowledges a meaningful minority opinion. Others suggest laws come about because there is a need that lacks consensus. Still others note that laws can be dictated, as was often the case throughout human history. Dr. Christopher Bailey acknowledges that many believe the law may become a socially acceptable point.[3] Activities can be legal and not moral or ethical. Activities can be moral and ethical yet not legal. Distinguishing how we think and

behave among these different definitions is important because it closes out the point of departure in the discussion. Merriam-*Webster* defines the law in many ways, including "a binding custom or practice of a community; a rule of conduct or action prescribed . . . or formally recognized as binding or enforced by a controlling authority."[4] The law is not always clear, and for members of the USG it is constantly refined and gray areas slowly resolved. However, there may still be moral and ethical challenges we face. Debate abounds on these issues, so it is best to delineate them this way for now.

Ethical and moral do not result in or equate to legal. For years, it was legal to enslave people, or deny women voting rights; yet, we can now agree this is both immoral and unethical and ***finally*** illegal. Human history is replete with these kinds of examples. Law often results when (1) society has consensus or general agreement, or (2) society cannot decide, and therefore leaders such as elected officials, courts, monarchs, or strongmen decide for them. I do not want to debate the law. I do want the USG and the IC to discuss, debate, and even argue about ethics and morals. The easy right and wrong answers of the world are not the ones we face. They are not the ones that haunt our dreams and drive insomnia. Instead, increasingly complicated dilemmas lay on the horizon, even if we do not see or acknowledge them. We must engage these dilemmas head on, and to do so we must have the mental wherewithal to unpack complex challenges where there is no easy, or even optimal, answer to a particular dilemma.

WHAT IS A DILEMMA?

I subscribe to the notion discussed by Dr. Karen Allen, who suggests there are two types. In the first type, there are pure dilemmas where more than one ethical standard opposes another. In these cases, one standard often is chosen over another. Though seldom binary, these point to a preference or ranking of one's individual moral framework, or an institution's ethical code (explicit or implied). An example I face often is the need to take care of people while achieving the mission, or vice versa. Like so many other organizations, my own Defense Intelligence Agency (DIA) has a clear enough mission, one I subscribe to on an ethical basis. I also believe this mission is one we, as members of DIA and the IC, have a moral obligation to fulfill. However, part of this obligation is taking care of our team members, our fellow citizens, and our sisters and brothers in humanity. When a member suffers a personal crisis, injury, or chronic affliction, do we pause and thereby impair or disrupt mission success to care for the person? It depends. Our default is often what the law says, rather than what our ethics and morals tell us. These classic issues are often pitted in a "mission first" or "people first" dilemma, when in reality there may be many other ways to solve a problem without damage to the person or organization.

The second kind of dilemma is more vexing—often referred to as an approximate dilemma. Allen tells us that in approximate dilemmas the friction lies between an individual who has a choice or set of choices, within other contexts as organizational polices, laws of a country, or regulations of a government. These require a dissection of issues relevant to the decision, and an understanding of organizational precedent.[5] No easy answers lie here either. One classic example is the whistleblower's dilemma. In this case, is something so bad one is compelled to fix it himself/herself? Is it something systemic he/she chooses not to blow the whistle about, and instead takes on the system within the constraints and the behaviors of the system? At what point does a member or team fall on its proverbial sword? Is there a more right or less right answer? Who makes these judgments? All of the answers are "it depends."

Some argue there is a third kind of dilemma in which a conflict exists between two principles—one where a principle is violated so another may be followed. For example, can we justify killing to save the lives of others? Is war justifiable because it is to save the world from ethnic cleansing or nuclear devastation? Some ethical and moral principles must be temporarily ignored so other hard-pressing dilemmas can be solved. My preference places this kind of dilemma into the approximate dilemma category above. In this case, we can consider the broad moral implications regarding "Just War Theory" or the "Responsibility to Protect" as very real conundrums.

It is not important if one subscribes to two or three types of dilemma. What is crucial is the constant inner dialogue and reflection that drives critical thinking. Parallel to these often-silent inner discussions, group and societal discussions should ensue. Leaders must advance these discussions in the workplace. Current events are loaded with moral and ethical opportunities. The most valuable of these discussions can focus on the hardest questions to answer. When these conversations unfold, answers may not always be clear or even exist. Nonetheless, they are essential to the advancement of moral and ethical behavior in the government and its institutions.

RATIONALE

Too often people talk about rationality and irrationality. I am not a member of the American Psychological Association, or a psychologist, and I am in no way offering a diagnosis. The accusation is one person or another is "irrational" when there is little or no evidence to support that assertion. In other cases, some use a "rational man" argument. This is really a veiled *ad hominem* fallacy or attack to seek superior advantage over another, or to mislead another in a debate. Sometimes it is witting, and other times it is naïve or unintended. This is important to the

discussion; just because a person does not subscribe to or align with your rationale does not make him or her irrational. Yet, the rational man fallacy often is used to diminish others, presuming our own rationale is superior. For the purposes of argument, I will define "rational" as taking a logical approach to a solution consistently and predictably. Using this definition, we can look at world leaders and ask if North Korea's Kim Jung Un is rational. If we understand his logic, his contexts, and his perceptions, then he is rational. On the other hand, based on his behavior available in the media, Muammar Gadaffi, the now-deceased leader of Libya, was irrational. It would not be fair or right to characterize his private behavior, because we lack sufficient data. Using the definition, his consistency and predictability were lacking, even when we cannot always conceive of his context and perceptions. Both men demonstrate unethical behavior and drive immoral activity on the international stage.

Finally, there is the issue of perception of time and historical considerations (how our opinions of ethical/moral behavior may change over time). When we are faced with a crisis, many of us feel we need to make decisions quickly so we can resolve the issue and move on or pass it off. Many of our systems incentivize this notion. We reward leaders for being decisive, even when they risk being wrong, unethical, or immoral. This is not always bad; instead, what is important is developing the judgment to know when a decision should not or cannot be rushed.

SEASONING

As we consider past decisions, whether we learn from them, or whether we incorporate them, do we become wiser? I mentioned the issue of law versus ethics and morality when it came to women's right to vote, or emancipation of people of color, particularly black and African-Americans who were enslaved. Our historical lens encourages us to grapple with the moral and ethical aspects of how the people in that time ***ever*** thought it was acceptable. It was ***never*** acceptable. This is an important thought process to go through nonetheless, even if we may never have a full understanding of the issues. Getting a legal opinion is important, though may be easier than making a moral or ethical decision. More recently, we might think about some of the moral and ethical dilemmas we faced personally and as a nation. There is no shortage of dilemmas from the headlines to keep our brains engaged and our conversations fruitful—pick one!

When making a decision during these dilemmas, keeping in mind the context, timing, and principles is challenging at best, and can paralyze if not cripple. Is it right? Who says? Does it change over time and, if so, why? The dilemmas abound and the answers are not easy; neither is getting to them. For example, in recent congressional hearings for political appointments many were asked how they felt about *Roe v. Wade*, or how they felt about *Brown v. Board of Education*. In the IC we are bombarded by questions about privacy versus security.[6] We are faced with making analytic leaps distinguishing a terrorist from a freedom fighter. Have you done a targeting package? How did you decide the location, or if the person was a legitimate target? Can a person even be a legitimate target? None of these issues has clear-cut or easy answers. The crux of the matter? There is no government-provided roadmap to get here. The USG and the IC do not provide us with the tools we need to get to these decisions. When and if they do, we are often decades into our public service, as were my students in PME. We do not talk about this enough, and when we do the response is half-baked, ill-conceived, and lacks the right emphasis.

Finally, the solution is NOT, repeat NOT, dumping training and discussion regarding ethics and morals on the Chaplain Corps or the lawyers once a quarter in a town hall meeting that might be half-attended. This is not a slight to either profession. Instead, it is an acknowledgment that chaplains and lawyers are advisors, and do not have a corner on the ethical and moral market. Yes, we expect them to have unique viewpoints, and be well informed and contemplative. The more people with whom we can consult, the richer our decisions can become. However, leaders must make decisions more holistically. Some have abdicated their responsibility to make decisions and echo what their lawyer or chaplain provides. This is not the answer, and such abdication in itself risks being morally and ethically flawed. The key is developing a good baseline of ethical and moral thinking and discussion. What follows are a few primers for those discussions.

TROLLEY CAR CASE

This is a classic introduction to ethical dilemmas that merits restating here to establish three of many baselines for further discussion. Essentially, a runaway trolley car is headed down the track.[7] At the end of the track is a team of workers, unaware of the threat careening toward them. Without a course change, it will surprise the workers and kill them all. However, you have the ability to pull a lever, redirecting the trolley car to a different rail, and a child is playing on the other track. Do you choose to let the group of workers or the child on the other track die?

Most people choose to let a single person die, rather than the larger group, even if it is a child. This example, almost cliché in the ethical and moral arena, gives us a chance to discuss why we might make this decision. Like Mr. Spock in "Star Trek – The Wrath of Kahn," who states, "The needs of the many outweigh the needs of the few . . . or the one,"[8] we

choose a numerical solution that allows us to maximize the outcome by saving multiple lives versus one. Alone this utilitarian or virtue ethics view might be acceptable. Others over the years have offered alternative solutions or caveats. For example, what if the child was the one who would someday invent the cure for cancer? What if the work crew were all convicted murderers?

It is reasonable to ask how the law would treat these scenarios. The answers are as great in number as they are in variety. Even the law allows for context as set in this scenario. For example, there may a legal determination after the fact that there was no good decision; hence, no action was required. There might be a compelling argument for action ***before*** this situation occurred. In other words, how did this predicament come about? Despite a rich litigious debate, there remain all the moral and ethical points to ponder.

Using the same scenario, now what if the child were ***your*** child, niece, or grandchild? How does this change the equation? When presented with this new twist, most people choose to let the workers die, rather than their kin or loved one.[9] As I struggled with the twists of this dilemma, I discussed it with my young son and found new ideas. I asked him, if the lone person on the second track were his dad—me, what would he do. When done, I told him, if he chose to kill me instead of the others, then I would be proud of his decision. Heavy? Yes. However, children need this kind of engagement as much as our adult colleagues do. With the many twists for this scenario, we are frustrated because we do not have these answers; yet, it is this kind of questioning that is most valuable. We talk about this at the conference table and the kitchen table. And we need more.

UBL AND TORTURE

The next scenario comes from Benjamin Wittes (2009) inhis unique consideration of torture and national security in the book *Law and the Long War: The Future of Justice in the Age of Terror*. In the book we are presented a fictional scenario where Usama bin Laden's (UBL) first wife, and their first-born sons, had been apprehended. The U.S. captors separated them and believed the wife knew UBL's whereabouts. The wife is in an interrogation room, with a window facing an airfield. She can see her adult sons, shackled and hooded, being led to an airplane preparing for departure. The captors give her a choice: tell us where UBL is or your sons will go to a country popular for torturing their captives that often results in death. Is this torture? Would ***you*** do it?

Countless times I presented this dilemma to senior officers and civilians including flag officers and department-level heads. They love the discussion that ensues. They also admit, often shyly or angrily, they do not have, or had little of, the mental framework to unpack such a complicated case. My family and friends have enjoyed this discussion over a meal or drink, and learn a lot when we talk about it. However, this is not talked about in the workplace; it is not a widely discussed topic, but it must be. What do you think? Is it torture? Would you do it?

We are in luck! This has already been decided for us. The law is clear, even if your own ethics and our organizations have not taught us more about it, leading to our social morals. The law states this is a very clear example of torture because it causes undue mental distress.[10] UBL's wife would be in duress. Would you do it? Certainly many others have in situations like this. Does this make it right? What if there is no permanent physical damage? What if no one found out? Does finding UBL after her confession make it right? I do not think so, but that is for another article. What is important is that we know torture, including this kind, does NOT work. There is ample data and even more anecdotes by victims of torture that show the person being tortured eventually will tell the torturers whatever it is he/she thinks they want to hear.

A globally recognized expert because of his years in a POW prison and a victim of regular torture, the late Senator John McCain (R-AZ) edified us all on the topic during his statement to Congress in early December 2014. I encourage everyone to watch this event and think about the role ethics, morality, and the law play in our national security.[11] Senator McCain cautions humanity against the slippery slope of torture for any reason, and how it clearly opposes the principles of the United States, its founders, and the U.S. Constitution. Mental anguish and duress are only a small part of the larger issue regarding torture. These and other severe measures present an omnipresent opportunity to discuss ethical and moral behavior.

There is a little more to the story. The UBL scenario Wittes presents is a contemporary twist on the post-World War II apprehension of Rudolph Hess in 1946 for the Nuremburg Trials. The British captured his wife and three sons, though not their daughter. Instead of a plane it was a train, and it was headed to communist-controlled Eastern Europe, where they would surely be tortured and killed. At the time, there was no international community outcry for a variety of reasons. Does the lack of outcry make it right? We know the law; how does it make us feel? What can we learn from both of these scenarios placed in different historical context?

KING DAVID

Where there was no international outcry in the previous case, the fall from grace by General David Petraeus was covered well in the media, and around water coolers in the United States and abroad. This convict's behavior included providing sensitive and classified material to the woman with whom he was having

an adulterous affair, who happened to be writing a biography on him. For this case study, I like the provocation from one of my CIA colleagues who catches people's attention by telling them Paula Broadwell was discovered to be a Russian agent. Russians and their Soviet predecessors employed "honey traps" throughout the Cold War and since. Imagine the uproar in the halls of the IC when they discover that not only one of their former leaders disclosed life-changing national security information to satisfy carnal yearnings, but then learn she was actually a spy for Russia! A lothario like this is disgusting, and the actions profoundly dangerous to any nation.

Fortunately, there is no indication Ms. Broadwell had these kinds of ulterior motives. Does it make the crime any less dire? While the law will distinguish shades of gray in words and crimes like "treason," "espionage," and "sedition," the actor (Petraeus) did not limit himself based on intent, or the knowledge his co-conspirator was not going to share the information. Does this mean he was ethical? Was Broadwell ethical for taking the information? What about Petraeus? Some argue his willingness to step down was an ethical move. Was it? Was it damage control instead because he was caught? Was this just an indicator of other secretive behavior that had not yet been discovered? What about his distinguished performance throughout his military career—should it be a mitigating factor in his sentencing?

In the end, while many argued for harsher punishment, Petraeus was charged with a misdemeanor, levied a $100,000 fine, and given two years' probation. Would a less public figure have it better or worse? Was there a double standard? Should lower-ranking people receive more severe punishment?[12] In the end, most press speculate and report that due to the high publicity and sensitivity of this case it made sense to settle it sooner and avoid more national-level exposure to sensitive topics. Having these discussions is crucial to the development of our own ethics, and also the shaping of our organizational and institutional morality. I challenge people to show where this is a deliberate part of professional development across the USG outside of the military and academic centers.

PROFESSION OR A JOB

On the heels of any discussion about Dave Petraeus is an important dialogue about the notion of profession. I believe being a government leader, and especially an intelligence officer, is a profession. The military is considered a profession much like lawyers or doctors. We often refer to this as a "Profession of Arms."[13] They all have explicit ethics codes; we have all heard about the Hippocratic Oath. From this grows a professional ethic and morality, followed by policies, regulations, and governing laws. Certainly attempts have been made over the years to create or become a profession like those elsewhere in the USG and IC. However, there is little quantifiable evidence a true profession exists. Hard attempts have been made but there is no codification, no formal obligation, and no social contract beyond an oath of office we all take when we join U.S. Civil Service.

With all this as background, the good news is we are generally ethical and moral. There is also a growing recognition among some senior leaders that this is a problem we must address. In 2013 when I was teaching a class on this topic, there was not even a USG or IC ethic. Where there were subordinate ones, they were buried next to the "contact us" and "sitemap" sections of their website, and lacked any meaningful support or additional context. Even the Office of the Director of National Intelligence (ODNI) did not have one. Today it does.[14] Far from perfect, it is a good start. A fistful of next steps for the USG and IC to take remains.

RECOMMENDATIONS

There are no easy answers for any of these questions. Further, there are no easy solutions to help us better discuss ethics and morality. I am often dismayed by the lack of mind tools, classes, resources, and roadmaps available to our people on this topic, but I cannot just issue a book to read, or develop an online training program. The grist of the mill only comes through hard, repetitive work on the topics of ethics and morality. What follows are some basic ideas to seed a field leading to more fruitful understanding of these deep issues.

LEADERSHIP BY EXAMPLE

Despite failures like GEN (Ret) Petraeus and others who fall prey to the temptations of the world, self-satisfaction, egotism, narcissism, and greed, there is hope. The world is filled with amazing leaders who embrace ethical behavior, and who struggle with dilemmas while sticking to their own code. Among the solutions is giving people role models who inspire. Talking about the moral dilemmas they faced—the processes by which they chose to make those hard decisions—is an excellent way both to have the conversation and to start conversations on ethics and morality. Equally important is recognition of being human and the flaws we all have. Just because a person has noted flaws does not mean he/she cannot make a good decision. In addition, we all make mistakes, and when lucky we grow from them. Keeping this balance in the conversations is critical.

The treatment of leadership studies typically focuses on unique events. Leadership classes in the military and commercial arenas are packed with management and

leadership tools and behaviors. Adding ethical and moral components to these studies is not easy, yet it is not as hard as it may seem on the surface. As a scholar of leadership, and an aspiring strategic leader, I personally place ethics and morals at the center of my own strategic leadership model. It is the foundation for all decisions I make, from when and how to spend money to how best to promote, reward, and discipline people. I do not always get it right, but I keep trying.

TOOLS, TRAINING, AND CASE STUDIES

Ethics and morality begin in childhood and carry us to the end of our lives—even sometimes how we or society view the ending of those lives. Videos and training modules are easily acquired and can be provided through a host of other online training. This will surely be a lesser, yet meaningful, component of ethical and moral awareness. There are even a few ethics board games out there. In fact, one could even use some traditional board games to address ethical and moral implications of personal behavior and societal norms. More powerful are those workshops and classes where ethics and morality are unpacked for a full day or week as part of a larger program. Including classic case studies and moving toward workplace and professional challenges is a well-accepted approach to lend to this endeavor.

While the notion of after-action meetings and conferences is good, their executions often are poor. They do not have to be. Intentionally setting up questions during after-action collection and conferencing on the topic can help all involved understand different contextual points and nuances that existed during an event. Giving thought to them, making personal and organizational decisions thereafter, can improve the long-term impact of the decisions in the future. This helps us all drive toward ethical and moral improvement.

Organizational development of case studies pertinent to the work of the entity is essential. The authors may often find linkages to traditional case studies, though highlight their immense differences too. A customized case study approach is an effective way to unpack current events, and give them strategic context. This tailored approach to case study development could focus on a particular part of the USG or IC, or to a career field and profession. For example, I often used the torture case study above in the introduction to classes on Human Intelligence and Counterintelligence. It also allows organizations to address implied and related issues including history, critical thinking, problem solving, and more.

Another approach, but certainly not the only one, would include brownbag or coffee events where the discussion is led. These allow smaller groups of people to talk about issues more relevant to their own spheres of life and workplace. They could be grassroots efforts of junior employees, or driven by executive leaders. There is no right answer; the key is doing something. There is precious little attention given to the topic outside of the military.

AN ETHICS BOARD

Developing an entity within institutions and organizations to focus on ethical conduct of individuals is a good start. It must also include deliberate consideration of the behavior of the organization as a whole. These boards should have regular meetings and be supported entirely by senior leaders. Over time, ethics experts could be groomed as key consultants. Perhaps a portfolio for ethics could be created. Imagine a Deputy DNI or an Undersecretary of Defense for Ethics. A note of caution—ethical consultants who are not from the Chaplain Corps or the Judge Advocate General Corps are a growing trend. It is equally important they not become the "answer person." Leaders need these tools themselves, but having someone dedicated to the consideration of ethics and morals would enrich further their final decision.

Ethics boards must be empowered and regularly report their work too—essential to sustained success. Today's workforce demands more transparency, accountability, consistency, and predictability. While ethical and moral decisions are not consistent, the regular public reporting of their debates and recommendations must be. This reporting would not only be a medium for new historical data; it would serve as educational discussion material for use across the other suggested activities in this article.

MORAL COMPASS

For fun you can conduct an Internet search of "Moral Compass Tests." While these often lack a lot of depth, they can spark interest in individuals and provoke new conversations. Just like taking personality tests, it is more about the self-awareness and its effect on behavior that I urge. Slowly one will develop his/her own moral compass. Mandatory reading and book clubs could enhance this too.[15] There are myriad books which explicitly or implicitly deal with ethics and morality. These would all contribute to the development and evolution of our ethical and moral conduct. My own experience in having these decisions with trustees at the board table and the kitchen table has been profound, and remains a place I often go for advice.

CONCLUSION

Today, nearly ten years after I intentionally began including classes on the topics of ethics and morality, many of my students still contact me and we discuss the issues they face. Many are in senior leadership positions, and ask for book recommendations, or provocative ways to initiate a discussion in small or large forums. We all consult the chaplains and lawyers, and we are proud to share the reality that we do not parrot their recommendations. The dilemmas have not stopped coming—in fact, as we pay closer attention, we are cognizant of even more. As I mentioned in the opening, this gives me hope.

In no way am I accusing large swaths of humans in the USG or IC of being unethical or immoral. I believe, despite the absence of formal discussions, training, or concerted efforts, we make generally ethical and moral decisions. What I outline above is sufficient to start a movement of thinking, toward a new and improved set of behaviors. It will not be easy, and we know the best things never are. What makes the United States a great country, and our citizens amazing people, are our shared guiding principles found codified foremost in the U.S. Constitution.

Imagine how much better we can become if we make some of the minor changes I recommend above across the U.S. government and the Intelligence Community. It will not be, it cannot be, a cookie-cutter approach. There will be times we disagree. This is a sign the recommended actions are working. There really are not metrics, measures of effectiveness, or measures of success for endeavors like these. It does not diminish their importance. I look forward to doing this in small ways in my own spheres in the meantime. Join me!

NOTES

[1] Ethical [Def. mult]. (n.d.). *Merriam-Webster Online.* Retrieved May 19, 2019, from http://www.merriam-webster.com/dictionary/ethical.

[2] Moral [Def. mult]. (n.d.). *Merriam-Webster Online.* Retrieved May 19, 2019, from http://www.merriam-webster.com/dictionary/ethical.

[3] Bailey, C. (2013). Public attitudes toward government spending. *American Journal of Political Science, 38*(2), 336-361.

[4] Las [Def. mult]. *Merriam-Webster Online.* Retrieved July 22, 2019, from https://www.merriam-webster.com/dictionary/law.

[5] Allen, K. (2012). What Is an Ethical Dilemma? *The New Social Worker*, *Volume 19*(2).

[6] Heaven, D. (2017). The Ethics Issue. Should we Abandon Privacy Online? *New Scientist*, accessed at https://www.newscientist.com/article/mg23531330-900-the-ethics-issue-should-we-abandon-privacy-online/.

[7] Thomson, J.J. *Killing, Letting Die, and the Trolley Problem,* 59 The Monist 204-17 (1976).

[8] Salin, R. (producer), & Meyer, N. (director). (1982). "Star Trek II – The Wrath of Khan" – [motion picture]. USA: Paramount.

[9] Davis, A., Kolber, J., and Tenney, H. (writers), & Nigro, M. (director). (2015). Morality [television series episode]. Kovnat, M. (executive producer), "Brain Games." Washington, DC, National Geographic.

[10] UN General Assembly, *Universal Declaration of Human Rights*, December 10, 1948, 217 A (V), available at: https://www.refworld.org/docid/3ae6b3712c.html [accessed July 22, 2019].

[11] McCain, J. (December 9, 2014). McCain: "I know from personal experience" torture doesn't work. *The Hill*. Retrieved from https://thehill.com/blogs/floor-action/senate/226476-mccain-i-know-from-personal-experience-torture-doesnt-work.

[12] Goldman, A. (January 25, 2016). How David Petraeus avoided felony charges and possible prison time. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/how-david-petraeus-avoided-felony-charges-and-possible-prison-time/2016/01/25/d77628dc-bfab-11e5-83d4-42e3bceea902_story.html?noredirect=on.

[13] Huntington, S.P. (1985). *The Soldier and the State: The Theory and Practice of Civil-Military Relations* (Cambridge. MA: Belknap Press).

[14] Principles of Professional Ethics for the Intelligence Community. (2014). Retrieved from http://www.dni.gov/index.php/how-we-work/ethics.

[15] There is a growing body of philosophical and practical approaches to ethics and morality. The following offers a survey of the field: *A Treatise on Human Nature*, by David Hume; *A Short History of Ethics: A History of Moral Philosophy from the homeric Age to the Twentieth Century*, by Alasdair McIntyre; *The Republic*, by Plato; *Utilitarianism*, by John Stuart Mill; *Ethics of Care*, by Carol Gilligan; and *A Theory of Justice*, by John Rawls.

Dr. Gus A. Otto is the DIA Senior Representative to NORAD and NORTHCOM. He is a career, full-spectrum, CI/HUMINT officer with leadership experience from the tactical through strategic levels. His doctorate is in ethical and creative leadership with two additional certificates. He is a graduate of the National War College, and later was the first DIA Chair at the Industrial College of the Armed Forces (now the Eisenhower School) and the Inter-American Defense College, and taught several electives at the National War College. Later, he served as the Commandant's Distinguished Chair of Defense Intelligence at the U.S. Army Combined Arms Center, where he taught across a broad array of PME programs, including CGSC, SAMS (ASLDP and ASLSP), WHINSEC, and the Sergeants Major Academy, and as an adjunct professor at the University of Kansas. He has been an adjunct faculty member at National Intelligence University since 2011.

China's Punitive Playbook:
A Case Study on Post-THAAD Sanctions

by Caroline E. Chang

INTRODUCTION

After a series of missile tests by North Korea, the South Korean and United States government (USG) announced the deployment of the THAAD (Terminal High-Altitude Area Defense) system on January 2016. The THAAD is an anti-ballistic missile system designed to intercept short- and medium-range missiles. Following the announcement, the Chinese government launched a series of unofficial sanctions to punish and deter the South Korean government from accepting additional THAAD batteries and components. Unlike previous Chinese sanctions that are normally targeted, the unofficial THAAD sanctions were sweeping, diversified, and comprehensive.

This research utilizes the THAAD sanctions as a case study to analyze the trends in Chinese sanction behavior and understand the evolution of its retaliatory playbook.

This research utilizes the THAAD sanctions as a case study to analyze the trends in Chinese sanction behavior and understand the evolution of its retaliatory playbook. For this study, I reviewed secondary literature on China's use of power; analyzed official U.S., Chinese, and Korean government policy white papers and strategy documents; and interviewed experts and policymakers in the U.S., including a National Security Council (NSC) Director in the Obama administration and a senior national security official from the Trump administration. I have anonymized the name of the subject who is currently serving in the administration and will refer to that individual as a "senior official in the Trump administration."

An analysis of recent Chinese sanction behavior demonstrates a strong correlation between Chinese economic capacity and assertiveness towards its neighbors. Through a thorough study of the THAAD sanctions and their implications on broader strategic balance, I argue that China's increasing desire for power projection, coupled with other economic expansion programs, all contribute to its grand strategy to become the regional hegemon in the Indo-Pacific.

POST-THAAD UNOFFICIAL SANCTIONS

When President Xi Jinping entered office, he made a concerted effort to prioritize Sino-Republic of Korea (ROK) relations over Sino-Democratic People's Republic of Korea (DPRK) relations. He had met with President Park Geun-hye frequently and, until the end of this case analysis, December 2017, he had never met with Kim Jong-un. To President Xi, serving as a lifeline for North Korea was a necessary evil. In recent years, as China looks increasingly outward, its interests appear to have grown increasingly incompatible with those of North Korea. Although the volatile Kim regime and its nuclear program has caused much trouble for Beijing, China has always supported the state that shares its socialist ideologies and, more importantly, serves as a buffer between China and South Korea, a strategic U.S. ally. Stability and preservation of the status quo on the Korean Peninsula remains a key priority for China.

As economic allies, both South Korea and China mutually committed to strengthening relations, but years of diplomatic gains were dismantled by a single hardline issue. After North Korea's fourth nuclear test in January 2016, the South Korean and U.S. governments announced negotiations for the THAAD deployment.[1] Following the announcement, South Koreans were divided on the matter. Conservatives supported the THAAD while liberals objected to it, seeking diplomatic policies instead. Under the conservative Park administration, the ROK Ministry of National Defense released a cartoon on its official website, "The Truth about THAAD," to pacify domestic disagreements surrounding the system.[2] After President Park was impeached, then liberal Presidential candidate Moon Jae-in campaigned on an anti-THAAD premise that South Korea would not become a pawn of the United States and that South Korea should be able to "say no to America."[3]

In July 2017, after two North Korean intercontinental ballistic missile tests, President Moon reversed his policy and reluctantly inherited plans for THAAD deployment from the Park administration. In response to the policy reversal, a South Korean official referenced the urgent necessity for the system that the administration was "trying to seek procedural legitimacy...yet feel the need to act fast on the situation that's unfolding."[4] While the U.S. and China may view the system as a grander symbol of strategic balance, when analyzing the events leading up to President Moon's acceptance of additional THAAD batteries it is apparent that the Moon administration viewed this purely as a necessity.

China takes issue with the invasiveness of the radar, specifically the radius, because it encroaches into mainland China's eastern region. China's missiles are clustered along the southeast coast and the radar would be able to detect China's missile activities.

The Chinese government's main grievance toward the system is the X-Band radar, which is a component of the THAAD that can monitor missile activities. If North Korea were to launch a missile, the radar would detect this activity and a launcher would then fire an interceptor and use the kinetic energy to destroy the missile.[5] China takes issue with the invasiveness of the radar, specifically the radius, because it encroaches into mainland China's eastern region. China's missiles are clustered along the southeast coast and the radar would be able to detect China's missile activities. My interview with a technical expert and fellow of the Nuclear Policy Program at the Carnegie-Tsinghua Center for Global Policy, Tong Zhao, revealed that specialists at the People's Liberation Army (PLA) also believed that the radar is capable of distinguishing real warheads from decoys on Chinese intercontinental ballistic missiles (ICBMs) and submarine-launched ballistic missiles (SLBMs).[6] In my conversation with Yun Sun, Senior Fellow at the Stimson Center, she describes the sentiments of the Chinese government:

> The short range covers 500 km and the long range covers 2500 km. If you really just want to monitor North Korean missile activities, why do you need the long range – who are you trying to monitor? The North Korean missile doesn't go beyond the 500km range. So that is one of the hypocrisies or loopholes in their argument that this is completely targeting North Korea. Because you don't need the long range to cover North Korea.[7]

Yun Sun had also spoken to PLA specialists and believes that they have every reason to be suspicious of the THAAD. Tong Zhao believes the claims of the PLA inspectors are inherently biased and wrote an extensive paper refuting the PLA technical assessment that the radar is as invasive as it claims.[8] From the various interview I conducted with Chinese and American experts and legislators, there were certainly varying opinions on the THAAD, the Chinese reactions, and subsequent sanctions. However, there was one consensus that everyone noted: initial bias may have led the Chinese government to overreact.

Chinese Overreaction

Previous Chinese sanctions were often vague threats, setting up an informal system that gives the government more flexibility without "losing face" from policy reversals.[9] The PLA was already biased toward a system based on widely held suspicions that the U.S. intends on obstructing China's rise. The Chinese interpreted the deployment as part of a concerted effort to bolster the U.S.'s strategic position in Northeast Asia at the cost of, or disadvantage to, the Chinese strategic position. From the Chinese perspective, the THAAD was not about North Korea at all; it was deployed to check China's rise. As soon as the Park and Obama administrations explored the idea of the THAAD, China condemned the move. There was no consideration for the fact that Kim Jong-un had tested an average of one missile per week following President Moon's election or that President Moon originally campaigned against the THAAD. An invasive system so close to Chinese borders prompted an immediate alarmist response toward the apparatus. Technical expert Tong Zhao remarks:

> The majority of Chinese experts and PLA officers genuinely believe the system poses a real threat to China's core security interests. And they also believe it's probable that the U.S. deliberately deployed the THAAD systems in South Korea for that purpose. For the purpose of neutralizing Chinese nuclear deterrence.[10]

The Park, Moon, and Obama administrations were steadfast in their positions about managing threats from North Korea. The ROK Ambassador to the United Nations stated at a UN session, "The THAAD...and the legitimate annual U.S.-ROK military exercise is a transparent and defensive exercise which cannot be put on par with North Korea's breach of obligations under Security Council Resolutions."[11] The U.S. government (USG) initially offered technical briefings, expert team visits, and strategic dialogues to the Xi administration. In addition, the USG also laid possible plans for when the THAAD would no longer be needed. However, according to Yun Sun, because the Xi administration personally identified

with South Korea and President Park as areas where China could push back on U.S. encroachment in the Chinese periphery, President Xi felt that his personal credibility was tarnished.

From the Chinese side, the damage was not only material, but also on the leadership level. Ryan Hass, then NSC Director for China Policy under President Obama, relayed the sentiments at the White House after the backlash from the Chinese government:

> I don't think that there was surprise as much as frustration on our part that the Chinese were unwilling or unable to hear what we were saying. It felt as if the PLA had gotten to President Xi and colored his interpretation of what the THAAD was.[12]

China launched its first wave of unofficial sanctions in August 2016, a month after the deployment announcement.

Effects of Post-THAAD Sanctions

Doghouse diplomacy, a phrase originally coined by *The Economist*, posits that "if China does not like what you are doing, it bullies you until you change; if you don't, it punishes you by putting you in the doghouse."[13] Unofficial THAAD sanctions display a unique case of China mobilizing a full spectrum of retaliation in hopes of influencing or stopping the South Korean deployment process. The Chinese government felt that there was still political space for the South Korean government to retreat from that decision. As opposed to sanctions in the past that were reactive and primarily intended to signal China's dissatisfaction, the THAAD sanctions were proactive and aimed at influencing the South Korean government's attitude.

One of the first industries that saw immediate externalities was the film and entertainment sector. The Korean pop industry combines elements from television shows, advertisements, music, and lifestyle; it has grown to become one of South Korea's greatest assets in garnering soft power and economic growth. When South Korea and the USG made the joint deployment announcement, stocks of Korean entertainment firms such as SM Entertainment, YG Entertainment, and CJ E&M fell in anticipation of Chinese backlash and content censorship. Chinese Hunan Television ordered all scenes with South Korean actors to be edited out, municipalities cancelled concerts and fan meetings, and private companies replaced Korean celebrities in advertisement campaigns.[14]

In addition to the cancellations, the Chinese government worked in tandem with television networks to promote anti-Korean propaganda messages and launched domestic media campaigns to criticize South Korea.[15] In January 2017, Chinese Foreign Minister Wang Yi responded to South Korea's request to lift the ban on "K-pop" stating, "The Chinese government will make efforts to resolve this conflict if the deployment is put on hold."[16]

On March 2, 2017, the Chinese National Tourism Administration announced a ban on Chinese tour groups traveling to South Korea. Approximately seven million tourists visit South Korea annually.[17] Local travel agency owner Jeon Gun Myung said, "The situation is really bad. We rely on Chinese tourists but now have to strategize towards the Southeast Asian and Japanese market."[18] The South Korean Ministry of Culture, Sports, and Tourism (MCST) held an emergency meeting to assess the Chinese market, strategize contingency plans toward the Middle East and Southeast Asia, and discuss industry damage.[19] The tourist ban particularly damaged the hospitality industry, but also significantly distressed the consumer companies that promote the K-pop lifestyle.

The prevalence of Korean conglomerate structure makes it easier for sanctions toward a particular industry felt by another under the same parent company. For instance, the South Korean conglomerate Lotte Group suffered the harshest retaliation because it supplied the golf course where the THAAD was deployed. Lotte Group has over 90 business units under the parent company including hotels, banking, food products, apartment complexes, petrochemical, and hospitality.[20] After the deployment announcement, China forced Lotte to shut down 87 of the 99 Lotte Marts, Lotte's superstores, under various pretexts such as violation of fire safety rules or air quality control. Lotte's supermarket sales in China fell 95 percent in 2017.[21] The Chinese government suspended the construction of Lotte and Hershey's joint chocolate factory and, that same month, Chinese hackers launched a cyberattack on Lotte's Chinese websites. Lotte's 2017 third quarter results explicitly state that sales in domestic stores have dropped due to the decline of inbound Chinese tourists and reported a significant operating loss of 43.1 percent in overseas stores from the THAAD impact.[22] In March 2019, Lotte ultimately announced that it was divesting in China; this included closing remaining Lotte Marts, department stores, and six confectionery and beverage factories. The company cited consumer boycotts from the THAAD fallout as the main reason for revenue losses.[23]

Since the deployment announcement, Chinese government-controlled media have urged citizens to boycott South Korean products.[24] The anti-THAAD and anti-Korean sentiments gained momentum among the citizenry. For instance, the Chinese rap group known as CD REV produced an anti-THAAD rap video. The rap includes language such as, "How many times do I ought to warn you, my lovely little

neighbor boy?" and "What's THAAD – terminal what? It ain't gonna terminate violence."[25] CD Rev has traditionally produced music videos that denounce foreign media coverage of China or blind worship of everything foreign. According to Rao Jin, a technology entrepreneur who runs a nationalistic website and media company, CD REV often fills a void where traditional state propaganda falls short. The intersection of government-led propaganda campaigns and popular nationalism contributed to widespread anti-THAAD and anti-Korean sentiments.

Analysis of Post-THAAD Sanctions

Tong Zhao's literature on sanctions classifies Chinese sanctions into two different groups: targeted and strategic. Targeted sanctions are usually punitive and reactive, directed at specific companies and industries, while strategic sanctions are comprehensive and intended to change the political system or ruling government. China's sole strategic sanction program was targeted at Vietnam between 1978 and 1988 against its military operation in present-day Cambodia. China reduced and subsequently terminated economic and military aid to Vietnam.[26] The remainder of Chinese official and unofficial sanctions have been targeted, specifically punishing an industry or company.

Until recently, Chinese sanctions were categorized into these two buckets; however, I believe the THAAD sanctions represent a combination of both. While one set of sanctions most affected the company Lotte Group for providing the land for the THAAD, the supplementary unofficial sanctions on other Korean multinational companies, the travel ban, and anti-Korean propaganda campaigns were indiscriminate, affecting every industry and citizen in South Korea. I found that the THAAD sanctions did not fit neatly into either category. Consequently, when I spoke with Tong Zhao, the author of Chinese sanctions literature and a technical expert on defense systems, I raised my concerns regarding his theory and categorization. He also agreed and stated, "I'm not sure I look at things through that particular lens anymore," iterating there was no longer a clear line to categorize these sanctions. However, he believes that THAAD sanctions represent much more than just punishing South Korea by describing the strategic implications: "The mainstream Chinese perception about the system is that it's very capable of undermining Chinese key security interests. The radar is so powerful that it can greatly undermine and neutralize Chinese nuclear deterrence."[27] Zhao confirmed that the Chinese sanction behavior has changed where his model of sanction categorization may not apply.

Gary Hufbauer relays the three motivations for sanctions: to punish, deter, and rehabilitate. China's motivation in its unofficial sanctions against South Korea was two-pronged: punitive and strategic.[28] The punitive approach is in retaliation for the deployment and the strategic approach is a deterrent intended to prevent South Korea from joining a U.S.-led missile defense network, a move that would increase U.S. visibility in the region. The punitive program is a continuation of China's past sanction behavior while the strategic element introduces China's will and commitment to its quest for regional primacy.

Sanction Outcomes

The two nations' diplomatic row came to a halt when both nations decided to normalize relations in November 2017. South Korea kept the THAAD, but the Moon administration made the following concessions called the "Three No's": South Korea will not accept additional THAAD batteries, will not join a U.S.-led regional missile defense network, and would not seek U.S.-Korean-Japanese defense cooperation as a military alliance. A THAAD battery is a set composed of a launcher, interceptor, radar, and fire control unit.[29] South Korea already possesses a full set of six batteries; not accepting additional THAAD batteries will not limit the functionality of the system already in place.

When assessing the post-sanction THAAD agreement, an analysis of the concessions begs the question: Which country made comparative gains in the process? Some scholars and legislators believe that South Korea was ultimately triumphant in the face of sanctions because the THAAD is still in position and its functionalities are all intact. During my conversation with a senior official in the Trump administration, he/she indicated the belief that China was not successful in the diplomatic row because South Korea still has a self-defense weapon on its territory, a strong symbol of U.S. presence in the Indo-Pacific.

Through the sanctions, South Korean perception of China completely changed into seemingly coercive, bullying, and excessive. In my interview with Michael Swaine, Senior Fellow at the Carnegie Endowment for International Peace, he stated the Chinese "have been very deliberate and assiduous about cultivating a good image in South Korea," and the course of action counters the continued promotion of the *peaceful rise* narrative.[30] During my conversation with local travel agency owner Jeon Gun-Myung, he expressed resentment toward China for disrupting the Korean tourism industry.[31] This demonstrates how the THAAD sanctions were counterproductive to Chinese efforts to revamp their image and soft power programs in South Korea at a grassroots level.

While Chinese foreign direct investment (FDI) into China surged 240 percent in 2018, South Korean companies began to diversify their investments and operations in the years following the diplomatic row.[32] SK Group, whose business was severely impacted when the Chinese government suspended operations of SK Innovation's battery production plant in China, began to invest in Southeast Asia at an unprecedented speed. In November 2018, SK's Chairman, Chey Taewon, went on an investment spree where he penned joint venture agreements in Malaysia, Singapore, and Vietnam. Chairman Chey announced that he hopes to invest $17 billion in the coming years in SK's ASEAN regional base, Malaysia.

In October 2019, Samsung announced that it would be halting all mobile phone production in China, partially due to the sanctions blowback and intensifying competition from domestic rivals. Samsung will be manufacturing its mobile phones in India and Vietnam. South Korean conglomerates such as Hyundai, Lotte, Samsung, LG, and SK have all begun to diversify their strategic plans and are diverting many of the assets previously allocated for China into Southeast Asia. According to the 2019 United Nations Investment Report, FDI flows into Southeast Asia rose by 3 percent to an all-time high of $149 billion in 2018.[33]

Throughout history, states with economic leverage have used or threatened to use sanctions against a particular industry, company, or nation to protect their national interests or condemn the violation of international norms.

From the Chinese perspective, the headline of a Hong Kong newspaper, *South China Morning Post*, reads "China Wins Its War Against South Korea's THAAD Missile Shield – Without Firing a Shot."[34] Internally, China promoted itself as a clear winner because it believed the "Three No's" are enormous concessions. From the ROK perspective, the "Three No's" are not concessions but rather a continuation of positions already in place. It is rather a face-saving agreement for China, a display of South Korea's commitment to diplomacy, and a return to the status quo.

In China's calculation of achieving its strategic objective, the use of unofficial sanctions was successful. It utilized its economic leverage to ensure South Korea was not falling completely into the United States' sphere of influence. It also signaled to South Korea the extent of economic and diplomatic damage China is willing to cause if a nation threatens its interests.

CHINA'S PREVIOUS SANCTIONS BEHAVIOR

Throughout history, states with economic leverage have used or threatened to use sanctions against a particular industry, company, or nation to protect their national interests or condemn the violation of international norms. Daniel Drezner defines economic coercion as "the threat or act by a sender government to disrupt economic exchange with the target state, unless the target acquiesces to an articulated demand."[35] Sanction theory and its effectiveness is often understood in terms of the existing relationship between the sending and targeted nations. Sanctions against countries with economic ties are more likely to succeed because they disrupt the status quo, where both sender and target nations must bear the losses.[36] Since the formal establishment of diplomatic relations in 1992, South Korea and China have enjoyed a strong bilateral relationship. China is South Korea's biggest trading partner and is the top recipient of Korea's outflow of investment.

The U.S. typically enacted comprehensive sanction programs on countries that violate international norms of behavior. Nations are usually cognizant of the limitations of sanctions programs because they have previously been inadequate or ineffective in evoking desired outcomes. Major powers understand that, sometimes, the most they could do is signal their dissatisfaction through sanctions.[37]

China has been the recipient of economic sanctions from the U.S. and other states, and this has certainly affected its attitude toward its role as a sanction-sending nation.[38] China had previously been sanctioned by the U.S. and the European Union for its response to the Tiananmen protests in 1989; its missile and nuclear equipment trade to countries like Iran, Pakistan, and Algeria; and intellectual property rights violations.[39] As a sanction recipient, China is very well aware of the ramifications of economic sanctions, as it previously viewed comprehensive sanctions as contributors to humanitarian disasters. If China had to impose or threaten to impose sanctions, it preferred a targeted and punitive approach, narrowing in on a specific industry or company.[40]

In our conversation, Tong Zhao mentioned that the Chinese sanction behavior is ironic because China has a long history of being invaded and humiliated by foreign powers. Early on, the Chinese leaders pledged that, when China becomes powerful, it would never try to bully other countries. He noted that even if present-day Chinese behavior contradicts this, the nation has long convinced itself of the peace-loving country narrative; this extends to the way Beijing always portrays itself as the victim. Currently as an emerging power, the Chinese government is similarly threatening to enact, or enacting, sanctions against countries that jeopardize its national interests. In recent years, the scope of its national

Table

Year	Targeted Country	China's Grievance	Proposed Sanction	Result
2007	United Kingdom	British Petroleum's joint ventures with Vietnam that took place in disputed territory in South China Sea.	Loss of business opportunities	Not executed
2008	United States	Exxon Mobil Joint ventures with Vietnam that took place in disputed territory in South China Sea.	Loss of business opportunities	Not executed
2009	France	President Sarkozy meeting Dalai Lama.	Cancellation of delegations and summits Froze an order for 150 planes from Airbus	Debated – Although China pulled out of the summits, there is debate whether the Airbus freeze was punitive or simply due to lower market demand.
2010	United States	Against U.S. arms sales to Taiwan.	Sanctions against companies that engage in arms deliveries to Taiwan (Boeing)	Not executed
2010	Norway	Nobel Peace Prize incident of Liu Xiaobo.	Cancellation of ministerial trade delegation Fall of salmon sales by half over eight months	Executed
2010	Japan	Arrest of Chinese fisherman in Diaoyu Islands.	Blocked shipment of rare earth elements	Executed
2012	Philippines	Dispute about Chinese fishermen operating in Scarborough Shoal.	Tighter measure on banana imports to China	Executed
2017	South Korea	THAAD deployment.	Lotte, Korean multinational corporations, K-Pop, travel-ban, high-level dialogues, etc.	Executed

interests have expanded to cover not only sovereignty and territorial disputes, but also China's role in the strategic balance.

The Table represents the unilateral official and unofficial sanctions launched by China from 2007 to 2019. I have deliberately excluded United Nations Security Council sanctions against Iran (2003-2015), North Korea (2006-2017), and others because they are affirmed by a multilateral organ at the United Nations (United Nations, 2003-2017).

The Table illustrates that, over time, Chinese sanctions evolved to become more robust and aggressive. The Chinese fight against Western sanctions after Tiananmen, entry into the World Trade Organization, stopping Taiwanese independence, and the successful hosting of the Olympics heightened nationalism after 2008.[41] The evolution of sanction behavior also demonstrates increased cognizance by the Chinese Communist Party (CCP) of its international influential power.

James Reilly conducted extensive research on recent Chinese sanction behavior in which he cites approximately five notable instances in which China executed punitive sanctions. Reilly cites the sanctions on Boeing following the U.S.'s arms sales to Taiwan in 2010, the freezing of Airbus orders following the Dalai Lama's visit to France, and sanctions against Chinese adversaries in the South and East China Seas to state that, in the past, China used foreign policy to advance economic policies but now uses its economic capacity to influence foreign policy.[42]

I agree with Reilly's argument that Chinese motivations and methods of sanction execution are changing. However, he also makes the claim that "China's capacity to use economic pressure should not be overestimated." This declaration, coupled with his characterization of Chinese sanctions as limited and incomprehensive, underestimates China's ability and will to utilize its economic prowess to achieve comparative gains in strategic balance. This underestimation may have been relevant during Reilly's research period but,

by 2012, China had significant state capacity and influential power on the global stage. China was already established as a global power with vast economic capacity to exercise its political will abroad. The shift in Chinese foreign policy behavior began around 2009-2010, after the 2008 Olympics, but has increased in intensity since then.

Evidence of Chinese Assertiveness

China cemented its status on the global stage in 2008. In the following years, the growth of its military power and heightened nationalism further contributed to the government's muscular foreign policy. The way that Chinese leaders viewed themselves in the world after resisting the global financial crisis is portrayed through increased demonstration of their willingness to use force.

Chinese maritime claims in the South China Sea can be traced back to 1947 under the Kuomintang Party. However, in recent years, tensions have escalated due to China's increasingly aggressive behavior in the disputed territory. Chinese construction of military bases in the Paracel and Spratly Archipelagos has been particularly alarming. Satellite images have shown Chinese infrastructure such as runways, helipads, radars, and surveillance structures.[43] China regularly conducts naval exercises in the disputed territories to display its new technologies in submarines, destroyers, and aircraft. Alastair Iain Johnston points to the longstanding claims in the South China Sea to argue that scholars' focus on China's new assertiveness underestimates continuity and Chinese assertiveness in the past.[44] However, I argue that the most important element in the evolution of China's behavior is *capacity*. China now has unprecedented economic capacity to be assertive and coerce countries with smaller economies.

China also demonstrated force in the East China Sea in 2010. When a Chinese fisherman was arrested in the disputed Diaoyu/Senkaku islands, China called off scheduled bilateral talks, arrested four Japanese nationals for illegally entering a defense zone, sent two marine surveillance ships to "assert the country's sovereignty," and blocked shipments of rare earth materials to Japan, a key component for electronic, hybrid car, and turbine manufacturing.[45] Through the retaliation, we begin to see glimpses of Chinese capacity and its will to make its grievances heard.

Deng Xiaoping's Dictum and Shift in Sanctions Behavior

Tao Guang Yang Hui(韬光养晦)is Deng Xiaoping's dictum of keeping a low profile that drove Chinese foreign policy in the 1990s and 2000s. Deng had two motivations to adopt this strategy: Western sanctions against China and the collapse of the Soviet Union. In the face of radical changes in Eastern Europe and the collapse of the Soviet Union, China had no desire to evoke an existential crisis or to challenge the lone superpower. It was primarily concerned with regime preservation and domestic stability. China also faced immense pressures from the West including suspended high-level diplomatic interactions and economic and political sanctions following the Tiananmen Massacre incident of 1989. [46]All things considered, it was in China's best interest to keep a low profile in the international sphere and strengthen its domestic policies.

In contrast to most of the Hu Jintao administration, the Xi Jinping administration has shown a clear abandonment of Tao Guang Yang Hui. Hu Jintao was often labeled as a "legislator of inaction" (无为 wuwei).[47] However, Table 1 illustrates that in 2010, during the second half of Hu's administration, there was a series of executed sanctions against Japan, Norway, and the Philippines, mostly as responses to calls for more decisive foreign policies. By the end of President Hu's tenure, we begin to see a clear shift in power execution.

Xi's ascent to power displays a clear abandonment of Deng's dictum and signals a critical juncture in Chinese foreign policy. President Xi addressed long-held nationalist beliefs that a rising China must have equally muscular foreign policies. He entered office as the head of government, party, and the military, a move that his predecessors avoided to level out balance of power. His attitude toward power consolidation in the domestic arena translated to the foreign policy stage. At the 19th National Party Congress in October 2017, he opened the Congress by stating, "It will be an era that sees China moving closer to center stage."[48] He also used the platform to solidify his grip on power by promoting a sizable number of allies to senior leadership positions. Xi's rhetoric at the 19th Party Congress, coupled with the constitutional amendment that removes presidential term limits, further consolidated his authority unlike that of any other former president. Under President Xi, Chinese behavior abroad has been the most decisive and forceful.

Opponents of Deng Xiaoping's dictum believe that the U.S. is trying to contain China's rise and that the policy is incompatible with China's expanding national interests. President Xi's Vice Ministry of Foreign Affairs, Wu Daiwei, also states, "As a matter of fact, Deng's low profile policy never simply meant a passive posture. It was a dynamic process to hide China's ambition and to bide its time."[49] President Xi's interpretation of China's potential and ambition has been evident through his increasingly outward and expansive policies. As China has gained more economic capacity, not only has the scope of its national interests expanded but also its political will to impose more robust and comprehensive economic retaliations.

Dr. Swaine's discourse analysis on China's use of the phrase "Core Interest" iterates that its increased use in official statements illustrates China's attempt to evoke greater respect from other nations. He also states that a stronger China might expand the scope of the interests, which will eventually pose a challenge to U.S. efforts to maintain a stable relationship.[50] Table 1 further illustrates that, when analyzing the evolution of sanctions behavior through Deng's approach, it is apparent that China has abandoned this position and will use economic coercion to accommodate its expanded interests. Further, China's interests now extend far beyond the traditional coverage of sovereignty to include its quest to reaffirm its sphere of influence.

During my conversations with a U.S.-China security expert, Dr. Michael Swaine, and President Obama's NSC Director for China, Taiwan, and Mongolia, Ryan Hass, both stated that this sanctions discourse about an emerging power is natural:

> The fact that the Chinese use their economic leverage to extract diplomatic and political advantages on its face should not be either surprising or necessarily threatening—from a global order perspective. Because other states do this all the time and big powers do it a lot.[51]

Would the Chinese like to create finalization of Asia where all the countries along the periphery are preferential to the Chinese and their strategic interests? Of course, they would. That's not atypical of the behavior of a rising power. That's typically what a rising power would try to do.[52]

I agree with Swaine's and Hass' claims that this behavior is unsurprising because states are rational actors and rising powers have very specific ideas about becoming a great power that exist in relation to their capabilities.[53] However, I disagree with Dr. Swaine's assessment that this behavior is not threatening. The next section outlines the intensity and speed of China's rise and how its economic programs pose as unambiguous threats to replace the U.S. as a regional hegemon.

IMPLICATIONS OF STRATEGIC BALANCE

Although China's strategic objective is not iterated explicitly, its behavior suggests that it has every intention of bringing more countries in the Indo-Pacific into its orbit and subsequently establishing itself as a regional hegemon. In addition to increased execution of sanctions, the Chinese government also introduced expansive economic programs to exercise its power on the global stage. Realist theory is often used to understand the power dynamics between a rising China and the incumbent hegemon, the United States. According to John Mearsheimer's offensive realist theory, states concerned with security must compete with each other for power. Under this model, China and U.S. will seize every opportunity to maximize their share of world power.

Sino-U.S. Competition

Professor Graham Allison of Harvard University analyzes U.S.-China dynamics as emerging and incumbent powers through the so-called "Thucydides Trap." The Thucydides Trap was initially drawn from the conflicts between Sparta and Athens during the Peloponnesian War and refers to the theory that threat perceptions between a rising power and an established power will inevitably lead the two into war. His study encompasses power transitions from both global and regional hegemonic perspectives. Allison conducted a historical examination of power transition in the last 500 years and found that, in the 16 case studies of ruling and rising power tensions, 12 engaged in war. When this global study is applied to the U.S.'s and China's status as the incumbent hegemon and the emerging power, respectively, Allison begs the question: "Can China and the U.S. avoid the Thucydides Trap?'" China is the sole nation capable of challenging U.S. hegemony in the Indo-Pacific. Allison's findings relay that, although war with China is more likely than not, there are ways to avoid the trap. Allison asserts that through radical changes in the attitudes of both countries' leaders and more frequent presidential summits and departmental working groups, China and the U.S. are able to avoid the trap.[54]

While I agree with Allison's assessment that there is room for cooperation, I argue that China's ultimate strategic objective to become the primal power in the Indo-Pacific will continue to clash with the U.S. interest to protect its hegemonic status in the region. Economic evidence beyond sanctions proves China's increasing threats to displace the U.S. in the region. I believe that fundamental differences in the Chinese and American governing systems make the clash more probable. I posit that the clash will likely take the form of a cold war, involving non-traditional warfare such as trade, space, and cyber war rather than conventional warfare involving direct military confrontations. The following section analyzes the evidence in China's quest for regional hegemony and the threats posed to U.S. primacy in the Indo-Pacific.

Evidence in Economic Policies

Based on gross domestic product figures and purchase parity terms, the Chinese economy is projected to surpass the U.S. economy, especially if the government continues to promote indigenous innovation and expand the domestic consumption market.[55] As demonstrated in previous chapters, China is no longer hesitant to impose sanctions on

countries that threaten its expanded interests. In addition to increasingly assertive sanctions behavior, China utilizes forced technology transfers, hackings, and the Belt and Road Initiative to gain a competitive edge in facing the U.S. on the global stage.

A visible tension in the bilateral relationship is the U.S. allegation that the Chinese government and companies steal U.S. intellectual property (IP) valued at billions of dollars in revenue.

The greatest difference between the U.S. and Chinese economies is the socialist element in China. Although China has abandoned Stalinist socialism of pursuing egalitarianism, it still retains the Leninist socialism of one-party rule. The Chinese Communist Party (CCP) understands that regime security and legitimization largely depend on economic growth and will impose frequent economic interventions and discriminatory policies to favor Chinese businesses. Many foreign manufacturers cannot gain access to the Chinese market without forming a joint venture partnership. Mandating foreign companies to operate as a joint venture for market access is one of China's most aggressive forms of forced technology transfer. Under joint venture regulations, foreign firms are forced to transfer critical know-how. Automotive companies with advanced technologies have been reluctant to bring their manufacturing to China, a move that would risk their intellectual property. Without joint ventures, Chinese consumers must seek the international market to import their foreign cars. Alternatively, if consumers want to import an American vehicle, the tariff is 25 percent of the wholesale value. A Jeep Wrangler in the U.S. costs $40,530 but could set back a Chinese buyer up to $71,000 because of taxes. This tactic has helped localize and boost the domestic automotive industry because fewer than five percent of cars in the country are imported.[56]

A visible tension in the bilateral relationship is the U.S. allegation that the Chinese government and companies steal U.S. intellectual property (IP) valued at billions of dollars in revenue. The allegations point toward forced technology transfers through joint ventures and illicit hacking as methods for IP theft. A *New York Times* investigation reveals that the Chinese hacking group "Comment Crew" has been extracting data from companies like Coca Cola and others involved in critical infrastructure such as electric power grid companies. Investigations reveal that "Comment Crew" is a group of contractors for the Chinese military. The cyber hacks have become so sophisticated and intense that they have potential to damage the bilateral relationship severely.[57]

The U.S. has broached this subject with its counterparts in Strategic & Economic Dialogues but, despite prolific evidence, the Chinese government continues to deny allegations. Both China's trade practices and intellectual property theft were key grievances that led President Donald Trump to impose tariffs and other trade barriers on China on May 29, 2018.[58] For the purpose of maintaining the scope of this research I do not analyze the U.S.-China trade war in terms of sanctions.

Evidence through Belt and Road Initiative

In 2013 President Xi outlined an infrastructure development plan tracing ancient Silk Road routes from China flowing westward toward Asia, the Middle East, Africa, and Europe. The plan called for the funding and coordination of major transportation and energy infrastructure projects across Eurasia. The Belt and Road Initiative (BRI) is not an innocuous development or aid plan but is rather a significant threat to the U.S. economy and the strategic balance. The current administration views this initiative as a way for China to focus its investments in the developing world and the Indo-Pacific region to "expand influence and gain competitive advantages against the U.S."[59] In a U.S. House Foreign Affairs Subcommittee hearing on "U.S. Economic Strategy Amid China's Belt and Road," Chairman Senator Ted Yoho stated that the U.S. needs more robust economic engagement in Asia because BRI "stands unchallenged as the region's premier economic engagement initiative" and will be utilized to "advance China's interests and influence sometimes at the expense of our own."[60]

As the initiative boosts China's political and economic influence in various regions, the U.S. believes it will simultaneously dilute American economic activity and power. The current administration fears that China will become the primary economic partner for many developing nations, giving China undue influence in these countries that can be used to advance Chinese interests at the expense of not only the U.S., but BRI participant countries themselves. Scholars and legislators also believe states are more likely to curry favor toward China on multilateral platforms. [61]

BRI can best be understood through a realist lens: Is this project making China more powerful? In official Chinese statements, Xi Jinping presents BRI as a plan to improve infrastructure, build linkages with border countries, narrow economic inequality between wealthy coastal and poor interior provinces, and boost international people-to-people and cultural exchanges. To some developing countries, World Bank loans for projects are beyond reach because they require countries to meet certain standards to receive the loans. World Bank loans are usually contingent upon the implementation of the Washington Consensus—contract

transparency and open bidding, project governance standards, anti-corruption measures, and environmental standards—while BRI loans and projects come with fewer strings attached.[62] Some countries are unable to meet the governance and transparency standards attached to World Bank loans, while others wish to pursue projects that the World Bank deems too risky.

Although China presents the BRI as a "win-win" form of cooperation, the infrastructure plans have created detrimental debt traps for some countries. In Montenegro's case, an 809 million euro BRI highway project has forced the government to raise taxes, partially freeze public sector wages, and end welfare benefits for mothers.[63] John Hurley's study for the Center for Global Development assesses debt risk associated with BRI projects and lists Montenegro as one of the most vulnerable countries to debt traps, along with Djibouti, the Maldives, Laos, Mongolia, Tajikistan, Kyrgyzstan, and Pakistan.[64]

BRI is not a completely zero-sum initiative, because it does fill a vast infrastructure need in developing countries, and inevitably many projects will be completed and improve the lives of people. BRI is not solely aimed at advancing Chinese interests at the cost of the U.S., since multiple U.S. companies such as General Electric, Honeywell, and Hewlett-Packard have been able to participate in BRI contracts.[65] However, U.S. firm participation is still low because companies often face an uneven playing field where Chinese firms have an edge through national subsidies and low estimated project costs. It is rather BRI's unspoken goals, and their potential boost to China's global standing, that are considered more threatening to the U.S. The tacit goal of utilizing BRI to orient trade toward China across Eurasia, presenting China as a source for large-scale projects, improving China's image on the global stage, and spreading Chinese soft power, altogether points toward China seeking to gain a strategic advantage over the U.S.

Xi Jinping's New Model of Big Power Relations

In a speech in Seattle in 2012, Xi Jingping stated that he does not believe the Thucydides Trap applies to U.S.-China relations.[66] Instead, he introduced a new model of big power relations that paves a way for both the United States and China to coexist as two superpowers. The U.S. has yet to recognize this model; however, President Xi and the Chinese media have been repeatedly using the framework since the 2014 Strategic and Economic Dialogue (S&ED). President Xi calls for (1) no conflict or confrontation, (2) mutual trust, and (3) win-win cooperation.[67] The rhetoric in the model places both China and the U.S. on equal footing.

A critical point of tension with Xi's model is the "mutual trust" clause. Lack of mutual trust automatically inhibits both nations from achieving the latter two clauses, "no conflict or confrontation" and "win-win cooperation." Although the model calls for a transition from a unipolar to a bipolar system, where both nations can cooperate on critical issues, I argue that fundamental differences in the Chinese and American governing systems and deep-seated mistrust will make this difficult. Lack of mutual trust causes even the most benign intentions to be perceived as equalizing or threatening.

Unfair trade practices, commercial espionage programs, THAAD sanctions, and the Belt and Road Initiative all contribute to erosion of American trust in the Chinese.

The evidence above illustrates tensions and pressure points in the U.S.-China economic relationship that pose as hindrances to the big power relations model. Unfair trade practices, commercial espionage programs, THAAD sanctions, and the Belt and Road Initiative all contribute to erosion of American trust in the Chinese. From the Chinese side, the perception of moves by the U.S. to check China's rise raises significant suspicion. While the two nations can agree to disagree in their beliefs, in the present anarchic international system one must remain as the dominant power. China is the sole nation capable of challenging U.S. hegemony, and its pursuit to increase its influence at the expense of the U.S.'s poses a direct threat to U.S. economic and military interests in the Asia-Pacific.

Global Order

From a strategic balance perspective, I researched whether the THAAD was a reflection of the U.S.-China rivalry rather than the South and North Korea conflicts. President Obama's NSC Director for China Policy, Ryan Hass, states his views on the conflict:

> That's certainly how [the Chinese] viewed it. It wasn't how we viewed it. We viewed THAAD as an instrument to address a very specific threat. We have 30,000 troops stationed in South Korea. South Korea is an ally. Seoul has a population of approximately 20 mil people. There's a very practical reason why we would want to create a multilayered missile defense system.[68]

The Trump administration's *National Security Strategy* describes China as a revisionist power that seeks to displace the U.S. in the Indo-Pacific, expand its state-driven economic

model, and reorder the region in its favor.[69] In my conversation with a senior Trump administration official, he/she confirmed the findings in the report and described the threats China poses to U.S. national interests. In addition, he/she stated, "The Chinese government uses the Thucydides trap to frighten our neighbors in the region. The more powerful China gets, the more willing it will be to inflict significant harm on democracies."[70]

While there is bipartisan understanding of the necessity of the THAAD by U.S. legislators, non-governmental scholars question the actual capabilities of the system.

Although the Trump administration inherited the THAAD program from the Obama administration, the two senior members of those administrations agreed on the necessity of a multilayered defense system in South Korea. In contrast to the NSC Directors, the scholars at the Stimson Center, a bipartisan organization specializing in nuclear and arms proliferation, condemned the system. During my interview with the Senior Fellow and Director of Stimson's Nuclear Safeguards Program, Cindy Vestergaard mentioned that the THAAD is simply an elaborate machine to create jobs and increase U.S. defense spending; Yun Sun, also at Stimson, believes that it is just a symbol of U.S. presence in South Korea. While there is bipartisan understanding of the necessity of the THAAD by U.S. legislators, non-governmental scholars question the actual capabilities of the system.

Although the two administrations agree on the THAAD, the differences are reflected in their approaches to a rising China. Both the interview with the senior Trump administration official and then-CIA Director Mike Pompeo's interview with *BBC News* confirm the Trump administration's clearly adversarial attitude toward China. Pompeo insists, "The Chinese are working diligently to put themselves in a position where they are a superpower," and points to China's state capacity to steal U.S. commercial information and infiltrate schools and hospitals.[71] The current administration views China as posing a very credible threat not only to American primacy in the region, but also to its economic, military, and political interests.[72]

In contrast to the Trump administration, the Obama administration viewed China's rise in a more constructivist context. According to the U.S. Department of Defense Report (2013), the Obama administration recognized China's rise and points of tension where it may clash with the U.S. but also acknowledges the areas where it can cooperate. The Obama administration's "Pivot to Asia" aptly portrays both the desire for cooperation to tackle the toughest global issues and the discrete responses to China's increasingly assertive behavior in the Indo-Pacific. The U.S. alone cannot combat world problems like climate change, nuclear proliferation, and terrorism. Without recognizing the common ground, this automatically degrades the relationship from cautious partners to complete adversaries.

From analyzing China's sanction behavior trends and utilizing the economic retaliation against South Korea as a case study, it is clear that China will be more forceful and assertive in addressing its interests and dissatisfaction in the future. Although the Chinese narrative regarding strategic balance promotes a multipolar world where both the United States and China can coexist as superpowers, the two countries' fundamental differences and heightened threat perceptions will inevitably lead toward a clash during China's quest for regional hegemony. As China narrows the economic gap with the U.S., both nations must cautiously find common ground for cooperation.

CONCLUSION

An analysis of Chinese sanction behavior in the past decade portray a strong correlation between Chinese economic capacity and forceful behavior towards its neighbors. China previously used sanctions, if executed at all, to threaten and condemn a particular industry or company. However, after 2010, Chinese sanctions have evolved to be comprehensive, containing both punitive and strategic motives. The change is likely due to China's growing economic capacity coupled with President Xi's attitude towards external power projection. Through the unofficial yet comprehensive THAAD sanctions, China demonstrated its capacity to express dissatisfaction and influence the strategic behavior of South Korea. This behavior, along with China's expansion of economic programs, all fit into China's grand strategy of displacing the United States in the Indo-Pacific to become the regional hegemon.

NOTES

[1] Ministry of Foreign Affairs of the Republic of Korea (2016), U.S. Assistant Secretary of State for East Asian and Pacific Affairs Russel Visits the ROK. [Online], 26 February.
[2] Ministry of National Defense of Republic of Korea (2016), The Truth about THAAD [Online], 2 September.
[3] Choe, S., and Motoko, R. (2017), South Korean Leader Boxed In as Trump Threatens North Korea [Online], *The New York Times*, 3 November.

[4] Reif, K. (2017), Moon Reverses THAAD Decision. [Online], *Arms Control Association*, September.
[5] Lockheed Martin (2018), THAAD Terminal High Altitude Area Defense [Online], Available from: https://www.lockheedmartin.com/en-us/products/thaad.html.
[6] Chang original interview: Zhao, Tong (2018), Nuclear Policy Program Fellow at Carnegie-Tsinghua Center for Global Policy, 23 April. Video communication.
[7] Chang original interview: Sun, Yun (2018), Co-Director of the East Asia Program and Director of the China Program at the Stimson Center, 1 May. In-person communication.
[8] Chang original interview: Zhao, Tong (2018), Nuclear Policy Program Fellow at Carnegie-Tsinghua Center for Global Policy, 23 April. Video communication.
[9] Reilly, J. (2012), China's Unilateral Sanctions, *The Washington Quarterly* 35(4), 121-133.
[10] Chang original interview: Zhao, Tong (2018), Nuclear Policy Program Fellow at Carnegie-Tsinghua Center for Global Policy, 23 April. Video communication.
[11] Ministry of Foreign Affairs of the Republic of Korea (2017), Security Council Thematic Meeting on Denuclearization of the DPRK [Online], 28 April. Available from: http://www.mofa.go.kr/www/brd/m_3874/view.do?seq=365841.
[12] Chang original interview: Hass, Ryan (2018), David M. Rubenstein Fellow at Brookings Institution and Former Director for China, Taiwan, and Mongolia at the National Security Council (NSC), 1 May. In-person communication.
[13] The Economist (2017), South Korea is making up with China, but a sour taste remains [Online], *The Economist*, 9 November.
[14] Jun, H. (2017) Hallyu at a Crossroads: The Clash of Korea's Soft Power Success and China's Hard Power Threat in Light of Terminal High Altitude Area Defense (THAAD) System Deployment, *Asian International Studies Review* 18(1), 153-169.
[15] Chang original interview: Swaine, Michael (2018), Senior Fellow at Carnegie Endowment for International Peace, 2 May. In-person communication; Chang original interview: Zhao, Tong (2018), Nuclear Policy Program Fellow at Carnegie-Tsinghua Center for Global Policy, 23 April. Video communication.
[16] Jun, J. (2017), China admits to retaliation against THAAD deployment [Online], *The Korea Times*, 5 January.
[17] Hancock, T. (2017), South Korean consumer groups bear brunt of China's THAAD ire [Online], *Financial Times*, 20 August.
[18] Chang original interview: Jeon, Kun-Myung (2018), Travel Agency Owner in South Korea, 3 May. Phone communication.
[19] Ministry of Culture, Sports, and Tourism of the Republic of Korea (2017), MCST, THAAD related Chinese Market Emergency Meeting. [Online], 3 March. Available from: http://www.mcst.go.kr/web/s_notice/press/pressView.jsp?pSeq=15934.
[20] Lotte Shopping Co., Ltd. (2017), 2017 Third Quarter Results.
[21] Hancock, T. (2017), South Korean consumer groups bear brunt of China's THAAD ire [Online], *Financial Times*, 20 August.
[22] Lotte Shopping Co., Ltd. (2017), 2017 Third Quarter Results.
[23] Singapore Times (2019), South Korea's Lotte seeks exit China after investing $9.6 billion, as THAAD fallout ensues, *Singapore Times*, 13 March.
[24] Meick, E., and Salidjanova, N. (2017), China's Response to U.S.-South Korean Missile Defense System Deployment and Its Implications, *U.S.-China Economic and Security Review Commission*, 26 July.
[25] Mullany, G. (2017), Chinese Rappers Take Aim at American Antimissile System in South Korea [Online], *The New York Times*, 12 May.
[26] Zhao, T. (2018), Sanction experience and sanction behavior: an analysis of Chinese perception and behavior on economic sanctions, *Contemporary Politics* 16(3), 263-278.
[27] Chang original interview: Zhao, Tong (2018), Nuclear Policy Program Fellow at Carnegie-Tsinghua Center for Global Policy, 23 April. Video communication.
[28] Hufbauer, G. (2009), *Economic Sanctions Reconsidered*, 3rd ed., Washington, DC: Peterson Institute for International Economics.
[29] Lockheed Martin (2018), THAAD Terminal High Altitude Area Defense [Online], available from: https://www.lockheedmartin.com/en-us/products/thaad.html.
[30] Chang original interview: Swaine, Michael (2018), Senior Fellow at Carnegie Endowment for International Peace, 2 May. In-person communication.
[31] Chang original interview: Jeon, Kun-Myung (2018), Travel Agency Owner in South Korea, 3 May. Phone communication.
[32] Jung, S.Y. (2019), China's FDI in South Korea Soars 240% in 2018 [Online], *Business Korea*, 4 January.
[33] (2019) World Investment Report 2019, United Nations [Online], available from: https://unctad.org/en/PublicationsLibrary/wir2019_en.pdf.
[34] Volodzko, D. (2017), China wins its war against South Korea's US THAAD missile shield – Without firing a shot [Online], *South China Morning Post*, 18 November.
[35] Drezner, D. (2003), The Hidden Hand of Economic Coercion, *International Organization* 57(3), 643-659.
[36] Drezner, D. (1999), *The Sanctions Paradox: Economic Statecraft and International Relations*, Cambridge, UK: Cambridge University Press.
[37] Drezner, D. (2003), The Hidden Hand of Economic Coercion, *International Organization* 57(3), 643-659.
[38] Reilly, J. (2012), China's Unilateral Sanctions, *The Washington Quarterly* 35(4), 121-133.
[39] Zhao, T. (2018) Sanction experience and sanction behavior: An analysis of Chinese perception and behavior on economic sanctions, *Contemporary Politics* 16(3), 263-278; Hufbauer, G. (2009), *Economic Sanctions Reconsidered*. 3rd ed., Washington, DC: Peterson Institute for International Economics.
[40] Reilly, J. (2012), China's Unilateral Sanctions, *The Washington Quarterly* 35(4), 121-133.
[41] Zhao, S. (2013), Foreign Policy Implications of Chinese Nationalism Revisited: The Strident Turn, *Journal of Contemporary China* 22(82), 535-553.
[42] Reilly, J. (2012), China's Unilateral Sanctions, *The Washington Quarterly* 35(4), 121-133.
[43] Council on Foreign Relations (2018), China's Maritime Disputes [Online], available from: https://www.cfr.org/interactives/chinas-maritime-disputes?cid=otr-marketing_use-china_sea_InfoGuide#!/chinas-maritime-disputes?cid=otr-marketing_use-china_sea_InfoGuide.
[44] Johnston, A. (2013), How New and Assertive Is China's New Assertiveness? *International Security* 37(4), 7-48; Chen,

D., and Pu, X. (2013), Correspondence: Debating China's Assertiveness, *International Security* 38(3), 176-183.
[45] Zhao, S. (2013), Foreign Policy Implications of Chinese Nationalism Revisited: The Strident Turn, *Journal of Contemporary China* 22(82), 535-553.
[46] Rennack, D. (2006), China: Economic Sanctions, Congressional Research Service.
[47] Li, C. (2016), *Chinese Politics in the Xi Jinping Era: Reassessing Collective Leadership*, Washington, DC: Brookings Institution Press.
[48] Buckley, C., and Bradsher, K. (2017), Xi Jinping's Marathon Speech: Five Takeaways [Online], *The New York Times*, 18 October.
[49] Zhao. S. (2013), Foreign Policy Implications of Chinese Nationalism Revisited: The Strident Turn, *Journal of Contemporary China* 22(82), 535-553.
[50] Swaine, M. (2010), China's Assertive Behavior – Part One: On "Core Interests," *China Leadership Monitor* 34(2), 1-25.
[51] Chang original interview: Swaine, Michael (2018), Senior Fellow at Carnegie Endowment for International Peace, 2 May. In-person communication.
[52] Chang original interview: Hass, Ryan (2018), David M. Rubenstein Fellow at Brookings Institution and former Director for China, Taiwan, and Mongolia at the National Security Council (NSC), 1 May. In-person communication.
[53] Miller, M. (2016), The Role of Beliefs in Identifying Rising Powers, *The Chinese Journal of International Politics* 9(2), 211-238.
[54] Allison, G. (2017), *Destined for War: Can America and China Escape Thucydides's Trap?* Boston, MA: Houghton Mifflin Harcourt.
[55] Huang, Y. (2012), In the balance: China's economic conundrum [Online], *OECD Observer*, available from http://oecdobserver.org/news/fullstory.php/aid/3679/In_the_balance:_China_92s_economic_conundrum__.html.
[56] Bradsher, K. (2017), China's Taxes on Imported Cars Feed Trade Tensions with U.S. [Online], *The New York Times*, 20 March.
[57] Sanger, D. (2013), Chinese Army Unit Is Seen as Tied to Hacking Against U.S. [Online], *The New York Times*, 19 February.
[58] Press release (2018), President Trump Announces Strong Actions to Address China's Unfair Trade [Online], Office of the United States Trade Representative, 22 March.
[59] The White House (2017), *National Security Strategy of the United States of America*.
[60] House Foreign Affairs Committee (2017), Subcommittee Hearing on Development Finance in Asia: U.S. Economic Strategy Amid China's Belt and Road [Online], available at: https://foreignaffairs.house.gov/hearing/subcommittee-hearing-development-finance-asia-u-s-economic-strategy-amid-chinas-belt-road/.
[61] Yuen, F. (2014), Primacy of World Order? The United States and China Rise – A Review Essay, *International Security*, Winter 2013, 153-175.
[62] Chow, D. (2017), Why China Established the Asia Infrastructure Investment Bank, *Vanderbilt Journal of Transactional Law* (49), 1255-1298.
[63] Reuters (2017), General Electric, China's Silk Road Fund to launch energy investment platform [Online], *Reuters*, 9 November.
[64] Hurley, J., et al. (2018). Examining the Dept Implications of the Belt and Road Initiative from a Policy Perspective, *Center for Global Development* 121, 1-37.
[65] Reuters (2017), General Electric, China's Silk Road Fund to launch energy investment platform [Online], *Reuters*, 9 November; Shepard, W. (2017), These 8 Companies Are Bringing The "New Silk Road" To Life [Online], *Forbes*, 12 March; Honeywell (2017), What Is the Belt and Road Initiative? [Online], 8 September, available from: https://www.honeywell.com/newsroom/news/2017/09/what-is-the-belt-and-road-initiative.
[66] *Xinhua* (2015), full text of Xi Jinping's speech on China-U.S. relations in Seattle [Online], 24 September.
[67] Yi, W., and Brookings (2013), Wang Yi: Toward a New Model of Major-Country Relations Between China and the United States [Online], translated by Brookings Institution, 20 September.
[68] Chang original interview: Hass, Ryan (2018), David M. Rubenstein Fellow at Brookings Institution and former Director for China, Taiwan, and Mongolia at the National Security Council (NSC), 1 May. In-person communication.
[69] The White House (2017), *National Security Strategy of the United States of America*.
[70] Chang original interview: Senior Trump administration official (2018), Senior Advisor to President Donald Trump, 2 May. In-person communication.
[71] Corera, G. (2018), CIA chief says China "as big a threat to US" as Russia [Online], *BBC*, 30 January.
[72] Chang original interview: Senior Trump administration official (2018), Senior Advisor to President Donald Trump, 2 May. In-person communication; Corera, G. (2018), CIA chief says China "as big a threat to US" as Russia [Online], *BBC*, 30 January.

Caroline Chang is an associate for a U.S. global advisory firm specializing in international trade and regulations. She has completed extensive field work in both China and South Korea. Previously, she spent two summers with the U.S. Department of State in Public Affairs at the U.S. Consulate in Shenyang and with the Office of Chinese and Mongolian Affairs in Washington. In these roles, she prepared remarks and briefing papers for principals, including the Secretary of State and the Under Secretary of State. Ms. Chang earned her master's degree from the School of Global and Area Studies, University of Oxford, and her bachelor's degree in Political Science and Chinese Language from the University of Notre Dame. She speaks Korean and Chinese.

Is a Chess Player an Intelligence Analyst? A Philosophical Analytical Comparison between Two Disciplines to Understand the Nature of Intelligence Analysis

by Dr. Giangiuseppe Pili

OVERVIEW

Is a chess player an intelligence analyst? Chess is considered one of the most interesting strategic games in the Western culture. Chess is still one of the most challenging strategic games for our intelligence and understanding. Even though chess is a perfect information game, it is sufficiently complex and difficult to be unsolvable by sheer calculation. Just as the intelligence analysts, chess players face uncertainty, tactical dilemmas, strategic conundrums, stress, pressure, and great epistemological problems. Chess players deal with these problems all the time and face them using knowledge and foreknowledge of the opponent's capability and intentions to try to solve difficult problems on the chessboard. All they have is information to be translated into practical knowledge. After half a century, the first chess computer appeared on the scene, and after hundreds of years of chess studies we are still learning how to play better on the chessboard. Chess is still the most esteemed and competitive game of our culture and it is time to bring it, with all its complexity, to the Intelligence Community in order to learn from it.[1]

INTRODUCTION

The main goal of this article is to draw a detailed comparison between chess and intelligence in order to learn from both disciplines. The study is structured as follows: first, a justification for the comparison is given. Since Clausewitz, many scholars and practitioners have been suspicious in drawing comparisons between chess and other disciplines very close to intelligence (e.g., war studies). This is due to the fact that chess, unlike intelligence, is a perfect information game and does not allow any uncertainty. Though this statement is *practically* false, it forces a lack of imagination toward a possible comparison between the two. Then, I thought it reasonable to pursue the problem from another angle—that is, to focus on the chess *players* and intelligence *analysts* because they face common problems and issues as far as confronting a common complex reality in which an opponent is both trying to deceive them and fighting back against all their moves. Next, I consider the common challenges, the uncertainty issue, the necessity of understanding intentions of the opponent's strategies, and a detailed view of the intelligence cycle is given. In addition, not only chess players and intelligence analysts face similar problems all the time, but they also share common burdens and pressures. The third section is devoted to showing how analysis is what really makes the difference in chess and intelligence. Therefore, I present the reasons for that first, and how chess analysis works. In this way, it is possible to show how deeply related chess and intelligence are, if we consider what the chess players and intelligence analysts really do.

Finally, I have been a chess player since the age of four. Since I was fourteen, I have been a member of the Italian Chess Federation (FSI), which is officially part of the International Chess Organization (FIDE). I am an average tournament player (1698 ELO FIDE). I was a chess trainer recognized by FSI. I was a regional referee, and I published several publications about chess and philosophy.[2] However, in order to maximize the accuracy of the analysis, I interviewed a stronger player, Herman Grooten (IM, 2337 ELO FIDE), the author of esteemed international books[3] and a trainer. I read research works on cognitive psychology.[4] Finally, I allowed the circulation of the first drafts of my work to my chess contacts in order to improve it.

CHESS AND INTELLIGENCE: A DEEP RELATION

Chess as an Old Profession if Not a Discipline

In the intelligence studies literature, there are other papers that consider the relation between intelligence and other disciplines[5] or how to learn from gaming.[6] Focusing our attention on the former, the scholars recognize the importance of drawing comparisons and developing new ideas from other *disciplines*: "Some practitioners have argued that intelligence analysis, in comparison with medicine and law, is an ascending profession that will require time to develop key attributes such as a distinct literature, certification, governing boards, and knowledge."[7] Is chess a discipline, a profession, or just a game?

Chess was a profession for centuries and today it is a discipline because it meets all the characteristics that define it: it has a technical and distinct literature, it has a world federation as governing board of all the national federations, and it has its own body of knowledge and a specific literature. Since early modern times, the strongest players have been highly paid and rewarded. During the 20th century, chess began to be a profession for many players, not only for the world champions. In the USSR, strong chess players had many benefits: they could easily have access to higher education and the state provided them the means to live. During two decades, from the 1970s to the 1990s, a major revolution occurred. It was the dawn of the professional chess players; chess started to be like all other sports, in which the top players are engaged in a world competition where the best accede to high payments and rewards granted by sponsors, patrons, and awards for the tournament winners.[8]

Chess was a profession for centuries and today it is a discipline because it meets all the characteristics that define it: it has a technical and distinct literature, it has a world federation as governing board of all the national federations, and it has its own body of knowledge and a specific literature.

All the aspects of chess are highly competitive, from the early training to the top levels of competition. In addition, as in tennis and other sports, chess has its own ranking, the ELO rating, which is international. It fixes categories (national and international) and establishes fixed ratios of access to major tournaments and training events. The ELO rating is certified and administered by FIDE. Certificates have begun to circulate. Official chess trainers are supplanting the self-declared experts.[9] In addition, chess is not only a Western game anymore. Apart from Russia and former Soviet allies,[10] China, Iran, Israel, India, the EU, and even the U.S. invest resources in chess education. Chess today is a mirror of the international, global geopolitical competition.

To be a top player, cognitive and practical skills must be trained and learned. Undergoing a continuous open-ended process of training is needed, preparing his chess, and studying his likely opponents are all necessary. A chess player, and his team, has his own intelligence cycle. Indeed, a chess player is a sophisticated intelligence analyst and his results are directly correlated to his quality and capacity to analyze strategically, tactically, positional moves, variants, positions, and games. All the analyses are carried out under many kinds of different pressures that can thwart and hamper one's capacity to deliver appropriate, timely analysis. How could there be uncertainty in a perfect informational game?

CHESS AND INTELLIGENCE: COMMON CHALLENGES FOR TWO SIMILAR PROFESSIONS

Chess Players and Intelligence Analysts Both Face Uncertainty

Chess players and intelligence analysts deal with a very complex reality in which an opponent is trying to win his own game. Even if a chess player knows his opponent, he cannot be sure of his intentions, especially from a strategic perspective. It is often said that chess is a perfect informational game; all the information contained in the game is readily available to both players and it can be theoretically exhausted by sheer calculation. It is so true that chess has been considered an example of this kind of game since the foundation of the theory of games.[11] However, after a certain degree of complexity, the human mind is not able to exhaust the game by sheer calculation.[12] Coupled with the average friction determined by the pressure to win against a real opponent, the chess player simply falls back against the curtain of uncertainty. However, it seems still counterintuitive to state that a chess player is doomed to strive against uncertainty on the chessboard.

The number of possible chess games is sufficiently high to be inexhaustible by any calculating machine that could be built in our universe.[13] The number of chess moves is so high as to exceed the number of atoms in the universe itself.[14] Therefore, nothing—and then *nobody*—can rely only on sheer calculation as far as it is impossible to calculate everything in advance and this is true even for the best computers.[15] If this is true for chess, then it is even truer for our reality taken as a whole. Nothing and nobody can exhaust all the possible situations that can happen in the future.[16] Consequently, both a chess player and an intelligence analyst face a certain degree of uncertainty. Perfect information is not a sufficient condition to avoid uncertainty and, therefore, if perfect information is not enough to get it, then everything less than perfect information would not be sufficient to avoid uncertainty. However, this does not mean that information is useless.

Chess players and intelligence analysts deal with a certain degree of uncertainty, and it is in their interest to do their best to decrease that uncertainty. Indeed, as we will see, a chess player is able to anticipate errors and exploit opportunities *only if* he is able to calculate variations (namely, possible positions that could happen in the future). A Grand Master (GM) is able to calculate up to 30 moves in advance, when needed. On the average, in a tournament game, a chess player calculates from three to five moves for each variation[17] considered for every position for the entire game with possible exceptions (chess is a very contextual

game). Before making a move, the chess player must usually calculate 2-4 different candidate moves, and they will be selected by strategic and tactical considerations that require calculation anyway. If we combine these two pieces of information, we discover how staggering the computational task is. A chess player can only minimize the uncertainty and only in some occasions is he able to reach complete certainty on the chessboard. Namely, he is able to forecast the future very precisely. This is possible when all the moves are "forced," namely, when the opponent can play only one move each time because only one move is left to be played. This variation of forced moves has a name in the chess jargon—"combination." Its study pertains to the training of the tactical ability of all chess players and several manuals and, today, chess apps-software are dedicated only to it.

The intelligence analyst's world view is based on a very complex ontology, namely on a great variety of facts (natural facts, social facts, mental states, fictional entities, and causal relations).

An intelligence analyst is challenged by a certain degree of uncertainty because all the *relevant* information is not always available to him and the risk of overloading information is also possible. Thus, the relevant information has to be selected by him during his mental analysis and during his preparation for it. In addition, reality does not resemble a perfect information game, as was shown above. The intelligence analyst's world view is based on a very complex ontology, namely on a great variety of facts (natural facts, social facts, mental states, fictional entities, and causal relations). This metaphysical statement should be proven in detail and it would be truly fundamental to advance the actual intelligence theory as was recognized by Stephen Marrin.[18]

An intelligence analyst cannot deal with uncertainty only through sheer calculation, whatever this means in the intelligence context (analysis of future scenarios, evaluation of alternative hypotheses, expectations of forthcoming events, etc.). For example, if we consider Clausewitz's theory, the "fog of war" cannot be dissolved only by intuition, common sense, and information. Simply, it is not enough. This is true also for a chess player, insofar as a chess player cannot calculate as much as he would like. An intelligence analyst conducts calculation on fictional future events in order to evaluate the present backwards; namely, the intelligence analyst always has to imagine possible scenarios in order to understand what kind of alternative situations could happen. When the mind is not able to evaluate the present clearly, it turns to possible futures to select the only one that seems to be more promising. Therefore, both an intelligence analyst and a chess player compare the present to alternative futures in order to catch the best option available in the present moving backward, and they do it searching for the truth because only the truth of the hard facts guarantees success. However, chess players and intelligence analysts do not face uncertainty only. They deal with other common challenges as well.

CHESS PLAYERS AND INTELLIGENCE ANALYSTS STRIVE TO UNDERSTAND INTENTIONS AGAINST THE OPPONENT'S DESIRE TO TAKE THEM CONCEALED

Strategic intelligence is mainly about understanding the intentions of enemy leaders and countries. The intelligence analysts focus their attention on the enemy's capabilities and behavior to figure out what an opponent intends to do. Therefore, strategic intelligence is about intentions, capabilities, and behavior.[19] The real challenge here is not only the uncertainty determined by the lack of (or by the overloading of irrelevant) information. Indeed, the opponent is alive, and he will strike back against the intelligence analyst's efforts.[20] In this context, the opponent will do his best to deceive the analyst in order to prevent him from knowing his *real* intentions. Chess is an example of a zero-sum game. Since Clausewitz, it is often said that a game of cards—let's say poker—and not chess, resembles more the reality of war or highly-conflictual situations than chess. This is because poker is a non-perfect informational game. However, as we have seen, perfect information does not lead necessarily to certainty. Indeed, a chess player knows quite well the uncomfortable feeling of being deceived or surprised by his opponent. I want to give a very simple example.

It is possible to choose different sets of moves in order to reach the same position. These different variations are *not* equivalent because, even though they arrive at the same result, they try to deceive the opponent's ability to grasp intentions, covering the real plan as much as possible. This usually strikes average opponents and they start to think, which is the desired effect. Then, this means practically that they have to calculate and select candidate moves. This is a very basic example for an average chess player, but it shows how a player thinks when he wants to cover his real intentions. At the GM level, chess players search for different ways to arrive at the desired positions without following the expected paths. Of course, this is not always possible, but GMs try to exploit the expectations of their opponents all the time in order to achieve a minor strategical surprise.[21] This is true for all the different moments of the game (opening, middle game, and ending).[22]

Even GMs are not able to anticipate all the opponents' plans because other GMs may discover new ideas and implement them in complex ways on the chessboard. Sometimes the plans are clear. Sometimes they are quite unintelligible. Then, an intelligence analyst has to understand the enemy's intentions through his behavior and capabilities just as a chess player has to ascertain the opponent's plan looking only at his moves. However, in both cases, to study the opponent's behavior and capabilities is not enough to discover his real plans and intentions.

CHESS PLAYERS AND INTELLIGENCE ANALYSTS UNDERGO A CONTINUOUS, OPEN-ENDED CYCLE TO GATHER INFORMATION ABOUT THE OPPONENT'S INTENTION AND BEHAVIOR

A chess player follows his own "chess cycle" that resembles the intelligence cycle. As it was described by Jan Goldman: "A continuous process that includes five phases that encapsulate the work done within the intelligence community. The five phases include the planning and direction phase of what intelligence needs to be developed based on existing gaps of knowledge, the collection phase of obtaining the information, the processing phase of converting the raw information into finished products (to include transcription, translation, imagery interpretation, etc.), the analysis and assessment phase of turning this information into a 'finished intelligence product' by evaluating and integrating the information, and the final phase of distributing the product to those that have a 'need to know'."[23] Approximately, this is what a chess player does all the time.

The chess player starts asking himself what his strategic goal is. Then, he plans the order of the moves to be played to realize his plan tactically. Therefore, the chess player has both the roles of decision-maker and intelligence analyst, whose balance is a task itself. After the definition of a strategic goal, he has to check that the opponent is not threatening him tactically, e.g., if there are no pieces hanging,[24] if the king is secure,[25] etc. At the same time, he verifies that he has no better opportunities to exploit, e.g., to capture an undefended piece/pawn, to checkmate the opponent in one move, etc. Therefore, the chess player has his own "chess cycle" which starts defining a strategic goal. It goes on analyzing the position by a tactical perspective and by calculating alternative variants based on a selection of candidate moves. The chess players undergo the chess cycle for the entire chess game and beyond. Indeed, on a professional level, he has to track the record of other GMs, and collect and gather update information on their games, their performances, etc. GMs have their own databases, based on what all the chess players can find online or on dedicated software such as ChessBase.[26]

The intelligence analyst implements the intelligence cycle because he has to deliver an intelligence report to the decision-maker. Therefore, he has to plan the intelligence collection, gather information, analyze it, and calculate possible scenarios in order to establish the relative likelihood of them. Then, he has to refine the findings, adding more information and data, and finally he arrives at delivering the intelligence outcome in which he grounds the rationality of the decision-maker's decision. Possibly, he has to employ structured analytic techniques to enhance the overall reliability of his outcome. Thus, the intelligence cycle performed by an intelligence agency as such is an open-ended ongoing process because the decision-maker needs updated, non-expired information on the context.

CHESS PLAYERS AND INTELLIGENCE ANALYSTS WORK ALWAYS UNDER GREAT PRESSURE

Time Pressure

A chess player is continuously under a great amount of pressure from within and from without, and his feelings vary accordingly to the situation on the chess board. Indeed, he has to struggle with different levels of pressure that can bring him to experience different kinds of feelings related to how he is able to cope with it. Time, informational and cognitive pressures, and psychological and physical pressures are all experienced simultaneously.

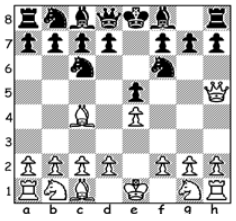
A chess game has a fixed time; the player who finishes the time first loses the game, whatever his position on the chessboard. Time control is so important to define different kinds of tournaments and chess games.[27] The classic chess rating games (1:30 + 30 seconds) are the only ones able to rate the players in the official FIDE ranking; namely, the official world chess champion has to be the winner of a classic chess tournament. Rapid games (15' + 10'') and blitz chess (3' + 2'') are the other two typical chess typologies. As far as the time control defines different kinds of chess styles and tournaments, time factor and time pressure are fundamental to chess (at least in the last 100 years). First, the less time you have, the less you can think and the more it is likely you will make mistakes and, possibly, totally blunder. Indeed, formal logic defines calculation as a finite process of elaboration of a finite input to a finite output through a finite set of rules of transformation.[28] Therefore,

calculation requires time to compute information and to select it in the correct, relevant way. Second, the chess player is always aware of the flow of time and, since he knows he loses the game if the time ends, he must always manage time.

The intelligence analyst faces the same time pressure. He has a decision-maker's requirement that has to be fulfilled in a very short amount of time. Indeed, quick decisions have to be readily taken and they demand intelligence outcomes delivered in a timely manner. Therefore, the intelligence analyst has a time constraint and he has to manage time effect and pressure constantly, especially in difficult cases such as 9/11. Indeed, as in chess, time pressure is considered one of the most (if not *the* most) important factors that can hamper a perfect intelligence outcome. After all, the intelligence analyst starts to work toward a decision-maker's need for information, which it is often determined by the urgency to decrease the uncertainty for a decision that must be taken as soon as possible and that is not possible to postpone. As observed by Randolph Pherson and Richards Heuer, "Intelligence analysts work under time pressure with information that is incomplete, ambiguous, and sometimes deliberately deceptive."[29]

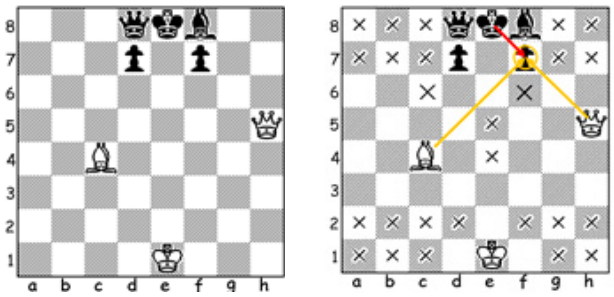
Informational and Cognitive Pressure

Intelligence analysts and chess players also face informational and cognitive pressures. The two are related. Informational pressure is the constraint determined by the threshold of information needed to accomplish a computational task. For example, a tactical chess puzzle can be solved considering the relevant information is available on the chessboard coupled with the right calculation. To give an example (the uninterested reader can skip it):



White to move

To solve this puzzle, a chess player can consider only a little information from that available. In the diagrams below, I selected only the pieces in action and relevant to solve the puzzle (left) and the useless information that a chess player has to avoid considering to maximize his result, minimizing time and calculation (right).



However, the chess player is always bombarded by non-relevant information and it is not always easy to select the right piece. In the example, all the pieces are on the chessboard but only seven of them are relevant and the information needed is to see that the black king is closed by his own pieces, that f7 is weak and attacked two times. No other information is needed to solve the puzzle.

This is a big challenge for the intelligence analyst as well, insofar as he has to search for the relevant information needed to solve a particular request. However, he has to select and discharge information that turns out to be useless in the particular situation that he is studying. In addition, in the usual case of alternative hypotheses, the analyst considers information that will turn out to be useless because only one scenario will materialize, but he has to be diligent in considering relevant alternative options and related evidence. Again, chess players and intelligence analysts are similar in this respect: the more knowledge they acquire and the more their analytical skills increase, the less they need to search and select and calculate to solve the task. Indeed, calculation is often used to clarify a present position which is not clear, and this is true also in chess. However, insofar as the result is always at stake and the pressure to be sure to have solved the problem correctly is always there, the chess player and the intelligence analyst experience the same informational pressure, namely, to find the right amount of information able to solve a problem beyond any reasonable doubt. This is shown by the ordinary attitude to search for new evidence or information to check the result. This could lead to overloading, psychological stress, and further uncertainty on the reliability of the outcome. This brings us to the cognitive pressure.

Cognitive pressure is determined by the need to process the information in the right amount of time. Here, the pressure is on the process. Chess players and intelligence analysts need to calculate and process information to reach their goals. Then, they use their cognitive capability, namely senses, inferential reasoning, and introspection, the main cognitive capabilities considered by the epistemologists.[30] They have to reach a reliable outcome through processing relevant information.

However, cognitive abilities are finite transformations of symbols through fixed rules whose work requires time and bio-chemical energy. Under time constraints and finite energy resources, the result could be flawed by local unreliability due to a malfunction of the cognitive processes. A chess player experiences cognitive pressure especially when he has to deal with long calculation and combination. This is true in war, where the enemy tries to use information warfare tactics to achieve cognitive pressure, but it happens all the time in chess.

Non-biased analysis demands openness and transparency...

The same happens to an intelligence analyst who is forced by the situation to analyze the scenario under great pressure. Indeed, an intelligence analyst knows that the result of his analysis could lead to big mistakes and, sometimes, the lives and physical security of other people could be at stake. Therefore, this pressure is not due to time because it deals directly with the problem of being sure that the calculation was right. It is not only a matter of the capacity to calculate but also to verify the calculation avoiding mistakes on the two distinct operations of the mind (calculation and evaluation of the calculation by analysis and introspection). The intelligence analyst faces the same scenario when he is not sure about his ability to make the right analysis, even though he tries to exhaust all the possible alternatives. Under a certain degree of friction, however, everybody can doubt their own cognitive capacity.

Psychological and Physical Pressure

Chess players and intelligence analysts experience psychological pressure. Indeed, during a chess game the chess player mood is completely related to the situation on the chessboard. He can experience tension, rage, aggressiveness, and depression, but also joy, excitement, and enthusiasm. Sometimes the tension is so high that players can behave very badly.[31] Focusing our attention on the result on the chessboard, psychological pressure could be induced by many factors such as the ELO rating of the opponent. The fear of decreasing the rating could bring the player to be more or less willing to take risks or to feel confident in being able to win the game. The expectation can vary from increasing the propensity to take risks to the opposite. Psychological pressure could be daunting because the players know that everything is, theoretically, under their own control, and they start from an equal position. However, they know by experience that only one mistake is sufficient to lose a game. This could be extremely frustrating; the chess player is alone in his defeat and it is not easy to manage the psychological burden.[32] The psychological pressure can be so harsh as to induce players to retire or even worse.[33]

The intelligence analysts are under great psychological pressure for many different reasons. First, their work implies a certain degree of responsibility in the national security and the lives of the citizens could be at stake. All parts of the intelligence cycle can lead to psychological friction. For instance, gathering human intelligence is a delicate issue and working under secrecy is a pressure itself, as far as the intelligence analysts cannot speak freely of their work even with their relatives. In addition, working under cover is even more demanding. Analysis is not an easy task, and it could lead to stress and fatigue that could be translated into further psychological pressure. It is not easy to accept being not omniscient and that a cognitive problem might not have a positive solution. However, the analyst is called to give an answer anyway and he ought to make his own decision in writing his report to the best of his knowledge. In addition, non-biased analysis demands openness and transparency but, even working respecting the integrity of his/her own profession, it is not always easy to be sure not to be biased. The relation between the officer and the policymaker is always challenging as it is reported by the politicization literature that underlines this.[34]

Finally, chess players and intelligence analysts work under physical pressure. A chess game can go on for hours and the player has to remain focused on the task. This is very tiring physically, as all chess players can testify. Indeed, the hard work of the brain requires a lot of energy. The chess player has to be able to endure and sustain prolonged mental activity, which is known as one of the most demanding of all, as far as chess activates many different cognitive areas of the brain.[35] The same argument applies to intelligence analysts, who must stay focused on their task for many hours or days. A chess tournament has an average of six games; instead, intelligence analysts work every week. Then, physical pressure cannot be underestimated because mental and psychological stress contribute to physical fatigue and further friction hampers analytical capacity.

CHESS AND INTELLIGENCE: WHERE ANALYSIS REALLY MAKES THE DIFFERENCE

Why Analysis Is Needed: Level of Complexities Involved in Chess and Intelligence

Analysis is a peculiar activity of many disciplines and professions, namely those that require selecting information to maximize the result while minimizing the risk of errors. Different disciplines and professions require different kinds of analytic techniques

and methods. In intelligence analysis theory, scholars such as Stephen Marrin and Efren Batches-Torres considered the case of medicine.[36] This means that we should seek improving intelligence analysis looking to other disciplines as well.

Both chess and intelligence require a selection of relevant information to formulate appropriate knowledge facing a live opponent. Indeed, intelligence without an opponent or an enemy is not intelligence at all, according to many scholars.[37] This means that intelligence is not an ordinary human science. It is not something entirely comparable to academic research. The intelligence analyst deals with both facts and intentions and he/she can be misled in connecting the dots between the two, insofar as knowing the facts is not always sufficient to reach the enemy's intentions. This is particularly true for strategic intelligence, where knowledge of enemy intentions and beliefs is at the core of the task.

This applies also to the chess players, as far as they deal with exactly the same problem: grasping intentions by facts is not always feasible and the opponent is always ready to strike back. Indeed, the big difference is that the chess player is the only one who pays for his mistakes, whereas the intelligence analyst usually sees the direct consequences of his blunders. Indeed, one of the most painful experiences for a chess player is losing due to a blunder after having led a game. Getting a winning advantage is not enough. However, chess players and intelligence analysts face a similar working environment as they both have an opponent and they have to decrease uncertainty studying facts and the opponent's behavior. In order to better fix this point, I am going to consider the different levels of complexity involved in chess and the intelligence analyst's world, comparing the two.

Factual Dimension

The first level of complexity is defined by the "sheer facts." On the chessboard, sheer facts could be defined in a rigorous way; everything that can be described by chess notation and appropriately reported in the chess form[38] is a fact. A set of moves is also a fact. Then variations, positions, and games are all facts; these are the all "pure" facts on the chessboard, where the simplest one is the square.[39] The equivalent conception of facts in real life is the so-called "natural fact." With this term, I mean just what it is outside the analyst's mind, and whose nature is defined by causal relations. This excludes social facts because they require more than that. Thus, natural facts are not the main goal of intelligence analysts, as far as they could be important as indicators, but they are not interesting per se. Indeed, the intelligence analyst has to provide a final assessment on a particular situation on the ground or on the enemy's intentions. This requires much more than natural facts; an evaluation of a state of affairs requires norms of judgments and principles of thought. This is true also for chess.

Indeed, one level of calculation in both intelligence and chess is just to imagine a future scenario. The evaluation of it is a completely different operation of the mind. To prove this point, we can just show different positions without giving any assessment of them. In fact, the assessment depends on rules that are not part of the world, so to speak, because they depend on the mindset of the human beings, their interests, and intentions. This is true for machines also.[40] Then, the evaluation of a specific position on the chessboard requires tactical and strategic considerations as is true in intelligence. The evaluation of x requires a set of rules that normalize the conditions to allow particular judgments. Evaluations without rules are not possible and, indeed, this is why only rational beings can really make a judgment.[41] Hence, the factual dimension is the basic layer of complexity.

Evaluative Dimension

Moves, positions, variations, and games are objects of evaluation. Different facts require different evaluations. Therefore, even with few objects existing in chess (pieces + squares), the evaluative dimension is so complex. If the factual dimension increases geometrically, the evaluative dimension increases exponentially. Indeed, a variation is a set of moves and, to exhaust it from a factual perspective, it requires only being able to memorize all the moves. As we have seen, this is not possible, as far as nothing can record all the possible moves. Instead, the evaluative dimension adds a further level. Indeed, even if a move has to be calculated in advance, its evaluation is not reduced to it. It requires a set of rules to value it. This is what we call the principles of strategy and tactics, and they apply both to chess analysis and intelligence analysis.

Moves, positions, variations, and games can all be evaluated, and we have appropriate symbols in the chess notation to track them. For the moment, it is sufficient to say that the evaluative perspective adds a layer partially disjointed by the factual dimension, as far as this is an evaluation from a strategic, tactical, or positional point of view. The chess player must consider all these different normative aspects together for each position. Sometimes, tactical considerations overrule strategic necessities, and vice versa. Therefore, chess analysis starts with knowing facts, goes on to considering the principles of strategy and tactics, and ends with a general evaluation of the position whose outcome is the decision (move). Chess is a highly contextual art.

Intelligence analysts face a similar cognitive environment. Indeed, they have to start knowing the facts in the geopolitical domain. Therefore, they have to know what is happening on the ground; by "ground" I mean a general space of action, whose definition is highly contextual and related to the kind of information request the decision-maker posed. Then, strategic intelligence is much more focused on social facts such as states, organizations, infrastructure, etc. than tactical intelligence, which can deal only with natural facts such as the description of the battlefield (let us put aside the description of the armies on the ground).

Then, the definition of the kinds of facts is highly contextual and, therefore, their evaluation is even more so (in information philosophy this is called "level of abstraction,"[42] whose definition depends on the initial research question, namely the decision-maker's informational request). Indeed, the evaluation of social facts in a conflictual scenario depends on understanding the principles of the strategy and tactics involved. For instance, evaluating China's Belt and Road Initiative (BRI) does not require knowing only the hard facts (dimension of financial investments, geographical details of the "road and belt," etc.), but also understanding what BRI is intended to be and what China's government wants to achieve. Again, hard, natural facts are not sufficient. The intelligence analysts have to consider strategic principles and goals in order to give a rational assessment where the rationality involved here is not the scientific one, which is mainly geared toward discovering new laws of nature. It is quite the opposite; as in chess, moves without principles cannot be evaluated. This is true also for chess engines (software), whose strength is related to their capacity to apply strategic principles to moves calculated in advance. Understanding and knowing are two different epistemological activities; evaluation means understanding strategic principles and applying them to a concrete, highly contextual case.

Informative Dimension

Evaluation is not exhausted by knowing facts. Today, chess engines are stronger than the world champion; they can calculate many moves in advance applying appropriately the strategic principles we programmed for them.[43] Then, there is a connection between evaluating-understanding and calculating-knowing the fact. The bridge lacking is information.

In order to maximize the chances to win, a chess player must select 2-4 candidate moves. This selection starts with a positional evaluation: threats and opportunities are considered. Then, if we look closely to the cognitive activity, the chess player starts knowing facts (possible moves); then he makes a first provisional evaluation (principles of chess applied to those moves). However, this is not enough because chess players always search for confirmation and falsification. This double process is carried out by calculation; the chess players imagine the different variations that start with the candidate moves. Then, they compare in their mind the different stop positions and they arrive at the move to play.[44] This cognitive activity is run by the chess players' minds.

Whatever a calculation is, it always requires information to be run. The information category defines the kind of cognitive task at stake. Mathematical calculation is different from chess calculation because it involves different kinds of information. Thus, information is what is needed to provide an answer to a question that, to be solved, requires a computation. Different tasks require different amounts of calculation and then different kinds of information and analysis. Therefore, knowing facts and their evaluations requires a certain amount of information, whose quantity and quality depend on the research question. Indeed, different chess puzzles require different information (amount of information), and not all information available is needed to solve the problem (quality of information). Then, we can define the "relevance of information" as a function of its effect in the calculation: the more the information is relevant in a certain position, the less we need to add to solve the puzzle. Then, we can say that relevant information is the precise amount of information needed to solve the problem, whose precision defines its quality.

The same argument applies to intelligence analysis. Indeed, as in chess, the facts are not enough to exhaust the intelligence analysis because the outcome has to be an assessment of the situation on the ground. The intelligence analyst is truly like the chess player in this respect. Indeed, he has to start searching for facts. Then, he has to keep in mind the stakes defined by the decision-maker and the principles of evaluation in order to make a sound judgment (intelligence assessment). However, between facts and principles a calculation has to be made. Actually, a calculation is not even enough because the intelligence analyst has to calculate different scenarios (the variations) in order to select the most likely outcome(s). His stop position will depend on his analytical skills and on the quality of information he has. The more a piece of information is relevant, the less the intelligence analyst has to calculate. This brings us to the next subject.

Psychological Dimension

The more relevant information we have the less we calculate, and then the less energy we need to do it, and then the less time we need to make the calculus: energy, time, information, and calculation are four different ways to speak about the same activity and we need to understand all four to grasp the complexity. The

psychological aspect is distinct from the others, as far as it deals with both cognitive processes and their emotional expressions.[45] Then, according to the externalist theories of knowledge, a cognitive process is a psychological mechanism able to produce beliefs, and it could be evaluated by its reliability.

Chess players and intelligence analysts both use all their cognitive capability to try to solve their tasks. The quality of their result is directly related to the other dimensions but also to their own cognitive skills; even with the best relevant information, a poor cognitive process will be unreliable anyway. Indeed, chess training is extremely demanding. It is aimed to enhance the overall reliability of the cognitive process for a prolonged time. It is estimated that a chess player must study eight hours per day, every day for ten years before becoming a GM.[46] Then, GMs and world champions all agree that very hard work is necessary to become a master in chess. Intelligence analysts are trained on different topics; they learn structured analytic techniques and how to apply them effectively; they study qualitative and quantitative methodologies and how to use appropriate technologies. This is all due to the psychological dimension, which was brilliantly considered by Richards Heuer in one of the best studies available in intelligence studies.[47]

CHESS ANALYSIS – DURING THE GAME AND AFTER IT

The previous section showed the different dimensions of complexity shared between chess and intelligence, and they are the different levels of a complex analytical ladder. In this section, I will focus my attention on how a chess player analyzes. Mainly, there are two different kinds of analysis in chess: (a) the analysis during the chess game and (b) the analysis after it is over. (a) is divided into three categories: (a.1) tactical analysis, (a.2) positional analysis, and (a.3) strategic analysis. As I will show in a moment, the order is not by chance. Instead, (b) can be divided into two (b.1) openings, and (b.2) analysis of the opponents.

Chess Analysis During the Game

The literature about all the different typologies of chess analysis is so huge that we do not know how many publications are available on the topic. Sometime ago, Mario Leoncini, an Italian chess historian, told me there should be more than 60,000 publications on chess.[48] I asked Claudio Selleri, one of the most influential chess publishers in Italy, how many books are available in English on the topic "chess analysis." He replied that it is impossible to have a precise number but it could be more or less 1,000 about analytical training only.[49] This number is impressive, if we consider that it indicates only one aspect of all chess analysis. In addition, it is questionable whether English is the language of the main chess publishers, as far as the Russian chess publishers were the most established of all. This means that chess analysis, again, is something truly fundamental for chess players.

Indeed, as I argue above, chess analysis is one of the two components that really make the difference during a game, where the second one is the pure will to struggle to the end. In order to give a very short picture of tactical analysis, I follow Ramachandran Ramesh,[50] just because his work explains all the aspects involved.

The tactical analysis is mainly based on four different operations: (1) detecting immediate threats (hanging pieces, undefended pawns, etc.) that can easily be exploited by the opponent; (2) pattern recognition (recognizing a schema—a pattern—in the position); (3) checking and selecting candidate moves; (4) sheer calculation and evaluation of the stop positions. As the cycle of intelligence is an idealized model of real intelligence activity, this tactical analysis is a generalization of something more complex; e.g., the evaluation of the stop positions cannot be exhausted only by tactical considerations, but it also requires positional and strategic assessments as well. However, I consider this model of analysis sufficiently plausible for our purposes.

Tactical analysis involves the simulation of variations in the mind of the chess player. Then, it is something very concrete and it is the first pillar of playing chess. However, tactics is not enough to decide what to do when immediate threats are not on the horizon and we have to decide how we want to approach the game: aggressive attacks to the king, positional proactive defense, expansion in the center, etc., are possible ideas for a strategic, long-lasting approach to the game. Then, a plan based on positional and strategic considerations is needed. From the short run we look to the long run. If tactical analysis involves mainly concrete variations and quantifiable advantages, positional analysis is much more subtle and qualitative. Indeed, if chess tactics are mainly about knowing facts and assessing them primarily by quantitative estimations, positional analysis is much more related to the qualitative features of the position. Then, positional analysis is considered the most subtle part of the art of chess.

According to Ramesh, positional analysis is based on seven different categories: safety of the king, activity of the pieces, materials, pawn structure, space, initiative, and structural weaknesses. I will not consider them, but it is worthy to observe how much these features resemble the kind of evaluation a military decision-maker must consider in wartime to elaborate a course of action; these categories are valuable for all the actors involved in non-cooperative

conflictual games, as war and chess. The positional analysis is focused on understanding the situation from both a static and dynamic perspective and what to do in the long term, considering qualitative features of the position. Qualitative features are not abstract properties because, if they are appropriately detected, they translate into material advantages and decisive positions. Finally, positional analysis is what grounds a strategic understanding of the position; namely, it is the kind of knowledge that enables the elaboration of a sound plan and counterplan. Indeed, positional analysis always considers both players.

Finally, strategic analysis is mainly focused on elaborating rational plans when time allows us to implement them. Indeed, chess is so difficult because the players are continuously engaged in a permanent friction, as far as the chessboard is not big; after 4-5 moves the pieces start to interact and threats and weaknesses pop up everywhere on the board. However, tactical analysis allows the player to know facts and to save the day (the position). Yet, this is not enough because, without a good plan, we cannot place the pieces in the right place, we do not know what to do, and we mainly react to our last opponent's move. This is not enough, especially at the GM level, where the players know they cannot win expecting errors.

Consequently, strategic analysis starts from three main questions: Where do I want to place my pieces in order to maximize their strength? What can I do to thwart the opponent's plan? What can I do to improve my position looking to the long term? The sophistication of the strategic analysis is quite high, especially when a GM analyzes his game. Indeed, the less a player is strong, the more he has to ground his analysis on tactics only. This shows that tactical analysis is essential, but only strategy makes the difference between the average chess player and the stronger one. Then, a chess cycle can be approximated to something like: search for facts (moves), analyze the position from a tactical perspective; if you are free from tactical conundrums, then take time to analyze your position in order to deliver a long-term strategic plan to improve your position. Different players prefer different approaches to chess analysis. Some are better tacticians; others are positional players. However, all chess players must master all the levels of chess analysis to be professionals.

Chess Analysis After the Game

Chess analysis after the game has devolved to training and to studying the opponents. This is even truer for stronger players. The professional players study the opponents all the time. They consider what opening they usually play and what are the best aspects of the opponents' chess skills. They search for weaknesses everywhere, from the opponents' training to their psychology. The study of a single opponent considers his comfortable zones, whether he prefers to play middlegames or endgames, etc. Then, this kind of chess analysis has devolved mainly to tracking the record of the possible opponents, studying their games, and finding biases, uncomfortable zones, and psychological weaknesses. Even given the chess engines ead programs, chess between humans is still only one thing: a battle of the mind. Hence, this aspect of chess analysis resembles the open-ended intelligence estimates, because the players study their likeliest opponents and search for threats, risks, weaknesses, and relative competitive advantages. Chess professionals are under continuous open-ended intelligence tradecraft!

CONCLUSIONS

Chess is still considered one of the most difficult strategic games in the Western culture. The parallel between chess and intelligence shows how much the two professions have in common from both a metaphysical and epistemological perspective. Indeed, strategy and tactics are both based on knowledge of hard facts and understanding of goals at stake. Chess requires training, skills, generally a specific preparation, knowledge, will, and discipline. In this article, it is argued that chess players and intelligence analysts share common problems and common goals. Therefore, the several comparisons between the two disciplines show that intelligence analysts could benefit by knowing how chess players try to solve their common problems. After all, chess as a game is highly considered as a fruitful, even if limited, comparison to war and battles. As argued, though, intelligence analysis as such can find many parallels, insights, and inspirations from chess and chess players. In addition, chess players, especially but not only at the top levels, experience a highly competitive environment in which knowledge, information, and analysis really make the difference between the top players and the rest of the world. This article would be the first to make this comparison in the intelligence studies literature and it would be the grounding work for further research in how to improve intelligence analysis over other disciplines. When we think about chess, we think about intelligence and we should take this comparison seriously.

[Author's Note: To a certain extent, this article was a collective enterprise. Many scholars and chess players helped me in developing and improving it. First, I am extremely grateful to Michael Landon-Murray for his invaluable suggestions, comments, and insights during and after the 2019 IAFIE conference. I want to thank Uberto Delprato, intelligence practitioner and good chess player (Candidate Master), for his insightful comments and corrections. I want to thank my renowned chess publisher, Claudio Selleri, for his help and information. I strongly appreciated Herman Grooten's talk and comments. Herman is

an International Master and the author of many relevant chess books. I was honored to discuss with him the topic of this article and to receive his feedback on it. I thank Stephen Marrin and Efren Baches-Torres for reading suggestions. Finally, I am grateful to the editor of this journal, William Spracher, for his encouragement and support. That said, of course, all errors are mine.]

NOTES

[1] The reader can find a presentation of this paper on YouTube: https://www.youtube.com/watch?v=1tqfVF09rfw (accessed October 3, 2019).

[2] Pili G., (2012), *Un mistero in bianco e nero – La filosofia degli scacchi, Bologna*: Le Due Torri. Pili G., (2014), L'eterna *battaglia della mente – Scacchi e filosofia della guerra*, Bologna: Le Due Torri. Pili G., (2019), "Formazione di uno scacchista da giovane – Gli scacchi come modello della vita ordinaria," *Anemo*s, IX:33: 26-32.

[3] Grooten, H., (2009), *Chess Strategy for Club Players: The Road to Positional Advantage*, New in Chess. Grooten, H., (2016), *Attacking Chess for Club Players: Improve Your Skills to Overpower Your Opponents*, New in Chess. Grooten, H., (2019), *Understanding before Moving 2 – Queen's Gambit Structures*, Thinkers Publisher.

[4] Bilalic, Merim; McLeod, Peter; Gobet, Fernand; (2006), "Does chess need intelligence? A study with young chess players," *Intelligence* 35, pp. 457-470.

Charness, Neil, (1992), "The impact of chess research on cognitive science," *Psychological Research* 54, pp. 4-9. Vezzani S., (2011), *Scacchi e psicologia*, Brescia (Italy): Messaggerie Scacchistiche.

[5] Marrin S., Clemente J., (2005), "Improving Intelligence Analysis by Looking to the Medical Profession," *International Journal of Intelligence and CounterIntelligence* 18: 707-729. Marrin, S., Torres, E., (2017) "Improving how to think in intelligence analysis and medicine," *Intelligence and National Security* 32:5, 649-662. Fisher R., Johnston R., and Clement P., (2014), "Is Intelligence Analysis a Discipline?" in George and Bruce (eds.), *Analyzing Intelligence*, 2nd ed., 2014, Chapter 4. Tang, Jeffrey; (2017), "How do we know? What intelligence analysis can learn from the sociology of science," *Intelligence and National Security* 32.5: 663-674. Phythian, Mark, (2017), "Intelligence analysis and social science methods: Exploring the potential for and possible limits of mutual learning," *Intelligence and National Security* 32.5: 600-661.

[6] Wheaton, Kristan J., (2011), "Teaching Strategic Intelligence Through Games," *International Journal of intelligence and CounterIntelligence* 24:2, pp. 367-382. Lahneman, W.J., & Arcos, R. (eds.), (2014), *The art of intelligence: Simulations, exercises, and games*, Rowman & Littlefield. Lahneman, W.J., and Arcos, R., (2017), "Experiencing the art of intelligence: Using simulations/ gaming for teaching intelligence and developing analysis and production skills," *Intelligence and National Security* 32(7), pp. 972-985.

[7] Bruce, James B., and George, Roger, "Professionalizing Intelligence Analysis," *Journal of Strategic Security* 8, no. 3: 1-23.

[8] The professional revolution started with Robert J. Fischer and ended with Garry Kasparov.

[9] Especially since the EU approved chess as an approved optional path in primary and secondary schools

[10] Players such as Zuckertort and the great Alexander Alekhine were all Russians. In addition, Russia is the superpower in chess since the early explosion of chess during the second half of the 19th century and then as a superpower during the Cold War, as it is very well known even in the public media.

[11] Von Neumann, John, and Morgenstern, Oskar; (1947), *Theory of games and economic behavior*, Princeton, NJ: Princeton University Press, p. 113.

[12] Ciancarini, P., (2005), "Il computer gioca a scacchi," *Mondo Digitale*, Vol. 3, p. 9.

[13] Ciancarini, P., (2005), "Il computer gioca a scacchi," *Mondo Digitale*, Vol. 3, p. 9.

[14] According to Ciancarini, Chess allows 33^{80} games; that is a number of 120 digits.

[15] Hassabis, Silver, et al., (2018), "A general reinforcement learning algorithm that masters chess, shogi, and go through self-play," *Science* 362 (6419), 1140-1144.

[16] Indeed, if mathematically chess is inexhaustible, therefore reality is inexhaustible too as far as chess is a piece of reality. For an interesting philosophical analysis of the DeepBlue match, see Van Gelder, T., (1998), "Into the Deep Blue Yonder," *Quadrant* 41 (2-1), pp. 33-39.

[17] According to the Oxford Companion to Chess, a variation is: "Any alternative line of play, especially one that could occur in the opening phase of the game."

[18] Marrin, S., (2018), "Evaluating intelligence theories: current state of play," *Intelligence and National Security* 33:4, 479-490.

[19] Yari-Milo K., (2013), "In the Eye of the Beholder: How Leaders and Intelligence Communities Assess the Intentions of Adversaries," *International Security*, Vol. 38, Harvard University Press & MIT.

[20] Warner, M., (2002), "Wanted: A definition of 'intelligence'," *Studies in Intelligence* 46 (3): 15-22.

[21] As was stated by one of my commentators, Uberto Delprato, Candidate Master and practictioner in the field of intelligence: "There is a lot of work put in by GMs and their teams in identifying how to enter a specific structure with a different move-order than the usual ones. If I am not mistaken, these are named 'permutations,' emphasizing the parallel with math. When one player manages to do that, it is usually said that he 'outfoxed his/ her opponent'."

[22] It is sufficient to hear the precious analysis of a GM such as Benjamin Finegold to discover how many surprising moves happen in every game all the time. I suggest to watch this video for an impressive straightforward analysis: Thanksgiving Open Middlegames – GM Ben Finegold, https://www.youtube.com/ watch?v=Rf096-0V-Xk (accessed April 13, 2019).

[23] Goldman, J., (2005), *Words of Intelligence*, Lanham, MD: Scarecrow Press, p. 30.

[24] In the chess jargon, a piece is "hanging" if it is attacked by an opponent's piece and it is not defended appropriately.

[25] The safety of the king is something more nuanced, but it could be defined in function by how easy it is to attack it by the opponent's pieces. A secure king has many pieces and pawns near it. An insecure king has few pieces near it but has many opponent's pieces ready to attack it.

[26] This was done in the past also. All chess players buy books that report the chess games of other GMs and they study their own games, whose record is mandatory in the official tournaments.

[27] Fide Handbook, https://www.fide.com/fide/ handbook.html?id=39&view=category.

[28] Everything that can be computed is called "Turing-computable" because x is computable if and only if a Turing-machine can

compute it. This is not the place to define this point more precisely but it gives the idea that a computation is a finite set of data and transformation that an appropriately programmed Turing-machine can calculate. For a deeper analysis, see Palladino, Frixione (2011).

[29] Pherson, R., and Heuer, R., (2014), "Structured analytic techniques: A new approach to analysis," in Bruce and George (2014), *Analyzing Intelligence*, Washington, DC: Georgetown University Press, p. 232.

[30] Goldman, A., (1986), *Epistemology and Cognition*, Cambridge, MA: Harvard University Press.

[31] Amazing behaviors are part of all chess club folklore. I will not report examples I have experienced to prove this point, but it is interesting that everywhere chess players complain about the opponents when they lose. Then, typical excuses are "I don't feel very well today," "I worked hard all the week," "I was better all the game but finally…," etc.. An average chess player can report an entire list of complaints.

[32] Magnus Carlsen, the current world chess champion, jokingly said that losing was so harsh that he was determined to avoid it as much as possible.

[33] Great chess champions like Paul Morphy (1837-1884), Wilhelm Steinitz (1836-1900), Akiba Rubinstein (1880-1961), and Robert J. Fischer lose their reason. And they are not alone.

[34] For example, Hulnick, A.S., (1986), "The Intelligence producer – policy consumer linkage: A theoretical approach," *Intelligence and National Security* 1:2, 212-233.

[35] Vezzani S., (2011), Scacchi e psicologia, Brescia (Italy): Messaggerie Scacchistiche.

[36] Marrin S., and Clemente J., (2005), "Improving Intelligence Analysis by Looking to the Medical Profession," *International Journal of Intelligence and CounterIntelligence* 18: 707-729, Marrin, Stephen, and Torres, Efren, (2017) "Improving how to think in intelligence analysis and medicine," *Intelligence and National Security* 32:5, 649-662.

[37] Clausewitz, Carl V., (1832), *On War*, Princeton, NJ: Princeton University Press; Gill, P., and Phythian, M., (2016), "What Is Intelligence Studies?" *The International Journal of Intelligence, Security, and Public Affair*s 18 (1): 5-19, Gill, P., and Phythian, M., (2012), "Intelligence studies: Some thoughts on the state of the art," in *Annals of the University of Bucharest* 14: 5-17; Horn, E., (2003), "Knowing the Enemy: The Epistemology of Secret Intelligence," *Grey Room* 11, Treverton, G., and Gabbard, B., (2008), "Assessing the Tradecraft of Intelligence Analysis," Santa Monica, CA: RAND; Luttwak, E., (2009), *The Grand Strategy of the Byzantine Empire*, Cambridge, MA: Harvard University Press; Pili G., (2019), "Toward a Philosophical Definition of Intelligence," The *International Journal of Intelligence, Security, and Public Affairs* 21 (2): 162-190.

[38] The chess form is the form in which the chess player must write all the moves of the games. The chess form appears like a matrix with three colums: number of moves, white's moves, and black's moves. Just to give an example:

	White	Black
1	e4	c6
2	d4	d5
3	Nc3	dxe4
Etc.		

[39] This condition has a lot of interesting consequences for a logical conception of chess, which is not the topic here.

[40] Hassabis, Silver, et al. (2018) "A general reinforcement learning algorithm that masters chess, shogi, and go through self-play," *Science* 362 (6419), 1140-1144.

[41] To prove this point further, it is possible to set software able to create random positions without any evaluation as it is also possible to describe the sunset without giving any evaluation of it.

[42] Floridi, L., (2019), *The logic of information: A theory of philosophy as conceptual design*, Oxford, UK: Oxford University Press.

[43] AlphaZero is a different story, but for the moment itis the only chess engine of its kind and it is not important for the moment to consider it here.

[44] Stop position is the position where a calculation ends. In the majority of cases, the stop position is just the position judged sufficient to discriminate betweena good variation and a bad one. Of course, to be able to arrive at the right stop position is one of the most challenging activities involved in chess calculation, and many errors depend on having to stop the calculus too early. Indeed, the ability to reach the appropriate stop position is related to the quality of the player.

[45] Comesaña J., (2010), "Reliabilism," In Sven Bernecker and Duncan Pritchard (eds.), *The Routledge Companion to Epistemology*, London: Routledge, p. 3.

[46] Vezzani S., (2011), *Scacchi e psicologia*, Brescia (Italy): Messaggerie Scacchistiche.

[47] Heuer, R., (1999), *Psychology of Intelligence Analysis*, Center for the Study of Intelligence.

[48] I cannot go into the details of the study, but I explain this number eslewhere. Pili G., (2014), *L'eterna battaglia della mente – Scacchi e filosofia della guerra*, Bologna: Le Due Torri.

[49] I want to thank Mario and Claudio for their precious information.

[50] Ramesh, R.B., (2015), *Fundamental chess: Logical decision making*, Metropolitan Chess Publishing. Ramachandran Ramesh is a Grand Master and he was the trainer of Viswanathan Anand, world champion and one of the top ten players in the last thirty years.

Dr. Giangiuseppe Pili is a former lecturer in intelligence studies in the International Master's Program in Security, Intelligence, and Strategic Studies (IMSISS) at Dublin City University. He earned a PhD in philosophy and sciences of the mind with a thesis on individual and social epistemology. He is part of the organizational committee of the Intelligence Lab at Calabria University. He authored a book/monograph about the philosophy of war. He is co-author of the book Intelligence Studies *with Prof. Mario Caligiuri. Dr. Pili was a chess instructor and referee in the Italian Chess Federation. He is a 1698 ELO FIDE player, and he is the author of two books on chess and philosophy. He considers the relationship between chess and war in his main works.*

Defending Liberal Democracies Against Disinformation

by LTC (USA, Ret) Jacob P. Matthews

[Author's Note: The views expressed in this article are those of the author and are not an official policy or position of the National Defense University, the Department of Defense, or the U.S. Government.]

INTRODUCTION

"Reality exists in the human mind, and nowhere else."[1] George Orwell may not have envisioned cyberspace in his classic book *1984*, but he clearly understood that truth was the bedrock ingredient in a free and open society. By injecting doubt into the minds of its citizens, Orwell's dystopian government replaced truth with lies, ultimately eliminating hallmark characteristics of democracy: independent thought, critical thinking, and free will. Disinformation, the deliberate provision of false information to mislead, has been practiced for centuries, but maturation of the Internet, proliferation of global connectedness, and saturation of social media have combined to increase its potency exponentially. Social media is now a weapon of enormous capability, and its malicious use poses an existential threat to liberal democracies unprepared to defend themselves. Disinformation campaigns use social media against the United States, threatening its vital national interests and its democratic form of government by sowing seeds of discord, promoting instability, and weakening national resolve. To address this problem, the U.S. must develop and execute a strategy to defend its way of life, detect disinformation, and attack disinformation at its source to protect national interests and preserve the international order.

INTERNATIONAL CONTEXT

The formulation of sound strategies begins with a clear understanding of the strategic situation. Major international drivers include significant technological advances in communication that increasingly connect people in a 24/7 world; globalization that weakens state sovereignty and traditional patriotism; and malicious use of social media, particularly by the Russian Federation, as a weapon to attack democracies and the current international order.

In their book *LikeWar: The Weaponization of Social Media*, P.W. Singer and Emerson T. Brooking claim that the Internet is the preeminent medium of global communication, commerce, and politics.[2] They go on to note that social media have allowed the Internet to surpass the telegraph, telephone, radio, and television, providing global and instantaneous communication in an ultimate combination of connection and mass transmission.[3] More than 75 percent of people in the U.S. are active on social media.[4] These numbers are similar in other developed nations and are rapidly increasing in the developing world.

This profound connectedness promotes globalization with its universal appeal to join hands across the borders that define the current international order. The growing interdependence of culture, economy, and technology is blurring the traditional national boundaries that have long defined state sovereignty, and many are rethinking their allegiances along tribal, ideological, and religious lines.[5] On the global stage, nationalism and patriotism are still powerful forces, but are now competing against globalism.

The Internet gives wings to the Russian disinformation engine that formerly relied upon less effective media, such as newspapers, radio, and television. Russian disinformation can now reach the masses and manipulate emotions to fan the flames.[6] Now able to communicate instantly, anonymously and expansively, Russia used the 2016 U.S. presidential election to demonstrate its capability to mislead. Its "…human trolls, backed by tens of thousands of automated accounts, infiltrated…US political dialogue…steered discussion, sowed doubt, and obfuscated truth, launching the most politically consequential information attack in history."[7] Russia similarly worked to influence the 2016 Brexit vote in the United Kingdom and the 2017 French national elections.[8] Transmission is only half of the communication process; reception is the other essential ingredient for any message to accomplish its purpose. Civilizations are built upon the innate need of human beings to congregate. Contrary to the saying "opposites attract," humans are social creatures mostly attracted to like-minded others.[9] Confirmation bias helps explain why we tend to interpret, favor, or remember information that aligns with what we already believe. These behavioral characteristics

offer an open door for Russian disinformation specialists to spread myriad mistruths to shape popular opinion, including those of U.S. citizens.

DOMESTIC CONTEXT

Major domestic drivers include inadequate popular recognition of disinformation, diminished trust between U.S. citizens and their government, insufficient trust between Big Technology (e.g., Google, Facebook, Apple, and Twitter) and the U.S. government (USG), and a fragmented USG response across multiple agencies. The average U.S. citizen consumes data at a high rate and without significant regard for validity.[10] In previous generations, information arrived by means of trusted couriers. Legacy newspaper outlets and federally-regulated radio and television broadcasts largely delivered objective truth from legitimate sources. However, the Internet changed this paradigm by exponentially increasing news sources while decreasing controls governing their content. Digital Age information consumers are not equipped to identify unreliable sources, nor are they trained to distinguish truth from lies.

Historically, U.S. citizens have been hesitant to place their trust in the government, even more so now due to Edward Snowden's theft and release of classified National Security Agency (NSA) files in 2013.[11] Many claimed this disclosure of NSA policy and tactics demonstrated a prioritization of security over rights of privacy. The increase of popular distrust in this "post-Snowden" world makes it more difficult for the USG to gain and maintain support for its policies.

Digital Age information consumers are not equipped to identify unreliable sources, nor are they trained to distinguish truth from lies.

The USG is similarly estranged from Big Technology. These firms own 100 percent of U.S. social media platforms, have occasionally identified as global citizens, and have not been averse to criticizing publicly USG policies and actions. Apple elevated privacy rights over national security by refusing to comply with an FBI request to unlock an iPhone belonging to one of the perpetrators of the December 2015 San Bernardino terrorist attacks.[12] In spite of Big Technology's American roots, the collaboration to counter disinformation that the USG is seeking with these firms is anything but assured.

The USG has distributed the responsibility to counter disinformation across multiple agencies. While the Department of Homeland Security (DHS) has lead agency responsibility, capabilities also exist within the Departments of Defense (DoD), State (DOS), and Justice (DOJ). This arrangement invites diminished performance due to inefficient intelligence sharing, increased cost, incoherent actions, and bureaucratic delays.

NATIONAL INTERESTS

Disinformation affects U.S. national interests, including the goals of life, liberty, and the pursuit of happiness. The 2017 *National Security Strategy* lists these interests as follows: Protect the American People, the Homeland, and the American Way of Life (Life); Promote American Prosperity (the Pursuit of Happiness); Preserve Peace Through Strength (Liberty); and Advance American Influence (Values).[13] The September 2018 U.S. *National Cyber Strategy* states that "adversaries use cyber tools to undermine our economy and democracy, steal our intellectual property, and sow discord in our democratic processes."[14] Clausewitz's "Trinity" establishes a critical link between the people and their government.[15] Effective disinformation can weaken this link, eroding stability and unity. Although this article focuses on malicious activity originating from foreign sources, disinformation also appears in a domestic variety. Regardless, a weakened democratic foundation undermines each national interest, diminishes the appeal of American values, and reduces U.S. influence around the world.

THREAT

The use of weaponized social media to spread disinformation is a specific threat to U.S. democracy and the current international order. Democratic forms of government are susceptible to disinformation and require cultivation and protection, as Benjamin Franklin was aware. When asked what type of government had been decided upon at the end of the Constitutional Congress of 1787, Franklin replied, "A republic, if you can keep it."[16] Democracies derive from consent, not coercion, and are fragile constructs, resting upon popular support. Weapons that insidiously undermine popular consent may be more dangerous than overt conventional means of attack. Disinformation is insidious because it is generally comprised of both truth and lies. Further, it is often passed along by those whom we know and trust. Russia's Internet Research Agency (IRA) specializes in disinformation, employing well-educated, creative individuals (often referred to as "trolls") to open multiple false accounts and post misleading articles on social media platforms. If these articles prove to be popular, as measured by "likes" or "retweets," then automated accounts (known as "bots") may reinforce the trend, increasing article appeal in an escalating cycle. Initially driven by human behavior, the bots now become the driver to influence human behavior further. Popular posts

may go "viral," receiving a significant amount of attention in a short period of time, as they are spread vigorously across the Internet.[17] Internet users often base their assessments of veracity upon virality, as they fall prey to these malicious disinformation peddlers.

OPPORTUNITIES

Good strategies also seek to take advantage of opportunities. By identifying and eliminating deceptive practices, the U.S. will have an opportunity to promote its values to a global audience and to increase its legitimacy. The benefits of democracy will be displayed as the U.S. openly practices its form of government and invites comparison to the lies and deceit inherent in authoritarian or autocratic regimes. Another opportunity arises through U.S. collaboration with like-minded nations to identify healthy and accepted practices that will, over time, become norms for acceptable behavior on social media. Although not discussed in detail in this article, these norms will ultimately enable increased law enforcement efforts to reinforce proper, and deter improper, behavior.

CONSTRAINTS

Clausewitz also noted friction's effect on any plan of action.[18] Four friction-producing elements are likely to constrain this proposed strategy. The first is the parochial interest of each USG agency that shares responsibility for countering disinformation. Collaboration will be difficult since each will likely be reticent to give up any of its autonomy. Agencies perceived as successful are likely to receive additional funds and staff to accomplish even more. This acts as a disincentive to work together selflessly and promotes a competition in which self-interest wins out over cooperation and teamwork.

The second element is the unbounded geography of the Internet. Cyberspace exists apart from national borders, crossing into multiple jurisdictions and presenting specific challenges in the determination of attribution and intent. This makes legislation difficult, and efforts to prosecute are complicated and time-consuming. Still, in 2015 the European Union (EU) began to unify online policy and practice to counter disinformation. EU progress includes a task force to catalogue, analyze, and raise awareness of Russian disinformation; a fusion cell to analyze hybrid threats against EU institutions; and a European approach for promoting a more transparent and trustworthy online environment.[19] In December 2018, the EU presented an Action Plan against disinformation and also created a Rapid Alert System to increase real-time disinformation awareness. Further, the EU General Data Protection Regulation (GDPR), a law designed to balance individual privacy rights against the collection of personal data by Internet advertisers, may inadvertently serve as a means to counter disinformation.[20] Agents of disinformation often rely upon collected personal data to focus the messages designed to provoke and divide. Without easy access to such data, disinformation specialists may struggle to be effective.

Democratic societies have vulnerabilities, and the third element arises from the need to preserve freedom of speech. Not all free speech will be truthful, but it cannot be classified as disinformation unless it is offered with the intent to deceive. Any effort to identify disinformation must be careful to make this critical distinction or risk blowback from citizens being denied their First Amendment rights and the subsequent loss of trust in the USG that would impede efforts to combat disinformation.

The final element is the need to ensure privacy. This Fourth Amendment guarantee must be carefully balanced against the needs of the government to ensure the security of its citizens. This element is further complicated by the lack of borders in cyberspace. One U.S. court ruled that data residing on servers outside the country's borders may be brought back for use in a trial. In a separate case, a different U.S. court ruled that such information may not be retrieved as U.S. warrants have no jurisdictional authority outside the country.[21] In spite of this confusion, few topics are as sensitive to U.S. citizens, and blowback over a perceived loss of privacy must be avoided to maintain trust and preserve the federal government's popular mandate to counter disinformation.

ASSUMPTIONS

The success of any strategy depends upon key assumptions that, if not realized, may cause the strategy to fail. This proposed strategy features three key assumptions.

First, USG leadership must portray an honorable, trustworthy, and non-partisan image while promoting a credible, moral narrative to ensure its legitimacy and generate consensus among all actors engaging in the effort to counter disinformation. A government perceived to be in opposition to these qualities will undermine its own freedom to act.

Second, Big Technology will work with the USG, setting aside its identification as global citizens to support U.S. democracy and the current international order. Big Technology firms have been hesitant to collaborate with anyone whose values seem contrary to their own. USG leaders must identify common interests, and preservation of the current international order to help these firms maximize profit may be a good starting point.

Third, U.S. citizens will accept the challenge of balancing privacy and security and will support USG efforts to provide both. Persistent promotion of a narrative that frames this dilemma as a pursuit of popular welfare is essential for success.

One final assumption is offered that is not essential for the strategy to succeed. It is possible to establish a unified USG interagency team for enabling effective collaboration to counter disinformation. This team will pursue specific objectives by orchestrating this strategy's ways and means.

GUIDING POLICY AND POLITICAL AIM

The guiding policy for this strategy will be to treat disinformation like a virus, containing its spread and reducing its effects through the pursuit of objectives to educate, identify, and eradicate. Accomplishing these objectives will achieve the political aim of a better-informed citizenry using an open, reliable, and secure Internet to sustain U.S. democratic government legitimacy and preserve the international order.[22]

OBJECTIVES, WAYS, AND MEANS

In treating any virus, physicians must keep up with evolving strains. It is likely that the rapid pace of technological advancement will continue over time and that methods to conduct and counter disinformation will change too. Accordingly, constant assessment and adjustment will be required to develop and execute successful strategies to counter disinformation. In this evolving and dynamic environment, the development of perfect strategic solutions will prove elusive. Nevertheless, effective strategies can be created, and to counter disinformation successfully in this strategic environment U.S. strategy must pursue four objectives. First, it must defend against disinformation to reduce its effects (*Education*). Second, it must detect disinformation (*Identification*). Third, it must attack sources of disinformation to reduce its practice (*Eradication*). Fourth, it must effectively coordinate a "whole-of-society" effort (*Orchestration*). Each of these independent objectives should be pursued immediately and simultaneously. The most important objective for strategy success is education, which is empowered by identification. Eradication will reduce the need for either education or identification but is not likely to be wholly successful. Finally, orchestration improves strategy efficiency and effectiveness but is not essential for success.

Objective One

The first objective, to defend against disinformation, features two sub-objectives, each making use of the information instrument of power. The first is to raise awareness of disinformation practices. As previously noted, the average consumer of digital information needs improved discernment skills. Media literacy campaigns, to include simple public service announcements delivered by respected and trusted personalities, could increase awareness and promote understanding of the dangers of disinformation. This short-term approach would target people of all ages, but the most effective means would likely be a long-term investment in the next generation. The Department of Education could play a key role here as an early adopter and implementer of public school curricula to promote media literacy and encourage responsible online citizenship. The USG appears to recognize this possibility by assigning responsibilities to the Secretary of Education in the workforce development portion of Executive Order 13800.[23] Both short- and long-term approaches appear necessary as this challenge is likely to persist and adapt over time. Basic numbers for participation in these campaigns, as well as for completing courses in school, would likely serve as the best metrics of progress.

The most important objective for strategy success is education, which is empowered by identification.

The second sub-objective is to develop a legitimate and persistent narrative. Joseph Nye has claimed that in today's connected world it is often the best story that wins.[24] Narratives directly affect legitimacy and its derivative freedom to act. The U.S. and its like-minded partners must pursue the moral high ground throughout their effort to counter disinformation. Narrative warfare can be more powerful than information warfare.[25] The immediate story to be told must be one that champions human dignity, women's rights, freedom, security, and peace. Democracies offer all of these qualities in stark contrast to the bleak landscapes of authoritarian and autocratic societies. Telling this story (a "narrative of liberty" but henceforth referred to as "narrative") will allow individuals to compare it to the narrative of their own leaders. Multiple media must be employed since some regimes censor the online content made available to their people. Voice of America is still a useful tool, and targeting of expatriate populations which can relay information to friends and family still living under repressive regimes could also prove useful. Ideology remains a powerful force in a modern world; truth and freedom continue to attract multitudes, compelling them to abandon lies and bondage. Promoting the narrative over the long haul will strengthen those promoting democratic values while weakening the legitimacy and resolve of those opposing the current world order.

Metrics to show progress of this action will be more elusive with opinion polls likely being the most effective method available.

Objective Two

The second objective, to detect disinformation, features two sub-objectives, each using the information instrument of power. Each sub-objective would also generate significant data that could be used as metrics for progress. The first is to partner with Big Technology to assess online content. This effort may also make use of the economic instrument of power, since financial inducements, persuasion based on a common narrative, or coercion (a last resort) through financial disincentives may be required to gain Big Technology's support. These companies answer to their shareholders; profit is king. Online information may be factual, opinionated, dishonest, or propagandist in nature, and only a small percentage of it may be categorized as disinformation. What does pass as disinformation must be considered as inappropriate content and treated in accordance with methods described in the next paragraph. Still, making such determinations takes time. Methods used to assess articles usually involve a review of the author, purpose, objectivity, accuracy, currency, and credibility.[26] The sheer volume of content on the Internet and the amount of new material added daily means that numerous assessments can be accomplished only by sophisticated computer programs. Social media platform owners must be persuaded to support this effort by committing resources, but the development of the required programming will be challenging because of diverging world views within a democracy. For example, today's U.S. political landscape features strong partisanship. Republicans who believe they are completely objective may still draw conclusions on a given topic that are diametrically opposed to equally objective Democrats as this process can be as much about the facts as the interpretation of those facts.[27] Any tool developed must be able to provide assessments based upon more than one point of view. Widely divergent scores from both sides of the political divide will invite further investigation, whereas similar scores will reflect a bipartisan consensus and strong confidence in the determination. Taking another step back, it will also be important to ensure the objectivity of assessment tool developers to avoid reflection of programmer bias in the tool. Private, independent, or non-profit organizations may be best suited to provide such services. Unlike Big Technology, these organizations may be more easily persuaded to act in accordance with the shared values of the narrative. The USG should continue to support the Defense Advanced Research Projects Agency (DARPA) in the development of next-generation assessment tools. DARPA is uniquely positioned to work objectively and effectively on this task and could provide mid- to long-range solutions to lessen dependence upon the private sector.

The second sub-objective is to partner with Big Technology to remove fraudulent accounts and inappropriate content. Big Technology has already begun this work as Facebook removed 2.8 billion fraudulent accounts from its platform between October 2017 and September 2018.[28] Impetus for this effort seems to be a combination of public shaming by media outlets such as *The New York Times*, Congressional scrutiny, and the threat of the EU taking legal and punitive action against the company. Given this behavioral trend, the USG may not need to invest significant effort to ensure its continuation over both the short and long term. However, it may need to begin work on legislation to enable more informed decision-making by these companies. Mark Zuckerberg's recent op-ed called for governments to help establish rules to regulate the Internet. In particular, Zuckerberg identified harmful content and election integrity as two focus areas.[29] His plea followed Facebook's removal in April through September 2018 of 90 percent of all content related to "…hate speech, terrorist propaganda, and violence and graphic content."[30] While encouraging, the size of Facebook's customer base means that the 10 percent of content that remains is still significant. More effort is required to approach 100 percent removal and to recognize that significant volumes of inappropriate content are added to the platform every minute. As previously discussed as a constraint, the identification of disinformation requires a determination of intent to deceive. Without such intent, the speech is merely untruthful and, aside from libel or slander, protected by the First Amendment, perhaps the most important democratic right, and one that must not be compromised in the effort to counter disinformation. Those entrusted with the responsibility to determine whether specific content is appropriate must not deprive others of their constitutional rights and must work to ensure that the USG does not exert control over this platform in a way that moves the country in a more authoritarian direction.

Objective Three

The third objective, to attack the sources of disinformation, features two sub-objectives. The first makes use of the military instrument of power by enabling DOD assets to counter threats at their source. Threats to the U.S. in cyberspace have been evident for many years, but the government has wrestled with how best to respond. Presidential Decision Directive 20 (PPD 20), signed in October 2012, provided policy and approval processes for offensive and defensive operations in cyberspace.[31] Nevertheless, the directive retained most approval authorities at the Presidential level, requiring operational requests to obtain National Security Council blessing. This precluded the U.S. from timely or effective response against malicious cyberspace actors. National Security Presidential Memorandum 13 (NSPM 13), signed in September 2018, improved U.S. capability to respond by delegating approval

authority to the Secretary of Defense,[32] enabling DOD assets to conduct operations rapidly to defend U.S. networks and attack malicious actors. NSPM 13 cites influence operations on its list of malicious activities in providing clear and effective policy to conduct persistent cyberspace operations. The U.S. possesses sufficient capability to act under NSPM 13 as even cursory reviews of U.S. Cyber Command (CYBERCOM) will attest. A recent example of CYBERCOM success was the suppression of the IRA's effort to disrupt the U.S. 2018 mid-term elections. CYBERCOM blocked IRA access to the Internet during that time period.[33] Offensive actions for this short- and long-term approach must remain measured and proportional, however, to avoid possible escalation that could lead to war. Cyberspace operations have not yet escalated to a kinetic conflict, but it is possible that a deadly cyberattack on U.S. critical infrastructure would be the first. One final note related to this action pertains to the ability to "name and shame" those who practice disinformation. Effectively practiced, this will reinforce the narrative that preserves U.S. legitimacy and maintains the consensus of like-minded nations. It could also serve as a metric to identify progress, since it would not be wise to publicize the more detailed measurements of CYBERCOM activity and success.

The second sub-objective makes use of both the diplomatic and information instruments of power by ensuring that law enforcement efforts to prosecute criminal activity do not violate First Amendment rights or feed authoritarianism. Proper use of the Internet over time will create the customs and expectations that will one day serve as cyberspace norms. This long-term effect does not assist current law enforcement efforts as norms, unlike laws, are not legally enforceable. As noted previously, the EU GDPR may indirectly help counter disinformation, but it does not provide a direct enforcement means. Meanwhile, other democratic nations have enacted or considered legislation to deter malicious actors.[34] Germany passed a law in 2017 requiring digital platforms to delete "obvious" hate speech and misinformation within 24 hours, or face fines up to $57 million. Yet, it is difficult to define what is "obvious," and classification of hate speech is equally challenging. Such broad language could have the unintended effect of forcing extreme censorship by companies seeking to avoid significant fines. The Philippines considered legislation to impose 5-year prison terms on anyone who published or distributed information to cause panic, division, chaos, violence, and hate. The proposal offered broad definitions for social networks and disinformation, allowing critics to point out that it would limit free expression and potentially criminalize investigative journalism.[35] Legislation proposed to counter disinformation must be thoroughly reviewed to ensure preservation of free speech. Censorship has long been a feature of authoritarian regimes and must not be given a foothold in democratic governments. Any efforts to pass laws to punish purveyors of disinformation must be made transparently, within the context of the narrative, and with the full awareness of the citizens whose First Amendment rights could be greatly affected.

Objective Four

The fourth objective makes use of the diplomatic instrument of power to coordinate effectively a "whole-of-society" effort through optimal orchestration of the efforts of USG agencies and Big Technology. The July 2018 U.S. Attorney General's Report of the Cyber Digital Task Force identifies the danger that disinformation poses to democracies and recognizes the seeds of discord it seeks to sow. It further confirms that "combating foreign influence operations requires a whole-of-society approach that relies on coordinated actions by federal, state, and local government agencies; support from potential victims and the private sector; and the active engagement of an informed public."[36] This comprehensive approach is essential, given the persistent and pervasive nature of the challenge and the potential impact of proposed remedies upon all citizens. It also implies the magnitude of the challenge to develop a single, effective organization to counter disinformation, which may explain the USG's fragmented approach. The U.S. should consider establishing a joint interagency task force (JIATF) to meet this need. Previous efforts to do so have not yet proven successful. In late 2018, the National Protection and Programs Directorate (NPPD) was established within DHS and assigned the mission of coordinating with local, state, tribal, and territorial governments on cyber and physical security initiatives while working to reduce threats to critical infrastructure.[37] While multiple U.S. government agencies share cybersecurity responsibilities, the NPPD has the authority to lead the overall effort. However, the Directorate is not an optimal solution since its focus is on terrorist attacks, catastrophic events, and natural disasters, not the persistent and pervasive threat that disinformation poses.

In 2016 the DOS Global Engagement Center (GEC) was established and assigned the mission to "lead, synchronize, and coordinate the efforts of the Federal Government to counter disinformation efforts aimed at undermining US national security interests."[38] The GEC, however, underfunded and understaffed to date, has been forced to rely upon the DOS to provide both.[39] Lacking a clear mandate to pursue its mission, the GEC does not appear to be the organization to orchestrate this whole-of-society approach either. A JIATF, established by Presidential Executive Order, comprised of department and agency senior leaders, and reporting to the National Security Council, would possess the mandate and capacity to orchestrate the whole-of-society effort to counter disinformation effectively. Senior leaders would serve exclusively on the JIATF, would

be granted authority to make decisions for their respective organizations (DHS, DOJ, DOD, DOS, and others from the Intelligence Community), and would be career service employees (not political appointees) to ensure continuity across changes in administration. The JIATF would not affect authorities or reverse the expeditious nature of NSPM 13, but would work at a more strategic level, eliminating redundant capabilities and enhancing coordination of efforts otherwise left to chance when agencies are unaware of one another's plans. Tasking a single organization, such as DHS, as the lead creates competition across all affected agencies as they seek to support the mission and preserve their status. Recent experience has demonstrated that a single, Cabinet-level official within the administration does not always persuade or induce agencies to work together effectively. Creation of a single organization similar to the Centers for Disease Control and Prevention from all agency components currently assigned cyber missions is unrealistic. Agencies would dig in to preserve their capabilities, and the cost to make this change would likely be prohibitive even if agencies were to support the plan fully. A JIATF seems to offer the best opportunity for centralized strategy and policy formulation, along with decentralized execution by existing organizations. Finally, a JIATF would be well positioned to seek Big Technology's support. A newly-created JIATF would have no history of disagreements with the private sector. Relying upon the narrative, the JIATF could work from a platform promoting the peaceful, open, and stable order best suited for Big Technology to continue its pursuit of innovation and profit. If the concept proves successful, then legislation could transform this short-term approach into a long-term solution by making the JIATF permanent.

COSTS AND RISKS

Sound strategies must minimize cost and risk. Costs to accomplish Objective 1 include the funding to raise awareness through media literacy campaigns and new curricula developed and implemented by the Department of Education. The cost to develop and persistently promote the narrative must also be considered. Costs to accomplish Objective 2 include funds required to induce Big Technology to partner with the USG, should the narrative prove insufficient. Additional costs will be required to develop the tools used to assess Internet content (if not fully covered by Big Technology) and those to implement and assess metrics for measuring progress in countering disinformation. Finally, if the decision is made to increase DARPA funding to develop additional capabilities, then these costs must also be considered. Costs to accomplish Objective 3 include the funding for CYBERCOM force structure and equipment to counter disinformation. Existing force structure levels may be increased as the size and persistence of the threat is fully realized. Finally, costs for Objective 4 include that to establish the JIATF and to increase the capabilities of the GEC, if it is determined this organization adds value to the whole-of-society approach.

Some of the risks associated with this strategy have already been identified during the discussion of specific objectives. There are several risks "to" the strategy. Risk for Objective 1 includes the inability to develop an effective narrative or the inability to deliver any narrative due to a lack of confidence and trust in U.S. leadership. Lack of domestic support will undermine U.S. legitimacy and the freedom to act to counter disinformation. Risks for Objective 2 derive from the lack of support from Big Technology and the inability to create tools to assess content. Risks for Objective 4 include the potential that JIATF membership and continuity could be adversely affected by changes in administration and the possibility that an insufficient mandate could undermine the task force's ability to orchestrate the whole-of-society effort effectively. There are also several risks "from" the strategy. Risks for Objective 2 include blowback from citizens who perceive a loss of First Amendment rights, leading to a loss of domestic support for countering disinformation. Another risk for Objective 2 is the potential for the USG to use the tools to further self-serving, identity politics or to increase authoritarian behaviors that favor the administration over the populace. Risks for Objective 3 include the potential for escalation to kinetic war as well as overreach by law enforcement organizations that would generate blowback from citizens over the loss (real or perceived) of First or Fourth Amendment rights. Finally, risk for Objective 4 could be the loss in trust for agencies previously assigned to lead the effort against these threats (e.g., DHS NPPD and DOS GEC).

VIABILITY TESTS

Cost and risk are important but do not provide sufficient predictive measures for successful strategy implementation. Viability factors must be also considered. This strategy is suitable since it protects U.S. national interests, provided that First and Fourth Amendment rights are preserved throughout. Further, the promotion of the narrative will strengthen U.S. legitimacy, providing the nation with greater influence to help preserve the current international order. It also is mostly feasible since it is sufficiently focused to accomplish the goal of an open, reliable Internet and increased U.S. legitimacy. The preservation of the current international order will also be facilitated by this strategy, but other factors may negate the contributions made by this strategy. Sufficient means exist to accomplish this strategy, as long as key actors across the USG and Big Technology support the effort. This strategy is desirable since potential benefits outweigh costs. Again, care must be taken to preserve First and Fourth Amendment rights, but cost is otherwise measured in an amount that

represents relatively small increases in the annual federal budget. The benefits of a well-informed society fully participating in democratic processes can realistically be anticipated. It is an acceptable strategy given that the political aim it seeks to achieve is fully aligned with U.S. values and interests. It is also acceptable to a large number of nations comprising the current international order since it strengthens the free and open societies they model. Ultimately, the appeal to freedom, liberty, security, and truth will be embraced by a majority of U.S. citizens who provide the mandate for the government to act in countering disinformation. Finally, this strategy is sustainable since overall costs are low, the political will of U.S. citizens will be sufficiently high, and the means required for its success are available. Once again, it must be noted that a key for continuing sustainability will be the preservation of First and Fourth Amendment rights. As with any strategy, popular support is essential.

STRATEGIC LEADERSHIP CHALLENGES

Strategic leadership will greatly affect this strategy's success. Strong Presidential leadership is the most significant challenge and is essential to convey the national narrative and unite the nation behind the effort to counter disinformation. Further, the President will set the tone for gaining the support of Big Technology and uniting government agencies in a whole-of-society approach. The challenge can be mitigated with substantial levels of trust and confidence in the President; these qualities will be in demand to safely navigate around the First and Fourth Amendment whirlpools. Overall, the USG must operate with an openness and transparency not in style during the years revealed by Snowden's crime. Finally, the President must address the challenges of globalization and take advantage of its opportunities while preserving U.S. national interests and strong relationships with like-minded allies. Such leadership is vital in both the near term and long term. It will always be in demand.

CONCLUSION

Disinformation endangers democracies, and this strategy recommends treating disinformation like a virus. Ironically, Russia's disinformation campaign against the U.S. during the 2016 national election may have played the role of vaccine to the virus it sought to spread. Many Americans have now awakened to the information war waged against us, and the first step toward victory is recognizing that there is a war to fight. The weapons of this war are not kinetic. Instead, words and images serve as implements of information to attack U.S. democracy and the current world order. The U.S. must remember its Constitutional heritage and renew its commitment to democratic rights and freedoms. The narrative of individual liberty must inform each instrument of power wielded in this long-term fight to establish truth and secure trust. The light that has attracted so many to the U.S. over the centuries must continue to shine brightly upon the construct of "We the people…" if we are to avert the dystopia that Orwell only imagined.

NOTES

[1] George Orwell, *1984*, accessed November 7, 2018, https://ebooks.adelaide.edu.au/o/orwell/george/079n/chapter3.2.html.
[2] P.W. Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media* (New York: Houghton, Mifflin, Harcourt Publishing Company, 2018), 21.
[3] Singer and Booking, *LikeWar*, 22.
[4] Statista: The Statistics Portal, "Percentage of US Population with a Social Network Profile 2008 to 2018," accessed November 16, 2018, https://www.statista.com/statistics/273476/percentage-of-us-population-with-a-social-network-profile/.
[5] Amy Chua, "Tribal World," *Foreign Affairs*, July/August 2018, accessed April 11, 2019, https://www.foreignaffairs.com/articles/world/2018-06-14/tribal-world.
[6] Singer and Brooking, *LikeWar*, 161-162.
[7] Singer and Brooking, *LikeWar*, 16.
[8] Ninon Bulckaert, "How France successfully countered Russian interference during the presidential election," *Euractiv*, July 17, 2018, accessed April 8, 2019, https://www.euractiv.com/section/elections/news/how-france-successfully-countered-russian-interference-during-the-presidential-election/.
[9] Brendan M. Lynch, "Study Finds Our Desire for 'Like-Minded Others' Is Hard-Wired," The University of Kansas, *KU Today*, February 23, 2016, accessed November 15, 2018, https://news.ku.edu/2016/02/19/new-study-finds-our-desire-minded-others-hard-wired-controls-friend-and-partner.
[10] Katharine Viner, "How technology disrupted the truth," *The Guardian*, July 12, 2016, accessed April 10, 2019, https://www.theguardian.com/media/2016/jul/12/how-technology-disrupted-the-truth.
[11] Paul Szoldra, "This is everything Edward Snowden revealed in one year of unprecedented top-secret leaks," *Business Insider*, September 16, 2016, accessed April 11, 2019, https://www.businessinsider.com/snowden-leaks-timeline-2016-9.
[12] Ellen Nakashima, "US wants Apple to help unlock iphone used by San Bernardino shooter," *The Washington Post*, February 17, 2016, accessed April 11, 2019, https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html?utm_term=.e04fda64ba75.
[13] Donald J. Trump, *National Security Strategy of the United States of America* (Washington, DC: The White House, December 2017).
[14] Donald J. Trump, *National Cyber Strategy of the United States of America* (Washington, DC, The White House, September 2018).
[15] Craig Beutel, "Disruption in the Trinity," *The Strategy Bridge*, October 31, 2017, accessed April 10, 2019,

https://thestrategybridge.org/the-bridge/2017/10/31/disruption-in-the-trinity.
[16] "Benjamin Franklin: Quotes by This Author," *Our Republic*, accessed November 15, 2018, http://www.ourrepubliconline.com/Author/21.
[17] Singer and Brooking, *LikeWar*, 139.
[18] General Carl von Clausewitz, *On War*, accessed April 10, 2019, https://www.gutenberg.org/files/1946/1946-h/1946-h.htm#link2HCH0007.
[19] "Countering Disinformation," *European Union External Action*, March 11, 2019, accessed April 11, 2019, https://eeas.europa.eu/topics/countering-disinformation/59411/countering-disinformation_en.
[20] Karen Kornbluh, "Could Europe's New Data Protection Regulation Curb Online Disinformation?" *Council on Foreign Relations*, February 20, 2018, accessed April 10, 2019, https://www.cfr.org/blog/could-europes-new-data-protection-regulation-curb-online-disinformation.
[21] Lucy Bertino, "Courts Continue to Split on the Fourth Amendment in Cyberspace," *North Carolina Journal of Law & Technology*, February 22, 2017, accessed April 10, 2019, http://ncjolt.org/circuit-split-4th-amendment-cyberspace/.
[22] Trump, *National Cyber Strategy*.
[23] Executive Order No. 13800, 82 FR (22391-22397), *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, May 11, 2017, accessed April 10, 2019, https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.
[24] Joseph S. Nye, Jr., "Think Again: Soft Power," *Foreign Policy*, February 23, 2006, accessed April 11, 2019, https://foreignpolicy.com/2006/02/23/think-again-soft-power/.
[25] David Wemer, "How to Kill a Disinformation Narrative: Make it a Whodunit," *Atlantic Council*, March 8, 2019, accessed April 11, 2019 https://www.atlanticcouncil.org/blogs/new-atlanticist/how-to-kill-a-disinformation-narrative-make-it-a-whodunit.
[26] "Evaluating Internet Resources," *Georgetown University Library*, accessed April 11, 2019, https://www.library.georgetown.edu/tutorials/research-guides/evaluating-internet-content.
[27] Richard Andres, email message to author, April 8, 2019.
[28] Nathan Ingraham, "Facebook removed over 1.5 billion fake accounts in the last six months," *Engadget*, November 15, 2018, accessed April 11, 2019, https://www.engadget.com/2018/11/15/facebook-transparency-report-fake-account-removal/.
[29] Emma Snaith, "Mark Zuckerberg calls for more government regulation of internet: 'We have too much power'," *Independent*, March 31, 2019, accessed April 11, 2019, https://www.independent.co.uk/news/world/americas/mark-zuckerberg-facebook-regulation-internet-government-washington-post-a8847701.html.
[30] Nathan Ingraham, "Facebook removed over 1.5 billion."
[31] Chris Bing, "Trump administration may throw out the approval process for cyberwarfare," *Cyberscoop*, May 2, 2018, accessed April 10, 2019, https://www.cyberscoop.com/ppd-20-white-house-national-security-council-cyber-warfare-tactics/.
[32] Morgan Wright, "New, more nimble cyberstrategy has learned from past mistakes," *The Hill*, September 27, 2018, accessed April 12, 2019, https://thehill.com/opinion/cybersecurity/408527-new-more-nimble-cyberstrategy-has-learned-from-past-mistakes.
[33] Ellen Nakashima, "The U.S. military disrupted the internet access of Russian troll factory on the day of 2018 midterms," February 26, 2019, accessed April 12, 2019, https://www.chicagotribune.com/news/nationworld/politics/ct-russian-troll-factory-midterms-20190226-story.html.
[34] Darrell M. West, "How to combat fake news and disinformation," Brookings, December 18, 2017, accessed April 12, 2019, https://www.brookings.edu/research/how-to-combat-fake-news-and-disinformation/.
[35] West, "How to combat fake news."
[36] Rod J. Rosenstein, *Report of the Attorney General's Cyber Digital Task Force* (Washington, DC: The Justice Department, July 2018), 8.
[37] Jessica Davis, "Homeland Security Gains Cybersecurity Agency with New Legislation," *Health IT Security*, November 15, 2018, accessed April 12, 2019, https://healthitsecurity.com/news/homeland-security-gains-cybersecurity-agency-with-new-legislation.
[38] "Global Engagement Center," U.S. Department of State, accessed April 10, 2019, https://www.state.gov/r/gec/.
[39] Deirdre Shesgreen, "Trump's State Department lacks money, clear mandate to fight Russian disinformation, 'fake news'," *USA Today*, September 21, 2018, accessed April 12, 2019, https://toinformistoinfluence.com/2018/09/23/global-engagement-center-lacks-financing-and-mandate/.

Jacob (Jack) P. Matthews is a Department of the Army Civilian and 2019 graduate of the National War College. He retired from the U.S. Army as a Lieutenant Colonel after serving on four continents, deploying twice, and commanding at the platoon, company, and battalion levels. Following his time in uniform, he served in leadership positions with two defense contract firms. In 2009 he returned to federal service with the Fort Worth District, U.S. Army Corps of Engineers (USACE), again serving in leadership positions in support of both the Departments of Defense and Homeland Security. Most recently, he served as Chief, Engineering and Construction Division, for the Europe District, USACE, in Wiesbaden, Germany, in support of both European and Africa Command. Jack is a 1980 graduate of the U.S. Military Academy. He earned a master's degree in engineering from the University of Florida, is a licensed Professional Engineer, and is certified as a Project Management Professional.

[Editor's Note: This article is adapted from Mr. Matthews' individual strategy research project at the National War College and is the winner of the 2019 NMIF Sherman Kent intelligence writing award at NWC.]

The President and Intelligence Communities:
A Study of Conflict

by Dr. William E. Kelly

American Presidents have always used intelligence organizations in one way or another to help themselves. Even George Washington found it necessary to rely on intelligence activity. As one source notes: "Indeed, Washington recruited and ran a number of agents, set up spy rings, devised secret methods of reporting, analyzed raw intelligence gathered by his agents, and mounted an extensive campaign to deceive the British armies. Historians cite these activities as having played a major role in the victory at Yorktown and in the ability of the Continental Army to evade the British during the winters at Valley Forge."(1)

Yet, some might say that a modern American intelligence system had its beginnings in 1947 with the passage of the National Security Act, which established the Central Intelligence Agency. There are 17 agencies which make up the Intelligence Community, but it seems that the Central Intelligence Agency (CIA) and the Federal Bureau of Investigation (FBI) get the most public coverage, even though Edward Snowden brought a lot of public attention to the existence of the National Security Agency (NSA) when he leaked information concerning its spying capabilities in terms of eavesdropping on conversations.

Throughout the Cold War and since then, intelligence organizations have continued to render a valuable service to this country and to the President of the United States. The importance of a good relationship between the President and the Intelligence Community is aptly reflected in an article by the Brookings Institution, in which Daniel Benjamin is quoted as saying: "No American president can succeed in foreign policy—and by extension his term as commander-in-chief—without a good relationship with the intelligence community."(2) However, today there appears to be a conflict between the President and that community. According to the Brookings article, President Trump ". . .smeared the CIA and its sister agencies with accusations of politicizing the intelligence, gross incompetence and even fabrication…"(3)

WHY A PRESIDENT COULD LOSE FAITH IN THE INTELLIGENCE COMMUNITY

It is not too difficult to understand why a President could lose confidence in the Intelligence Community (IC). For example, a President may believe that the IC has failed a number of times to provide adequate information, which could have either embarrassed the President or prevented disastrous consequences. Perhaps possible examples could relate to Pearl Harbor, the U-2 spy plane downing, the Bay of Pigs disaster, an assertion that weapons of mass destruction were possessed by President Saddam Hussein of Iraq, and a more recent view that the Russians interfered with the 2016 Presidential election, giving an unfair advantage to Trump.

Another reason why Presidents could possibly lose faith in the IC is that foreign penetration of our intelligence agencies at times has been successful.

Another reason why Presidents could possibly lose faith in the IC is that foreign penetration of our intelligence agencies at times has been successful. The activities of Aldrich Ames of the CIA, Robert Hanssen of the FBI, and Edward Snowden of the NSA are still remembered by many today and viewed as very serious for the security of the United States. Their activities may cause one to wonder how many similar situations really have taken place in our Intelligence Community in the past and how many are taking place today. They could also show that an intelligence agency is not taking enough precautions to prevent these situations and has endangered American security.

In addition, there may be a belief held by the President that the IC has leaked information embarrassing to him to the general public, such as the allegation that the Russians have a dossier suggesting he behaved in an improper manner. The President may also believe that

information has been leaked to the media from intelligence agencies concerning improper conduct with the Russians on the part of his close aides. His response to the alleged improper conduct has been to refer to it as a "witch hunt."(4)

WHY THE INTELLIGENCE COMMUNITY MIGHT NOT LIKE A PRESIDENT

Yet, currently available public information also suggests that the Intelligence Community might not favor a President. There are good reasons for this view. For example, some public Presidential comments and other actions would understandably not be appreciated by members of the IC. One example of a Presidential statement receiving considerable attention in the media occurred when the President drew a parallel comparison between Nazism and intelligence activities. This public comparison was probably not appreciated by those who work in the IC or who support their activities and see them as important to the security of the United States. For example, former CIA Director John Brennan was critical of Mr. Trump's comment. A source noted: "Brennan…said he took 'great umbrage' at Trump's suggestion that agencies biased against him were behaving as if the U.S. were "Nazi Germany."(5) It is not only the negative public comments made by the President but also his particular actions toward individuals within the IC. Firing James Comey has been described as a negative action by many, not only because he has been viewed as a successful director but because the firing may have demoralized many within the Bureau who supported him as well as many in other agencies who respected his professional demeanor. As one source noted: "FBI agents were enraged by the firing… Agents regarded him as a good manager and an independent director."(6) Such an action by a President may also be viewed as sending a message to other high-ranking officials within the IC that unless they support the President they may suffer the same consequences as Mr. Comey.

In addition, a belief within the Intelligence Community that the President might engage in "leaks" of classified information which could endanger those who secured this information in a covert manner would not help matters. Perhaps an example of this view would be the allegation that Trump leaked to the Russians classified information given to him from the Israelis about ISIS. Interestingly, David A. Graham noted in *The Atlantic*: "Even if what Trump did is legal, what is legal and what is acceptable are, of course, not the same thing. For one, passing such information along, intentionally or not, could jeopardize American intelligence relationships around the world, and potentially weaken national security."(7)

THE EFFECTS OF A LACK OF TRUST BETWEEN THE PRESIDENT AND THE INTELLIGENCE COMMUNITY

The lack of trust between the President and the Intelligence Community could have negative consequences. One source has some interesting comments about this lack of trust: "American military and intelligence agencies must assume from now on that the president of the United States is a security risk. He cannot be trusted to protect state secrets."(8) This particular source also points out: "When officials at one agency of government become convinced that another cannot be trusted to preserve secrets, they slow the information to that agency. Can they do that when the distrusted agency is the White House, the distrusted person the president of the United States?"(9)

The lack of trust could also encourage those American opponents to work harder to sow seeds of discontent in this country between two important political entities. These opponents may believe that there is more opportunity for them to make inroads into the safety of the United States and strengthen their own role in the area of international relations. Therefore, they may even increase their covert attempts at bringing about more distrust between the IC and the President. It would seem that leaders of some foreign countries could be quite content with the present situation in the United States involving President Trump and his workings with intelligence agencies.

There are also a host of other possible negative results from the rift between the President and the Intelligence Community. Low morale may come about for those who are employed in both entities. Individuals who are very qualified to work in government may also believe that they would not feel comfortable working in a situation characterized by conflicts between the President and an intelligence agency. In addition, valuable time, which in itself is considered a critical asset, may be wasted when both the President and the IC believe they have to work harder to prove that they have been doing a commendable job.

WAYS TO LESSEN THE RIFT BETWEEN THE PRESIDENT AND THE INTELLIGENCE COMMUNITY

Yet, In spite of the apparent current state of affairs between the President and the Intelligence Community, which appears to be acrimonious at times, there are ways on the part of both to make U.S. intelligence activities more effective. For example, the President could stop making comments that are critical of the IC. When these comments are made, they tend to have

negative consequences, such as lowering the morale of agency employees and creating distrust in these agencies among the public. The negative comments could also be viewed as being helpful to our foreign enemies because they impair the effectiveness of the IC, which is necessary to protect this country.

Praising the Intelligence Community publicly would also help lessen the rift between the President and the Community. Generally, the U.S. IC has done a commendable job in spite of some limitations placed upon it. Hence, it would serve the President and this country well if he were to emphasize publicly the positive aspects of the IC and downplay those considered negative. A good example of this is when the President visited the CIA and remarked, "I just want to let you know I am so behind you…" and "…you're the No. 1 stop…"(10)

One should realize that no part of government can be said to be perfect all the time and this certainly includes the executive branch and the Intelligence Community as well. At present, it seems that too much criticism is directed toward the IC and too little praise is given to its many successes. As John Kennedy said after the United States was embarrassed as a result of the Bay of Pigs fiasco, "Victory has a hundred fathers, but defeat is an orphan..."(11)

Of course, there are many formal ways that a President can improve the effectiveness of the Intelligence Community and increase morale within it. One would be the nomination of respected qualified individuals to head the agencies within the IC. Doing so would demonstrate that the President is interested in the continued professionalization of the IC. It would probably also result in higher morale within the Community because such a choice would be viewed as non-political and based on capabilities needed in the intelligence enterprise. It would also lessen the chances of opposition from those government bodies which approve a President's nominations. Thus, whoever is nominated by the President to serve as head of an intelligence agency should have a number of qualifications. For example, this individual should have had successful managerial experience in intelligence activities or international relations. One must remember that the director of an intelligence agency is in fact a manager, and that an intelligence agency is quite different from a traditional business organization. Thus, an appointee should be one who has had a long and distinguished career in national security or international relations, not one who is a relative or a close personal friend. Secondly, the nominee must be someone who can be confirmed by the Senate, and it would help if such a person did not have a history of strong preference for a particular political party. In other words, the President should avoid demonstrating political partisanship in his nomination of an intelligence director. Thirdly, the nominee must recognize the value of objectivity in providing information to the President regardless of the latter's preference for a particular type of intelligence finding.

Some time ago a progress report was declassified which concerned the relationship between American policymakers and intelligence officers, which could be said to relate to the current relationship between the U.S. President and the Intelligence Community. This particular report emanated from the CIA's Center for the Study of Intelligence and Georgetown University's Institute for the Study of Diplomacy. It highlights the importance of shared responsibility for the effective use of intelligence. This implies that close cooperation between policymakers and intelligence officials has benefits for the effective use of intelligence. There should also be inquiries by those who participate in intelligence meetings because asking questions often stimulates valuable input and may prevent unfortunate results. This also has the advantage of clarifying important points made in such a meeting. Finally, it is suggested in the report that an intelligence agency should not be reluctant to note its disagreement with a particular policy. There is a limit as to what an intelligence agency is capable of doing and this should be recognized by both the IC and the policymaker.(12)

THE FUTURE RELATIONSHIP BETWEEN THE PRESIDENT AND THE INTELLIGENCE COMMUNITY

Today it could be said that the relationship between the President and the Intelligence Community is not what it should be. Perhaps the most obvious characteristic is the negativity that seems to be present in that association. History, however, has shown that the relationship can change for the better over time. One thing is certain, and it is that both political entities must want to improve the relationship. Too much is at stake for the security of the United States for a situation in which these two valuable institutions seem at times not to be working harmoniously together for a common goal.

One must remember that what the President does today can affect the future of the Intelligence Community. Negative public comments by the President about the IC can create a hostile view of them among the American public and be an asset to our international enemies. That view can last a long time. Certainly the appointment by the President of directors of intelligence agencies will have an impact on those agencies. This is why such appointments are so important. It is also important that trust exist between the President and the IC. Without this trust there could be a lack of communication between them, which hampers the effectiveness of decision-making.

The publication *Lawfare* has an interesting essay written by Joshua Rovner, an intelligence scholar associated with Southern Methodist University, titled "Donald Trump and the Future of Intelligence." One part of his provocative essay deals with "Intelligence Under Trump," in which the author suggests that the Intelligence Community faces two dangers in the next few years. One is neglect and the other is the manipulation of intelligence to reflect policy preferences. Both of these could seriously hamper the effectiveness of the IC. Another part of Rovner's essay concerns "Intelligence After Trump." Here the author notes that intelligence leaders should consider the long-term effects of their actions and that agencies are expected to be under pressure for some time. He also suggests that intelligence agencies should consider a number of questions, such as how to regain a reputation for impartiality, how to restore public confidence, and how they can attract the best personnel.(13) The answers to these questions are not easy but they should be considered and acted upon.

The Trump administration is still relatively immature, and things could change in the future regarding the relationship between its leader and the IC. Mr. Trump himself is not a professional politician, and has had little experience working with government machinery compared to others in government such as U.S. Congressmen or Senators who seem more likely to recognize the importance of good public relations. Perhaps President Trump's style of seeking accomplishments and public recognition of them comes from his background, which might be more successful in the private sector than the public, where a different style of leadership is found. Yet, he is the head of state and arguably the most important public policymaker in the world. This is why the President is so important to the Intelligence Community and why only measured, prudent change in their relationship is recommended.

NOTES

[1] "The Evolution of the U.S. Intelligence Community-An Historical View," https://fas.org/irp/offdocs/int022.html. Accessed May 19, 2017.

[2] Daniel Benjamin, "How Trump's Attacks on the Intelligence Community Will Come Back to Haunt Him," https://www.brookings.edu/blog/order-from-chaos/2017/01/12/how-trumps-attacks-on-the-intelligence-community-will-come-back-to-haunt-him/. Accessed May 19, 2017.

[3] Ibid.

[4] Mark Lander, "Trump, Citing 'a Witch Hunt,' Denies Any Collusion with Russia," *The New York Times*, May 18, 2017, https://www.nytimes.com/2017/05/18/us/politics/trump-back-on-twitter-complains-of-witch-hunt.html?_r=0. Accessed May 18, 2017.

[5] Staff and Agencies, "John Brennan: Trump's 'Nazi Germany' Tweet to US Agencies was 'Outrageous," *The Guardian*, January 15, 2017, https://www.theguardian.com/us-news/2017/jan/15/john-brennan-trump-nazi-germany-russia. Accessed May 23, 2017.

[6] Michael D. Shear and Matt Apuzzo, "F.B.I Director James Comey Is Fired by Trump," *The New York Times*, May 9, 2017, https://www.nytimes.com/2017/05/09/us/politics/james-comey-fired-fbi.html?_r=0. Accessed May 23, 2017.

[7] David A. Graham, "What Did Donald Trump Tell the Russians?" *The Atlantic*, May 15, 2017, https://www.theatlantic.com/politics/archive/2017/05/trump-classified-information/526797/. Accessed May 19, 2017.

[8] David Frum, "What Happens When Intelligence Agencies Lose Faith in the President?" *The Atlantic*, https://www.theatlantic.com/.../what-happens-when-intelligence-agencies-lose-faith-in. Accessed May 22, 2017.

[9] Ibid.

[10] Amber Phillips, "Analysis: Trump Has Had a Rocky History with His Own Intelligence Agencies," *The Washington Post*, May 15, 2017, http://www.chicagotribune.com/news/nationworld/politics/ct-trump-intelligence-agencies-20170515-story.html. Accessed May 22, 2017.

[11] David Greenberg, "The Goal: Admitting Failure, Without Being a Failure," January 14, 2007, *The New York Times*, http://www.nytimes.com/2007/01/14/weekinreview/14green.html. Accessed May 22, 2017.

[12] James A. Barry, Jack Davis, et al., "Bridging the Intelligence-Policy Divide," https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol37no3/html/v37i3a02p_0001.htm. Accessed May 23, 2017.

[13] Joshua Rovner, "Donald Trump and the Future of Intelligence" (a foreign policy essay), *Lawfare*, January 8, 2017, https://www.lawfareblog.com/donald-trump-and-future-intelligence. Accessed May 24, 2017.

Dr. William E. Kelly earned his PhD degree from the University of Nebraska. His awards include being selected three times as the Outstanding Political Science Teacher at Auburn University by Pi Sigma Alpha, a Mortar Board Favorite Teacher of the Year Award at Auburn, and a teaching award from the American Political Science Association. He has also been nominated for the College of Liberal Arts as the outstanding advisor, as well as by his department for an alumni professorship in political science. In addition, he has been nominated three times by his department as the outstanding teacher in the College of Liberal Arts. He has taught at military bases, community colleges, and a private religious college. Dr. Kelly teaches American government and criminal justice and also serves as the political science internship coordinator. Bill has published in The Journal of Education and Psychology, The New Review of East-European History, Public Sector, The Journal of the Alabama Academy of Science, *and* South Arkansas Historical Journal. *Other publications appear in various encyclopedias. In addition, he has published over 100 book reviews and his review work has appeared in* Military Intelligence, Perspectives on Political Science, The American Political Science Review, The Journal of Politics, American Intelligence Journal, Parameters, The Journal of Military History, Air University Review, *and* Armed Forces and Society.

Pakistan and the Taliban:
South Asian Geopolitics and the Reemergence of the Taliban in Afghanistan

by Andrew H. Fraser

In one of the greatest intelligence failures of the post-9/11 era, the West failed to foresee the dramatic resurgence of the Taliban in Afghanistan. Beginning around 2005, the Afghan Taliban went from a seemingly spent force to a fearsome enemy that was fielding men in battalion-strength numbers and carrying out a sustained campaign of suicide bombings, improvised explosive device attacks, and hit-and-run assaults. How the Taliban have been able to reestablish as a battlefield force remains a mystery. However, a series of local and international media excursions to the village of Shabqadar, in northwestern Pakistan, to cover the story of young local men who volunteered to die as martyrs in Afghanistan offers stark insight into this perennially opaque and potentially defining issue of the war in Afghanistan.

What the excursions uncovered provides startling clues about the rebirth of the Afghan Taliban. It appears that well-established Pakistani militant organizations that have often functioned as assets of the Pakistani state have been recruiting and training fighters and suicide attackers for the Afghan Taliban. For the most part, they have faced little resistance from the authorities. When placed in the broader context of regional geopolitics, these events suggest that the answers to the Taliban's resurgence in Afghanistan are found in Pakistan.

In the mid-1990s, it was only through massive Pakistani investment that the Taliban was able to propel itself from being an upstart regional rebellion to a military power with a national reach. It would seem unlikely that the extraordinary re-ignition of the Taliban as a battlefield force could have ever taken place without considerable outside help.

Islamabad's long-held strategic interest in exerting substantial influence over Afghanistan and thwarting the emergence of Pashtun nationalism touches on Pakistan's national survival. It is also inextricably tied to Pakistan's lifelong rivalry with India. After the 9/11 attacks, the United States seemingly expected Pakistan to abandon the Taliban while Washington proceeded to back a government in Kabul that was both ineffectual and hostile to Pakistan's vital interests in Afghanistan. With no other organization that can credibly represent its interests in Afghanistan, it would be naïve to suggest that official sources in Pakistan would vacate their profoundly important relationship with the Taliban.

THE RETURN OF THE TALIBAN

The return of the Taliban as a sustained military entity started to become apparent in 2005 as NATO forces were expanding their operations in southern Afghanistan. That year, the number of Americans killed in Afghanistan nearly doubled from the previous year to almost 100.

By 2006, heavy fighting was raging in Afghanistan between NATO forces and a startlingly resurgent Taliban. After having been driven from power and seemingly scattered in late 2001, the Taliban was now fielding combatants in battalion-strength numbers in the southern part of the country. It was also mounting a campaign of ambushes, suicide bombings, and roadside improvised explosive device attacks throughout both the south and the east. Suicide bombings alone mushroomed from being almost non-existent in Afghanistan prior to 2003 to 160 in 2007.

As of this writing, the Taliban's renewed campaign has raged for close to a decade and a half. The insurgency has lasted far longer than the Soviet occupation. That ten-year campaign was itself only made possible through massive outside assistance.

SHABQADAR

As the Taliban's resurgence was blossoming, a series of both Pakistani and international correspondents travelled to the market town of Shabqadar in Pakistan's North-West Frontier Province.[2] They were searching for answers about reports of young men from the community being drawn into the brutal war hundreds of miles away in southern Afghanistan.

A Pashtun frontier town known for both its bustling market and its historic fort perched just south of the main population center, Shabqadar was long the gateway to the nearby Pashtun tribal areas. The town stands at the center of a naturally occurring triangle. The craggy hills of the Mohmand Tribal Agency lie to its west. The Swat and Kabul Rivers flow to the south and to the north before merging near the town's historic fort. This fortuitous geography has sustained Shabqadar's traditional role as an agricultural center and breadbasket of the region.[3]

Shabqadar had played host to everyone from Sikh imperial ruler Ranjit Singh to a young Winston Churchill, who spent time at the historic fort during an expedition to the region.

In past centuries, Shabqadar had played host to everyone from Sikh imperial ruler Ranjit Singh to a young Winston Churchill, who spent time at the historic fort during an expedition to the region.[4] Even with its historic role as a market town and agricultural heartland, Shabqadar had faced exacting economic hardship and substandard government services, leaving a sizable pool of young men jobless and grappling with an uncertain future. Rampant corruption endemic throughout Pakistan that tends to favor wealthy landholders heavily has doubtlessly exacerbated the plight of the common Shabqadari.

Visiting reporters on an excursion to the community met with three local families who told stories of having a son killed in Afghanistan. A large contingent of militants had visited each of the families carrying the dreadful news that one of their sons had perished as a suicide bomber. One was Aminullah, who at 22 was an officer in Pakistan's paramilitary Frontier Constabulary. By nature a serious young man, he was enticed away to die as a martyr in Afghanistan. His father was presented with a handwritten note attributed to his son expressing a final wish to die as a martyr on the grounds of religious duty.[5] He had previously expressed indignation at the deaths of civilians in Afghanistan at the hands of international forces. The militants who broke the news to Aminullah's family specified that the attack occurred in Kandahar Province and provided a timeline that makes it very likely that Aminullah was one of two bombers who blew themselves up in an attack on a NATO convoy in Kandahar in July 2006.[6] Two soldiers and five bystanders were killed.[7]

Another was Bahar Ali, a 23-year-old laborer who had worked in Saudi Arabia and had apparently spent time as a militant fighter in Indian-administered Kashmir. His family and the few friends he had described him as a solitary and seemingly lonely young man who drifted under the sway of Islamic militants.[8]

In the heat of late August 2006, a large group of men from the well-known Pakistani militant organization Hizbul-Mujahideen came to visit the family home to tell relatives that Bahar had been martyred, indicating he had died in a suicide bombing in Kandahar Province around August 11, 2006.[9] The date and location are consistent with an attack on a NATO vehicle that claimed the life of a medic who had been posted halfway around the world to serve in Afghanistan.[10]

The third was a teenager named Aminullah Hakim, who refused his father's offer both of a job and an arranged marriage before one day disappearing while ostensibly on a trip to visit Rawalpindi some 120 miles away. His father received the familiar visit from a large group of militants; by his account no fewer than 20 men arrived to tell him that his son was dead.[11] The details they provided matched those of a suicide attack that occurred in the capital of Kandahar's neighboring province Helmand. A local man who had once been a police official was the target of the bombing. He was killed along with 16 bystanders when the device Aminullah was carrying exploded in a market.[12] Locals told the visiting reporters that about 100 boys and men from the Shabqadar area were feared to have gone to Afghanistan.[13] The recruiters were not members of the Afghan Taliban but were instead from well-established Pakistani militant organizations.

When contemplating the ease in which recruiters were able to operate in Shabqadar, it is important to remember the local tradition of using violent means to crush those who dissent from the conservative social and religious order that reigns in the area. Shabqadar gained passing mention in the international media in 1995 when mob rage against members of the tiny and oft-discriminated-against Ahmadi Muslim sect degenerated into savagery.[14] Authorities had arrested an Ahmadi telephone company employee named Daulat Khan on heresy-related charges. He was a resident of a village just outside Shabqadar. Sunni clerics in the area branded the man an apostate and decreed that he be killed. Posters went up around Shabqadar calling for Khan's execution.[15]

Local Mullahs whipped villagers into a frenzy by parading through the streets in a truck broadcasting over a loudspeaker vitriol about the heretical Ahmadis.[16] When a trio of Khan's supporters arrived at the courthouse next to Shabqadar's main market with the intent of bailing him out, they were set upon by an enraged mob. With many locals joining in, the mob stormed the courthouse in pursuit of the oldest man in the group, beating and hacking him to death. His two companions narrowly escaped with their lives.

The visiting reporters determined that recruiters were active in many communities throughout the region. *The New York Times* discovered that in the same time frame similar recruitment drives were under way in the vicinity of Quetta in Pakistan's Baluchistan Province, long reputed to be the location of the Afghan Taliban leadership.[17] Although recruiters often met little resistance, in the community of Tank, 150 miles south of Shabqadar, gun battles erupted when the authorities tried to thwart the recruiters who were even going so far as to recruit boys nor just from madrassas but from local private schools as well.[18]

THE MILITANTS

Among the most shocking aspects of the stories that have emerged from Shabqadar is the central role given to established Pakistani militant organizations that are more associated with the war against Indian rule in Kashmir than recruiting and training combatants for the Afghan Taliban. The Pakistani government and its ubiquitous intelligence services have a long history of using such groups to accomplish goals in the region. Islamabad often employed them both as a relatively inexpensive foreign policy instrument to fight the Soviet Union in Afghanistan and later the Indian Army in Kashmir, and also as a domestic policy tool to intimidate opponents in Pakistan.[19] It would appear that some of these same groups became involved in supporting the Taliban in Afghanistan.

Hizbul-Mujahideen was founded in 1989 as part of the uprising against Indian rule in Kashmir.

The role of such organizations is often overlooked in discussions surrounding the resurgence of the Taliban in Afghanistan. By 2002, there were 24 Islamist militias operating in Pakistan.[20] Young men faced with a stifling economic climate that frequently left them without jobs could find a sense of both social belonging and spiritual purity.

Hizbul-Mujahideen was founded in 1989 as part of the uprising against Indian rule in Kashmir.[21] It envisaged a unified Kashmir under Pakistani control and supported the Islamization of the region. The organization was created at the reported direction of Pakistan's powerful *Inter-Services Intelligence Directorate (ISI)* to act as a counter- weight to the Jammu and Kashmir Liberation Front (JKLF), which sough outright independence for Kashmir. Its members were recruited from both Indian- and Pakistani- ruled areas of Kashmir as well as other parts of Pakistan, particularly the Punjab and to a lesser extent the North-West Frontier Province. Although not known for carrying out particularly sophisticated attacks, Hizbul-Mujahideen emerged as one of the leading militant organizations battling the Indian security forces in Kashmir.

In the early 1990s, the organization reportedly established ties with Hizb-e-Islami, an Afghan Mujahideen organization that was a perennial favorite of Pakistan before its faltering reliability caused Islamabad fatefully to shift its support to an emergent militia movement in Afghanistan's south in the mid-1990s. As if to attest to the high degree of influence the ISI exercised over Hizbul-Mujahideen, the organization declared a three- month ceasefire in Kashmir in June 2000 on orders from the ISI's commanding general.[22]

Harkat-ul-Mujahideen emerged as a militant organization in Pakistan in the mid-1980s with a mandate to fight the Soviets in Afghanistan. When the USSR withdrew from Afghanistan in 1989, the group shifted its focus to participating in the rebellion against Indian rule in Kashmir. The group reportedly forged ties with al-Qaeda in the 1990s. It was responsible for the high-profile tourist kidnappings in Kashmir in the mid-1990s and the hijacking of an Indian airliner flying out of Kathmandu in December 1999.[23]

Harkat-ul-Mujahideen had a visible presence in Shabqadar. It maintained a formal office in a two-room building near the town's central market. A local citizen in his mid-20s, who purported to have fought for the Taliban in Afghanistan under the *nom de guerre* Abu Hamza, shared with visiting Associated Press correspondents that he had recruited a number of locals on behalf of the latter militant group. He recounted offering them wondrous promises about the heavenly paradise that awaited them after they martyred themselves.[24] Once they had been enticed, he recounted, local enlistees were sent to the tribal badlands in Waziristan for training before their final journey into Afghanistan.

Police in the region reported that they shuttered the Harkat-ul-Mujahideen office in November 2006. They claimed that by the time they arrived the recruiters had left, leaving no one to arrest. When the Associated Press writers published the account of their visit to the town in early 2007, they noted that the office was still unoccupied. According to the recruiter, by late 2006 locals had largely stopped volunteering, prompting a career change for the militant who took to selling groceries at a neighborhood shop.[25]

In addition to pressure from both the authorities and from villagers themselves, Harkat-ul-Mujahideen's efforts were apparently hampered further by the reported battlefield deaths of several of its senior members. It should be noted that these developments occurred in the immediate wake of ferocious fighting between NATO forces and insurgents in western Kandahar Province in August and September 2006.

The central role that locals attributed to Pakistani militant organizations suggests a connection between well-established Pakistani militant organizations and the Afghan Taliban, which has not been fully explored in discussions about Afghanistan. Based on the events that took place in Shabqadar and the surrounding area, it would appear likely that these groups shifted their operations toward backing the Taliban in Afghanistan.

PAKISTAN'S STRATEGIC INTEREST IN AFGHANISTAN

Achieving the fabled goal of "strategic depth" on its western flank and gaining a level of control over Afghan affairs are long-standing aims of Pakistani foreign policy going back to Partition in 1947. The division of the British Indian Empire ignited generations of wrenching tensions between India and Pakistan. It also shaped Pakistan's modern interest in its Afghan neighbor. Pakistan is locked in a geostrategic vice that compresses the nation between a mortal enemy on one side and a perpetually unstable political sinkhole on the other. In the event of a war with India, a friendly Afghan regime could allow the Pakistani military to use Afghanistan as a springboard to regroup and launch a counterattack.[26]

If Pashtun nationalist sentiment ever got out of control in Afghanistan, it could foment rebellion and ethnic violence involving Pakistan's own considerable Pashtun minority. This is particularly dangerous in Baluchistan, which borders Kandahar Province, where ethnicity is largely divided between Pashtuns and ethnic Balochs who have their own proclivity for potentially disruptive nationalist sentiment.[27] Such an outcome could also be highly troublesome in the teeming port city of Karachi, where between 20 and 25 percent of the population is Pashtun.[28] This is the largest urban Pashtun population in the world.

Islamization also consolidated the power and the legitimacy of the Pakistani government and its shadowy intelligence apparatus.

Pakistani authorities have long encouraged Islamic fundamentalism, both in Pakistan and Afghanistan, to sooth tensions along Pakistan's combustible ethnic fault lines. This formed part of a comprehensive program of Islamization in Pakistan's military, bureaucracy, and educational system that intensified with the ascent of Muhammad Zia-ul-Haq as President in 1977 after he overthrew and subsequently executed his predecessor Zulfikar Ali Bhutto.[29]

If an elixir was not found to ease the country's ethnic divisions, a crisis of ethnic particularism could potentially have destroyed Pakistan. Islamization also consolidated the power and the legitimacy of the Pakistani government and its shadowy intelligence apparatus. Given the state's growing role in administering religious aspects of Pakistani life, challenging the state became much closer to challenging Islam itself. The legacy of such policies also creates a potential affinity between Pakistan's upper crust and the hardcore Islamist ideology embraced by the Taliban.

Pakistan played a pivotal role in molding the Taliban into an effective fighting force in the mid-1990s. Although reluctant at first, Pakistan grew progressively more interested in funding and nurturing the Taliban, which allowed it to transform itself from a regional Pashtun militia with little money filling a void in southern Afghanistan to a potent military organization with a vast national reach.

The Pakistani government invested massively in the organization, even arming thousands of Pakistani citizens and sending them to wage war on behalf of the Taliban, spurring its rise to power.[30] These volunteers were recruited locally in Pakistan and they included many who were drafted out of madrassas. The depth of this investment and the critical strategic goals that it accomplished remained poorly understood in the United States when Washington demanded that Pakistan sever its relationship with the Taliban.

For Pakistan's political and military elite, the Taliban proved itself to be a useful subordinate partner.[31] It allowed for the fulfillment of Pakistani strategic goals that went back to the time of Partition. The Taliban's rise to power gave Islamabad a high degree of influence over Afghan affairs, provided a more stable western border, and eliminated the potential for India to gain influence in Afghanistan and thereby tighten the geographic noose that permanently constricts Pakistan. Given that the Taliban's brand of Islamic fundamentalism was in large part mutually exclusive of Pashtun nationalism, it dampened the possibility of an emergent Pashtun nationalist movement in Afghanistan demanding a Pashtun homeland, including parts of Pakistani territory.

CRISIS AND OPPORTUNITY

U.S. demands that Pakistan turn on the Taliban while Washington sought to shatter the Taliban's grip on power in Afghanistan had the makings of a dangerous crisis for Islamabad. Pakistan needs an influential ally that can represent its interests in Afghanistan and there are no other suitors with the potential reach of the Taliban. The potential loss of Pakistan's hard-earned influence on the other side of the Durand Line would be an unacceptable

outcome. However, Islamabad had no real choice when it came to supporting the U.S.-led assault on Afghanistan lest it be branded an international pariah and subjected to an unbearably brutal level of international isolation.

Pakistan's ostensible alliance with the United States has granted the Pakistani state an aura of international legitimacy that otherwise would not have existed...

Yet the international intervention in Afghanistan also brought with it considerable opportunity. After Islamabad's 1998 nuclear weapons tests and a military coup in October 1999, Pakistan was at risk of being branded an international pariah and inflows of international aid could have been in grave peril. This would have been advantageous to India and resulted in Pakistan's geostrategic vice being tightened to near-suffocating proportions. The pleasing mirage that Pakistan was a loyal ally of the United States in the wake of the September 11 attacks solved that problem.

Pakistan's ostensible alliance with the United States has granted the Pakistani state an aura of international legitimacy that otherwise would not have existed, particularly in light of Pakistan's already deteriorating international reputation in the years leading up to 2001. This was made even worse because the previous year had seen India both announce the largest ever increase in its military budget and redouble its efforts to brand Pakistan as a global haven for state-sanctioned terrorism.[32] Moreover, in the run-up to the September 11 attacks, Pakistan's leadership was increasingly anxious about the Bush administration adopting what it perceived as a creeping pro-India stance at Pakistan's inevitable expense.[33] Pledging apparent support to international operations in Afghanistan was beneficial in mitigating that worry as well.

Pakistan has reaped a generous windfall from its alliance with the United States. The General Accountability Office calculated that between October 2001 and June 2007 the U.S. sent $5.5 billion to Pakistan to "reimburse" Islamabad for operations carried out in supposed support of NATO actions in Afghanistan.[34] Between 2002 and 2008, Pakistan had received $10.9 billion in U.S. military and non-military aid and was relying on the U.S. for a quarter of its $4 billion annual military budget.[35]

Lucrative foreign handouts are of particular importance given that the Pakistani state has enormous difficulty raising revenue by traditional means. A traditional feudal structure, endemic corruption, and a toxic system of political patronage that sees political parties seeming to exist as little more than networks of patronage and under-the-table dealings have rendered even basic tax collection sometimes beyond the realm of the authorities. In fact, as of 2009 only about 2 percent of Pakistanis paid income tax.[36] Well-connected feudal landlords often avoided taxes entirely. These landlords were so successful in stopping taxes on their agricultural spoils that, although agriculture accounts for 22 percent of Pakistan's GDP, it represented only 1 percent of tax revenue.[37]

Nominally supporting U.S.-led operations in exchange for massive amounts of money, while at the same time at the very least allowing militant groups with histories of being assets of the Pakistani state to undertake recruiting in Pakistan, is an example of the double game that has long been central to the cold-blooded brinkmanship that has defined the world of Pakistani political power.

PAKISTAN AND AFGHANISTAN: A HISTORY OF COVERT WARFARE

Throughout Pakistan's often tumultuous history, Afghanistan has been a source of fear, crisis, and considerable opportunity. Islamabad continuously has resorted to covert means when confronted with a hostile situation in Afghanistan. The emergence of the Pakistani state at the time of Partition ignited an immediate territorial dispute with Afghanistan, whose leadership wanted Pashtun lands in Pakistani territory ceded to it. This was a blatant threat to Pakistan, whose national existence was based on the concept of diverse ethnic populations with potentially contradictory aspirations forged together beneath the unifying pennant of Islam.[38]

Covert warfare ensued; storms of propaganda were traded across the Durand Line and Afghan goods en route to ports on the Indian Ocean frequently fell victim to attack while travelling through Pakistan.[39] Tensions between the two countries over the Pashtun question eventually eased but then erupted anew with the re-ascension of Mohammed Daoud Khan, who originally came to power in a coup in 1973. A renewed firestorm of anti-Pakistan propaganda was soon emanating from the Afghan side of the border. Pakistan, for its part, surreptitiously backed an insurrection against the Afghan regime in 1975.

The Soviet invasion prompted yet another Pakistani crisis centered on Afghanistan. Massive inflows of refugees from Afghanistan threatened to exacerbate tensions along Pakistan's already precarious ethnic fault lines.[40] The Soviet incursion into Afghanistan drove anxiety in Rawalpindi and Islamabad that Pakistan itself could be in mortal danger. Fears abounded among the Pakistani elite that the USSR was looking for ports on the Indian Ocean and would use its

presence in Afghanistan to collaborate with India either to facilitate an attack against the Pakistani-ruled portion of Kashmir or to embark on an even more insidious plot with India to encircle Pakistan and carve it up between them.[41] A hostile force in power in Afghanistan was intolerable.

Pakistan played a wide-ranging role in supporting the Jihad against the Soviet Army in Afghanistan in the 1980s.[42] As domestic and international support for the Afghan resistance flowed through Pakistan, ISI, the nation's preeminent intelligence service, saw a massive expansion of its power. The organization was now a major instrument of Pakistani foreign policy.

After the Soviet withdrawal, the Iran-oriented Rabbani regime in Kabul frustrated Pakistan's long-held ambitions in Afghanistan.[43] Pakistan backed warlord Gulbuddin Hekmatyar's Hizb-e-Islami organization as its primary proxy in Afghanistan. Pakistan's powerful and ever fearful intelligence establishment was worried that, if Hekmatyar were to lose influence, the Rabbani administration would consolidate its power with famed warlord Ahmed Shah Masood, and that would trigger a gradual shift toward India and an open door toward expanded Indian influence in Afghanistan.[44] After Hekmatyar was unable to deliver as desired, Islamabad turned to the upstart Taliban movement in the mid-1990s, reluctantly at first but then investing greatly in the organization when it appeared it could deliver results.[45]

Although Pakistan officially parted ways with the Taliban after September 11, 2001, it would be unrealistic to expect that generations of Pakistani strategic thinking which led to Islamabad's alliance with Afghanistan's Taliban would evaporate simply because the United States attempted to buy Pakistan's loyalty with billions of dollars in aid.

This history of Pakistan's continuous and often clandestine engagement in Afghanistan does not simply vanish into the thin air of the Hindu Kush because the United States launched a massive intervention in the region. This is particularly true given that Islamabad saw the Karzai regime, which the United States engineered and backed, as dangerously hostile to its interests and stacked with anti-Pakistan remnants of the Northern Alliance. In modern Afghanistan, there does not appear to be anyone other than the Afghan Taliban who can reliably represent Pakistan's fundamental strategic interests in the country.

PAKISTAN AND THE TALIBAN

Although Pakistan officially parted ways with the Taliban after September 11, 2001, it would be unrealistic to expect that generations of Pakistani strategic thinking which led to Islamabad's alliance with Afghanistan's Taliban would evaporate simply because the United States attempted to buy Pakistan's loyalty with billions of dollars in aid. The restoration of the Taliban to power in modern Afghanistan would once again secure Islamabad's long-term strategic goals on its western border. It would allow Pakistan to reassert its influence over Afghanistan and would obviate the frightening prospect of creeping Indian influence in Kabul, something which Pakistan associated with the government of Hamid Karzai. It would also give Islamabad something resembling the client regime in Afghanistan that it has long desired. In the decade and a half since the reemergence of the Afghan Taliban, no other organization has come into being with the reach that could help Islamabad secure its coveted goals in Afghanistan.

Pakistan has often alluded to fighting between the Pakistani security forces and the collection of organizations referred to as the Pakistani Taliban in the Federally Administered Tribal Areas as proof of the commitment by powerbrokers in Islamabad and Rawalpindi to battle the Taliban and al-Qaeda. However, unlike the Afghan Taliban, these militants are challenging the Pakistani state within Pakistan. Islamabad's efforts to confront domestic militants should not be confused with a commitment to oppose the Afghan Taliban. Unlike the Afghan Taliban, if the Pakistani Taliban is not pushed back it could signal to other potentially restive militant groups in Pakistan which trawl the country's combustible ethnic fault lines that they too could benefit by directly challenging the Pakistani state.

Despite the intermittent efforts of the Pakistani Army to battle radicals in the tribal areas who also threaten Islamabad's influence over the region, other militant structures in Pakistan which affect the situation in Afghanistan more directly remain curiously untouched. Most prominent among them is the Afghan Taliban Shura, widely reputed to be based in Quetta, which is in Baluchistan and near the border with Kandahar Province.[46] Nevertheless, it has existed largely undisturbed by Pakistani authorities, who officially deny its existence. Such an arrangement could not flourish without the complicity of the Pakistani state and its powerful intelligence apparatus. It should be noted that the paramilitary policeman Aminullah's last call to his family before he committed suicide in Afghanistan came, according to his family, from Quetta.[47]

A similar principle applies to Pakistan's intermittent operations against al-Qaeda figures living in areas of Pakistan that are thoroughly under the grip of the Pakistani government. Pakistan pledges its support for operations against al-Qaeda, occasionally offering up an al-Qaeda fugitive while others remain free.

When Osama Bin Laden was finally killed, he was slain in a compound adjacent to a military academy in the town of Abbottabad, where many current and former military personnel reside. Given the tense security situation in Pakistan and the omnipresence of the Pakistani intelligence apparatus, it seems unlikely that the most wanted fugitive in the world could be residing in such a sensitive location without at least some high-level support in Pakistan. It makes perfect sense that Pakistan would resist handing over the ultimate prize to the United States, just as it makes sense that Pakistani authorities would only offer piecemeal assistance by capturing al-Qaeda figures in Pakistani cities like Peshawar and Karachi.

If the al-Qaeda network in Pakistan was rounded up and abolished, there would be diminished reason for the U.S. to continue its generous aid to Pakistan. There would be little to stop al-Qaeda from branding Pakistan a nuclear-armed rogue state and throwing its lot in with India, all the while continuing its operations in Afghanistan. In its place, the Pakistani leadership, long a master of the double game, would likely do exactly the same thing. It would dispose of a potentially dangerous client the moment its usefulness had elapsed.

PAKISTAN AND THE WEST: MUTUALLY MISUNDERSTOOD PERSPECTIVES

An underlying problem is that the United States and Pakistan likely never understood each other's positions and strategic interests in Afghanistan. Pakistan's military elite believed that a client regime in Afghanistan was owed to Islamabad after the enormous Pakistani investment in the war against the Soviets.[48] The elite were terrified over the potentially devastating consequences of Afghanistan coming under the control of forces unfriendly to Pakistani interests.

Pakistan invested greatly in the Taliban beginning in the mid-1990s while it was being asked by the United States to set aside that investment as a complete loss and abandon deeply held strategic goals which Islamabad saw as important to the survival of the nation to suit Washington's interests. To worsen the situation, the United States disregarded Pakistan's pleas that the hostile Northern Alliance be excluded from the Karzai regime, seemingly without realizing the impact it would have on Pakistan's national interests.[49]

By 2001, the Taliban had grown into a difficult but ultimately reliable partner which protected Pakistan's interests.[50] The Karzai regime that replaced it in Kabul offered no such advantage to Pakistan. Karzai's regime ended up with diminished influence outside Kabul and was seen in Islamabad as dangerously susceptible to Indian influence.

The return of the Taliban to a position of higher influence in Afghanistan coincides with lifelong Pakistani strategic goals of abolishing Indian influence on its western border, influencing Afghan affairs, and dampening the potential spread of Pashtun nationalism in Pakistan.

On the other hand, it is unlikely Pakistan truly understood that much of what the United States wanted in Afghanistan was a measure of stability which would foreclose the country's use as a staging ground for terrorist attacks against the United States. If that was achieved, there would be little motivation to continue with the presence of large numbers of foreign forces in Afghanistan.

Fewer attacks against international forces in Afghanistan would have offered a greater illusion of stability and likely served as an impetus for U.S. and international forces to wind down or at least scale back their operations under the belief that victory was in hand. The Taliban's reemergence actually provoked instability that greatly prolonged the deployment of international forces to Afghanistan in contradiction of the Taliban's goals.

The return of the Taliban to a position of higher influence in Afghanistan coincides with lifelong Pakistani strategic goals of abolishing Indian influence on its western border, influencing Afghan affairs, and dampening the potential spread of Pashtun nationalism in Pakistan. Yet, by giving the Afghan Taliban and its allies, at the very least, a high degree of autonomy within Pakistan, Islamabad has likely prolonged the massive international military deployment in Afghanistan rather than abbreviating it.

(DOUBLE) DEALING WITH PAKISTAN

Forging even the possibility of a long-term solution in Afghanistan will require the United States to accommodate Pakistan's strategic interests. This will require wrenching compromise and a systemic reevaluation of Western goals in Afghanistan. Does the West want Afghanistan to be an emergent democracy or does it want to deny Afghanistan as a base and a training ground for

terrorist attacks against the West? Given Pakistan's influence, the noble ambition of the former may not be reconcilable with the reality of the latter. Pakistan will always be there, sharing a border with Afghanistan, and so long as there is a regime in Kabul that is alien to Islamabad's interests there will likely be violent instability in Afghanistan.

In the search for peace, the West will have to invest in Pakistan's desire for a friendly regime holding sway in Afghanistan. It will have to abide by Pakistan's long-term interest in exercising a high level of influence over Afghan affairs. Washington and its allies will have to accept a framework that satisfies Pakistan's interest in having a western neighbor impervious to Indian influence, a secure western border, a rally point in Afghanistan to launch a counterstrike against India in the event of war, and the absence of Pashtun nationalism and irredentism on the Afghan side of the border.

There is a great deal that can, and likely will, brutally frustrate such an outcome. The United States may not be willing to compromise, and the daring brinkmanship and ruthless double-dealing that are central to Pakistani power-brokering mean that Islamabad is not the most reliable of negotiating partners. The noble aspirations that many in the West had for Afghanistan—that it could be a democracy with a reliable government and a credible education system for boys and girls, and that the country could be delivered from its instability and medieval poverty—are unlikely to survive the strategic rivalries and ethnic politics that have burned so brightly in the region since long before the partition of British India.

CONCLUSION

The work of international correspondents in northwestern Pakistan raises alarming questions about the extent to which events in that country have been driving the resurgence of the Taliban in Afghanistan. The local story of young men from the village of Shabqadar recruited as suicide bombers for the Afghan Taliban has far-reaching implications for understanding the war in Afghanistan. The recruiters were not members of the Afghan Taliban, but were from well-established Pakistani militant organizations that are better known for fighting the Indian Army in Kashmir. Although sometimes officially outlawed, such domestic Islamist militant groups are also well-established assets of the Pakistani state and its influential intelligence community.

The omnipresent role of Pakistani militant groups with long-standing ties to Pakistan's powerful intelligence services in recruiting suicide bombers in Shabqadar generates ominous questions about the extent to which official sources in Pakistan have allowed, if not out rightly facilitated, the operations of militant groups in places like Shabqadar. It also suggests that such groups have shifted their operations from Kashmir to Afghanistan.

These events did not emerge from a void. They resulted from a very specific context and geopolitical history. A dominant Taliban in Afghanistan would align with Pakistan's long-term strategic interests. These include exerting influence over its perpetually unstable western neighbor, securing its western border, eliminating Indian influence in Afghanistan, and dampening the prospect of emergent Pashtun nationalism that could cause wrenching ethnic tensions if it emerged among Afghan Pashtun and then spread to the Pashtun who live in Pakistan. At the moment, there is no other potential strategic partner that could offer Pakistan even the potential of securing its long-term goals.

Pakistan has played a ruthless double game allying itself with the United States and at the very least allowed the Taliban to use Pakistan as a base for recruiting and planning for its resurrection as a viable fighting force in Afghanistan. This suggests that, if the United States wants a solution in Afghanistan, it will have to accommodate Pakistan's desire for a friendly regime in Kabul. If the West does not want that regime to be the Taliban, then it will have to find an alternate arrangement, which will likely mean some form of Islamist government in Kabul and Kandahar that will abide by Pakistan's requirement for an Afghanistan both free of Indian influence and uninterested in provoking nationalist sentiment among Pakistan's vast Pashtun population. The tragedy of Shabqadar is emblematic of the U.S.-led intervention in Afghanistan itself—violent, potentially intractable, and shaped almost entirely by the deep-seated regional rivalries and strategic ambitions that will define all political and military outcomes in the region.

NOTES

[1] Louis Charbonneau, "UN reports sharp rise in Afghanistan attacks," *Reuters*, March 11, 2008. Accessed March 11, 2008. http://www.reuters.com/article/featuredCrisis/idUSN10517034.

[2] The North-West Frontier Province has since been renamed Khyber Pakhtunkhwa (KPK).

[3] *The Dawn*, "Munda Headworks restored in record time," August 28, 2010. Accessed September 19, 2010. http://www.dawn.com/wps/wcm/connect/dawncontentlibrary/dawn/thenewspaper/local/peshawar/mundheadworks-restored-in-record-time-880.

[4] Mureeb Mohmand, *The Express Tribune*, "Shabqadar Fort: Even an earthquake couldn't free chained gates," October 28, 2015. Accessed February 24, 2018. https://tribune.com.pk/story/980340/shabqadar-fort-even-an-earthquake-couldnt-free-chained-gates/.

[5] Ashfaq Yusufzai, "Suicide Bomber Cult Alive and Well,"

The Inter-Press Service, September 14, 2006. Accessed July 29, 2007. http://ipsnews.net/news.asp?idnews=34718.
[6] Riaz Khan and Matthew Pennington, "Mixed Emotions Greet Taliban Recruiters," *The Washington Post* and the Associated Press, January 28, 2007. Accessed May 23, 2007. http://www.washingtonpost.com/wp-dyn/content/article/2007/01/28/AR2007012800546.html.
[7] Reporters Without Borders, Asia Press Releases, "Follow-up Suicide Bomber Kills TV Employee Covering the Death of Two Canadian Soldiers," July 24, 2006. Accessed March 12, 2007. http://www.rsf.org/article.php3?id_article=18345.
[8] Isambard Wilkinson and Ashraf Ali, "Father's pride at suicide attack on troops," *The Telegraph*, September 1, 2006. Accessed May 25, 2007. https://www.telegraph.co.uk/news/1527790/Fathers-pride-at-suicide-attack-on-troops.html.
[9] Ibid.
[10] Donald McArthur, "Afghan interpreter grateful to fallen Canadian medic," CanWest News Service, *The Windsor Star*, August 21, 2006. Accessed November 2, 2007. http://www.canada.com/topics/news/national/story.html?id=78089d2f-3fbd-4a13-8cb1-cfb48ec175f9&k=38819.
[11] Khan and Pennington, "Mixed Emotions Greet Taliban Recruiters."
[12] Abdul Waheed Wafa, "Suicide Bomber Kills 17 in Afghan Bazaar," *The New York Times*, August 28, 2006. Accessed May 16, 2008. http://www.nytimes.com/2006/08/28/world/asia/28cndafghan.html?_r=1&oref=login&ref=world&pagewanted=all.
[13] Khan and Pennington, "Mixed Emotions Greet Taliban Recruiters."
[14] "Stoned To Death," *The Guardian*, April 10, 1995, 9.
[15] Jennifer Griffin, "Mullahs Lie in Wait to Kill Jailed Convert," *The Observer*, May 14, 1995, 20.
[16] Ibid.
[17] Carlotta Gall, "At Border, Signs of Pakistani Role in Taliban Surge," *The New York Times*, January 21, 2007. Accessed May 18, 2007. http://www.nytimes.com/2007/01/21/world/asia/21quetta.html?&pagewanted=print.
[18] "Jihadis try to recruit students; 3 killed in clashes," *The Dawn*, March 27, 2007. Accessed December 6, 2007. http://www.dawn.com/2007/03/27/top4.htm.
[19] Steve Coll, *Ghost Wars: The Secret History of the CIA, Afghanistan, and Bin Laden, from the Soviet Invasion to September 10, 2001* (New York: Penguin Press, 2004), 478.
[20] Hassan Abbas, *Pakistan's Drift into Extremism: Allah, the Army and America's War on Terror* (Armonk, NY: M.E. Sharp, 2005), 201.
[21] "Who are the Kashmir militants?" *BBC News On-Line*, August 1, 2012. Accessed November 1, 2015. http://www.bbc.com/news/world-asia-18738906.
[22] Abbas, *Pakistan's Drift into Extremism*, 194.
[23] John Schmidt, *The Unravelling: Pakistan in the Age of Jihad* (New York: Farrar, Straus and Giroux, 2011), 94.
[24] Khan and Pennington, "Mixed Emotions Greet Taliban Recruiters."
[25] Ibid.
[26] Zahid Hussain, *Frontline Pakistan: The Struggle with Militant Islam* (New York: Columbia University Press, 2007), 30.
[27] Mehtab Ali Shah, *The Foreign Policy of Pakistan: Ethnic Impacts on Diplomacy, 1971-1994* (London: I.B. Tauris, 1997), 91.
[28] Laurent Gayer, *Karachi: Ordered Disorder and the Struggle for the City* (Oxford and New York: Oxford University Press, 2014), 26.
[29] Hussain, *Frontline Pakistan*, 14.
[30] Carlotta Gall, *The Wrong Enemy: America in Afghanistan, 2001-2014* (Boston and New York: Houghton Mifflin Harcourt, 2014), 43-45.
[31] Rizwan Hussein, *Pakistan and the Emergence of Islamic Militancy in Afghanistan* (Burlington, VT: Ashgate, 2005), 204.
[32] Abbas, *Pakistan's Drift into Extremism*, 194.
[33] Coll, *Ghost Wars*, 552.
[34] Daniel Markey, *Council on Foreign Relations, Special Report No. 36*, "Securing Pakistan's Tribal Belt" (New York: August 2008).
[35] Ibid.
[36] Schmidt, *The Unravelling*, 42.
[37] Ibid., 41.
[38] Hussein, *Pakistan and the Emergence of Islamic Militancy in Afghanistan*, 55.
[39] Frederic Grare, *Pakistan and the Afghan Conflict, 1979-1985* (Oxford, UK, and New York: Oxford University Press, 2003), 2-3.
[40] Ibid., 41.
[41] Ibid., 3.
[42] Hussein, *Pakistan and the Emergence of Islamic Militancy in Afghanistan*, 78.
[43] Ibid., 202.
[44] Schmidt, *The Unravelling*, 103.
[45] Gall, *The Wrong Enemy*, 45.
[46] James Mazol, "The Quetta Shura Taliban: An Overlooked Problem," *The International Affairs Review*, November 23, 2009. Accessed April 27, 2011. http://www.iar-gwu.org/node/106.
[47] Yusufzai, "Suicide Bomber Cult Alive and Well."
[48] Hussein, *Pakistan and the Emergence of Islamic Militancy in Afghanistan*, 202.
[49] Ibid., 226.
[50] Gall, *The Wrong Enemy*, 49.

Andrew Fraser is a Canadian attorney and independent scholar. He has previously published on the fall of the Arbenz regime in Guatemala, the role of the news media in the Korean War, and NATO operations in Afghanistan. He holds a master's degree in history from the University of Toronto, where he specialized in Cold War-era diplomatic history, and a master's degree in international affairs from the Norman Paterson School of International Affairs at Carleton University in Ottawa, where he specialized in global finance.

Analysis of 15 Cases and 15 Interviews: Lessons Learned from U.S. Forces in the Operational Environment

by Dr. Rad Malkawi

OVERVIEW

Unintentional violation of local norms and beliefs can aggravate a welcoming and hospitable community into becoming a hostile population as these unintentional actions can offend detainees as well as bystanders.[1] The February 6, 2006, Quadrennial Defense Review (QDR) states that the U.S. Department of Defense (DoD) "must dramatically increase the number of personnel proficient in key languages such as Arabic, Farsi and Chinese and make these languages available at all levels of action and decision – from the strategic to the tactical."[2] It is postulated that DoD "must foster a level of understanding and cultural intelligence about the Middle East and Asia comparable to that developed regarding the Soviet Union during the Cold War."[3]

At the general level for all cultural settings, "U.S. troops need cultural guidance to operate roadblocks and checkpoints, conduct searches, reconnoiter areas, ask questions of natives and interact with friendly native officials, soldiers and police."[4] Moreover, Jandora specified that "such guidance should include basic verbal and nonverbal communication aids, behavioral 'dos and don'ts,' precautions to be respectful towards Islam and instruction on: the importance of greetings (in a word-oriented culture); the avoidance of non-mission-related probing questions (in a culture that values propriety); the necessity of respecting women's privacy (in a culture where women are shielded); the necessity of avoiding affront to honor (in a culture where honor is of utmost value)."[5]

Misunderstanding culture at the strategic level can produce policies that exacerbate an insurgency and can lead to negative public opinion. Moreover, ignorance of the culture at a tactical level endangers both civilians and troops.[6]

INTRODUCTION

Before deployment, cultural training is primarily rooted in acculturation.[7] Through acculturation, the goal of cultural training prior to deployment is to prepare soldiers in both retaining original culture while at the same time contributing an integral part of the dominant culture.

After the terrorist attacks of September 11, 2001, the Pentagon initiated a number of new policies to increase national security and international communication. This resulted in a number of policies dealing with critical languages and international study for the purpose of improving national security in the coming years.[8]

This study involved the analysis of 15 research cases and 15 interviews with members of the United States military who have served in Vietnam, Korea, Germany, the Philippines, Iraq, Afghanistan, Bahrain, Saudi Arabia, and Kuwait. Moreover, this study was also aimed at identifying the positive and the negative impacts of teaching foreign cultures to members of the U.S. military.

Teaching culture is a pressing need across foreign language curricula, and this is even more true in Arabic since the crucial differences between the Arab culture and Western culture make the mutual understanding, based on linguistic knowledge alone, problematic. The importance of cultural knowledge becomes apparent, for example, in understanding the role of religion (particularly Islam) in daily interactions in the Arab World.[9] The soldiers' ability to communicate effectively while displaying respect for a population's values, customs, ethnicity, family, and religion is critical.[10] Cultural training is not new to the military; however, it has never received the necessary emphasis or resources required for soldiers to attain the cultural acuity required in the contemporary operational environment.[11]

LITERATURE REVIEW

The literature used in this research examined the theory and practice of teaching and learning culture associated with acculturation learning theory. There is much documentation of lessons learned from U.S. military operations in Iraq. These lessons highlighted a recurring theme of skills, additional training, and education that are and will continue to be required of soldiers operating and fighting in the long war. Some examples are the recognition of the need for improved language proficiency and cultural training which, over time, will build a more culturally capable force that is better able to create victory in a long war.[12]

Culture is most commonly viewed as the pattern of knowledge, skills, behaviors, and attitudes, as well as material artifacts, produced by a human society. In other words, culture includes people's intellectual, social, technological, political, religious, economic, moral, and aesthetic accomplishments.[13] The U.S. military exists to serve the American people, protect enduring national interests, and fulfill the nation's military responsibilities.[14] This means that DoD has to be prepared to develop a new team of leaders and operators (soldiers) who are comfortable working in remote regions of the world, dealing with local and tribal communities, adapting to foreign languages and cultures, and working with local networks to further U.S. and partner interests through personal engagement, persuasion, and quiet influence rather than through military force alone.[15]

Over the past 30 years, "The U.S. military has conducted operations in many countries such as Lebanon, Grenada, Panama, Somalia, Liberia, Haiti, Turkey, Bangladesh, Iraq, and Afghanistan."[16] The application of cultural intelligence and awareness on the ground in Iraq is essential to improving relations with the native population. A lack of officers cognizant of the native culture has led to countless misunderstandings and escalating violence between U.S. forces and the Iraqi insurgency.[17]

Unfortunately, U.S. soldiers lack adequate educational training regarding foreign cultures. They do not have all the proper tools necessary to deal with an insurgency and to work with the local population.[18] Numerous articles and reports prove how little American soldiers understand about the cultures of the countries in which they are currently fighting.[19] "The mission of soldier acculturation is too important to be relegated to last-minute briefings prior to deployment. Acculturation policy has to be devised, monitored, and assessed as a joint responsibility.[20]

METHODOLOGY

For this study, qualitative research was used to explore lessons learned by the U.S. military in the operational environment. The study was conducted in two phases: Phase I was an analysis of 15 published documents conducted by researchers about soldiers who have worked at the U.S. Military Academy, and have traveled oversees and interviewed Regular Army prisoners of war, U.S. combat troops, and embedded media.[21] Phase II was conducted through interviews of 15 military personnel who have served in Vietnam, Korea, Germany, the Philippines, Afghanistan, Iraq, Bahrain, Saudi Arabia, and Kuwait.

CASE STUDY FINDINGS

Phase I – Documented and Public Release Resources: The 15 research cases were investigated according to the following:

The political situation in foreign countries to understand how to reduce the high-profile attacks throughout the U.S. operating environment.

Case Study One: "Transforming the American Soldier: Educating the Warrior-Diplomat." Hudson and Warman accomplished this case study. This study analyzes the current problems and difficulties reported to be occurring while attempting to combat irregular forces in non-Western environments.[22]

Hudson and Warman cited numerous examples of the U.S. military's forceful practices that have served to alienate the Iraqi population and undoubtedly turned some "fence-sitters" into insurgents. For instance, there is misunderstanding of the terms "liberation" and "occupation," and how they have different and detrimental meanings politically, morally, and legally for the Iraqi people.[23]

Case Study Two: "The Importance of Cross-Cultural Awareness for Today's Operational Environment," This thesis was submitted in partial fulfillment of a Master of Strategic Studies Degree.[24]

Many members of the Coalition Provisional Authority (CPA) and Combined Joint Task Force 7 felt that anti-coalition and anti-American rhetoric was a threat to security and sought to stop its spread. Closing Muqtada al Sadr's *Al Hawza* newspaper contributed to an Iraqi perception that Americans do not really support freedom of speech despite their claims to the contrary, reinforcing the view of Americans as hypocrites. These points demonstrate how necessary it is that a cultural subject matter expert be required at least to explain the players and organizations and their motivations behind the actions.[25]

"Once the kinetic phase of the fighting in Iraq ended, soldiers and Marines found themselves immersed in an alien culture unable to differentiate friend from foe or to identify those within the population they could trust to provide useful and timely tactical intelligence. The military relied on intelligence-gathering tools and methods left over from the Cold War."[26] The military possessed the technological means in Iraq to conduct net-centric warfare with unparalleled proficiency. "But it lacked the intellectual acumen, cultural awareness, and knowledge of the art of war to conduct culture-centric warfare. When

the enemy adapts and finds ways to overcome the advantages of net-centric warfare, a focus on the art rather than the science of war becomes necessary to secure success."[27]

Case Study Three: "The Use of Culture in Operational Planning." Knowing the center of power for the Iraqis, for instance, Captain Ayers was responsible for providing security for Ramadi, a town in the Sunni Triangle.[28] In order to gain popular support, Captain Ayers discovered and established relationships with key people in the town. In Ramadi there is a confusing network of more than 100 tribes, subtribes, sheiks (tribal leaders), and sub-sheiks. Ayers enlisted the assistance of the local police force and established joint patrols and information sharing. Despite continuing attacks and punishment by the insurgents, Captain Ayers has gained and maintained a certain degree of loyalty and cooperation from the Ramadi people due to his cultural sensitivity and respect.[29]

Case Study Four: "The Military Utility of Understanding Adversary Culture." Montgomery McFate, a cultural anthropologist and a defense policy fellow at the Office of Naval Research working on an initiative to promote social science research in the national security area, published this study.[30]

At the operational level, the military misunderstood the system of information transmission in Iraqi society and consequently lost opportunities to influence public opinion. One Marine recently returned from Iraq noted, "We were focused on broadcast media and metrics. But this had no impact because Iraqis spread information through rumor. Instead of tapping into their networks, we should have visited their coffee shops."[31] Unfortunately, the emphasis on force protection prevented soldiers from visiting coffee shops and buying items to support the economy. Soldiers were unable to establish one-to-one relation-ships with the Iraqis, which are key to both intelligence collection and winning hearts and minds. A related issue was our squelching of Iraqi freedom of speech. Failure to understand adversary culture can endanger both troops and civilians at a tactical level. Although it may not seem like a priority when bullets are flying, cultural ignorance can kill.[32]

In 1998 the Office of Naval Research conducted a number of focus groups with Marines returning from Iraq. The Marines were quick to acknowledge their misunderstanding of Iraqi culture, particularly pertaining to physical culture and local symbols, and to point out the consequences of inadequate training. Most alarming were the Iraqis' use of vehement hand gestures, their tendency to move in one's peripheral vision, and their toler-ance for physical closeness. One Marine noted, "We had to train ourselves that this was not threatening. But we had our fingers on the trigger all the time because they were yelling." A lack of familiarity with local cultural symbols also created problems. For example, in the Western European tradition, a white flag means surrender.[33] Many Marines as-sumed a black flag was the opposite of surrender—"a big sign that said shoot here!" as one officer pointed out. As a result, many Shia who traditionally fly black flags from their homes as a religious symbol were identified as the enemy and fired at unnecessarily. There were also problems at roadblocks. The American gesture for stop (arm straight, palm out) means welcome in Iraq, while the gesture for go (arm straight, palm down) means stop to Iraqis. This and similar misunderstandings have had deadly consequences.[34]

CAPABILITY TO UNDERSTAND THE MAIN RELIGIOUS SECTORS IN FOREIGN COUNTRIES

Case Study Five: "United States Institute of Peace, Association for Diplomatic Studies and Training, Iraq Experience Project."[35] Plotkin interviewed retired USAID officer Lary Crandall, who had two tours in Iraq. His last assignment was a reconstruction program for Iraq.[36]

According to Plotkin, the religious culture in Iraq is a very important part of Iraqi culture. "People usually are very kind, they talk a lot about the religion, so you can learn a lot about this, and from this knowledge of religion, you know a lot about what the Arabic culture is, and the way Arab people are thinking about things and doing things. [Plotkin thinks] religion really has a deep impact on Iraqi people's life."[37] Christopher Varhola, a U.S. Army major and cultural anthropologist, argues that the U.S. military was unprepared for governing an Islamic nation.[38]

Varhola cites numerous examples of the U.S. military's forceful practices that have served to alienate the Iraqi population and undoubtedly turned some "fence-sitters" into insurgents. Here are a few examples of what the Army has not considered:

(1) American male soldiers searching Iraqi females—a highly disrespectful action that violates a family's honor and begs vengeance by the male family members.
(2) Arrests of religious leaders who preach against the coalition. Unwarranted arrest of religious leaders for what they say just leads Iraqis to believe Americans really do not believe in freedom of speech."[39]

According to Colonel (Ret) Leonard Wong, a research professor at the United States Army War College, strategic leaders must take it upon themselves individually and as

professionals to bear the responsibility for understanding the role culture plays in operations. "The Army's future leaders clearly need to be well versed in interacting with cultures outside American borders. The term 'cross-cultural savvy' refers to more than just the ability to work with non-U.S. militaries. This 'metacompetency' includes the ability to understand cultures beyond one's organizational, economic, religious, societal, geographical, and political boundaries."[40]

Learning Counterinsurgency

"Strong evidence suggests a need to better understand insurgencies and foreign cultures given the complex situations that have arisen today in both Afghanistan and Iraq."[41]

Case Study Six: "Operational Leadership Experiences in the Global War on Terrorism." Christopher K. Ives, a U.S. Army Major and cultural anthropologist, interviewed LTC John A. Nagl in support of the Operational Leadership Experiences Project at the Combat Studies Institute, Fort Leavenworth, Kansas.[42] LTC Nagl served as the operations officer for Task Force 1-34 Armor, part of the 1st Brigade Combat Team, 1st Infantry Division, during the battalion's September 2004 deployment to Iraq's volatile Anbar Province, during which he discovered an environment that was "far more difficult than [he] had imagined it could be."[43] In this email interview, Nagl discusses the often complicated intersection between counterinsurgency theory and practice, stressing among other things the need for far greater interagency presence and cooperation.[44]

During the Vietnam era, the defense community recognized that familiarity with indigenous, non-Western cultures was vital for counterinsurgency operations. In 1966, the British counterinsurgency in Malaya succeeded because it took account of tribal and ethnic distinctions, while similar U.S. efforts in Vietnam were bound to fail because they lacked anthropological finesse.[45]

Despite the fact that cultural knowledge has not traditionally been a priority within DoD, the ongoing insurgency in Iraq has served as a wake-up call to the military that adversary culture matters. As a returning commander from the 3rd Infantry Division observed: "I had perfect situational awareness. What I lacked was cultural awareness. I knew where every enemy tank was dug in on the outskirts of Tallil. Only problem was, my soldiers had to fight fanatics charging on foot or in pickups and firing AK-47s and RPGs [rocket-propelled grenades]." As this commander's observation indicates, understanding one's enemy requires more than a satellite photo of an arms dump. Rather, it requires an understanding of the enemy's interests, habits, intentions, beliefs, social organizations, and political symbols—in other words, their culture."[46]

Countering the insurgency in Iraq requires cultural and social knowledge of the adversary. Retired Admiral Admiral Arthur Cebrowski, Director of the Office of Force Transformation, noted that "the value of military intelligence is exceeded by that of social and cultural intelligence. We need the ability to look, understand, and operate deeply into the fault lines of societies where, increasingly, we find the frontiers of national security." However, we must also provide the commanders on the ground with "detailed information regarding local customs, ethnicity, biographic data, military geography, and infectious diseases." Producing intelligence on these factors can be challenging.[47]

Today's operating environment for successful counterinsurgency depends on attaining a holistic, total understanding of local culture. This cultural understanding must be thorough and deep to have practical success. "To defeat the insurgency in Iraq, U.S. and coalition forces must recognize and exploit the underlying tribal structure of the country, the power wielded by traditional authority figures, the use of Islam as a political ideology, the competing interests of the Shia, the Sunni, and the Kurds, the psychological effects of totalitarianism, and the divide between urban and rural, among other things."[48] "Understanding and working within the social fabric of a local area is initially the most influential factor in the conduct of counterinsurgency operations. This is often the factor most neglected by U.S. forces."[49]

The current deficit in cultural awareness and understanding insurgency results in the erosion of trust between the American soldier and indigenous populations.[50] This leads to difficulties while conducting military operations. The U.S. military lacks training in both the Arabic language and support activities such as local law enforcement, administration, and various reconstruction activities, all of which should be considered paramount in working with a host nation's population and countering insurgency.[51]

In order to defeat an insurgent force, U.S. forces must be able to separate the insurgents from the general population. At the same time, U.S. forces must conduct themselves in a manner that enables them to maintain popular domestic support. "The counterinsurgent reaches a position of strength when his power is embodied in a political organization issuing from, and firmly supported by, the population."[52]

There are numerous examples of the U.S. military's forceful practices that have served to alienate the Iraqi population and undoubtedly turned some "fence-sitters" into insurgents. Here are a few examples of what the Army has not considered:

- Detaining all the males in a given area for weeks or months on end without regard to legitimacy.
- Detaining family members of suspects in the hope that the suspects will turn themselves in.
- Using dogs, which Iraqis consider unclean animals, to search Iraqi homes, even though this is viewed as a disgrace by Arabs and an attack upon their honor.
- "Creating more enemies or at least hardening them when American soldiers place their boots on the heads of Iraqi captives, for Arabs consider such acts as inhumane and disgraceful. Soldiers must come to understand the values of honor, shame, and dignity in Arab social systems."[53]

Case Study Seven: "Innovation or Inertia: The U.S. Military and the Learning of Counterinsurgency." DoD "seeks to improve the U.S. military ability to conduct counterinsurgency. The U.S. military has typically paid little attention to the nature and requirements of counterinsurgency and stability operations."[54]

None of the elements of U.S. national power—diplomatic, military, intelligence, or economic—explicitly takes adversary culture into account in the formation or execution of policy.

In its history with counterinsurgency, the U.S. military has often adapted successfully with the lessons learned at the operation's close. DoD's attempts to overcome "institutional failures" began in earnest in 2004, when senior Pentagon officials came to recognize the situation in Iraq as a protracted insurgency rather than the death throes of a defeated field but failed to institutionalize the lessons learned. Subsequent institutional innovation has occurred on three levels. Conceptually, the U.S. military has gained a clearer understanding of counterinsurgency, a process fueled by the Iraq War and driven by a community of officers and civilians well-versed in these types of campaigns. Institutionally, counterinsurgency has come to be integrated with military training, education and planning.[55]

Case Study Eight: "Anthropology and Counterinsurgency: The Strange Story of their Curious Relationship." McFate states that "there is a lack of cultural awareness for the United States military members who have served in Iraq. Countering the insurgency in Iraq requires cultural and social knowledge of the adversary. Yet, none of the elements of U.S. national power—diplomatic, military, intelligence, or economic—explicitly takes adversary culture into account in the formation or execution of policy."[56]

Case Study Nine: "Cultural Intelligence and the United States Military." The Center for Advanced Defense Studies" (CADS) staff introduced the concepts of cultural awareness and how to apply cultural intelligence, and examined current challenges to their implementation in mainstream operations. The application of cultural intelligence and awareness on the ground in Iraq is essential to improving relations with the native population. "A lack of officers who are cognizant of the native culture has led to countless misunderstandings and escalating violence between US forces and the Iraqi insurgency."[57]

Negotiation Skills Training

Case Study Ten: "Preparing the American Soldier in a Brigade Combat Team to Conduct Information Operations in the Contemporary Operational Environment." Beckno introduces negotiation as a process that occurs when parties are trying to find a mutually acceptable solution to a complex conflict. Throughout Iraq, young Army and Marine captains have become veritable mayors of micro-regions, meeting with local sheiks, setting up waste-removal programs to employ young men, dealing with complaints about cuts in electricity and so on. They have learned to arbitrate without losing patience.[58]

Case Study Eleven: "Cultural Awareness and Negotiation Skills Training: Evaluation of Prototype Semi-Immersive System."[59] This study shows that the U.S. Army has recognized "the need to provide additional training and to better prepare soldiers for conducting bi-lateral engagements and negotiations. The Army has taken a number of steps to integrate this instruction during pre-deployment training."[60]

Case Study Twelve: "Negotiation in the New Strategic Environment: Lessons from Iraq."[61] This study demonstrates the experiences of U.S. Army and Marine Corps officers returning from Iraq. It integrates academic research on negotiation theory and practice with their experience on the ground.[61] U.S. soldiers in Iraq conduct thousands of negotiations with Iraqi leaders while pursuing tactical and operational objectives that affect the strategic import of the U.S. mission in that country. As long as U.S. troops operate under conditions like the ones they currently face, while at the same time conducting a counterinsurgency and stability, security, transition, and reconstruction (SSTR) operation in Iraq, negotiation will be a common activity and an important part of achieving mission objectives. Lessons from experience negotiating in Iraq can be helpful in future operations.[62]

A significant majority of the officers interviewed highlighted the importance of understanding the context. "One Marine officer who served as the commander of an Iraqi army base near Tall Afar, Iraq, and negotiated often with a local sheik noted that, "If you didn't have a good understanding of the situation, you were flatfooted. . .[and] could be easily taken advantage of, manipulated, or maybe unintentionally promise something that you couldn't deliver on. . ." It was critical, he said, that he have a thorough understanding of the entire situation, and not just his own position. He believes that his success was limited in a series of negotiations with a local sheik over the use of equipment needed to enhance security at his base, because the sheik may not have been the right person to talk to or may not have been someone who could be trusted."[63]

Most of the officers interviewed felt they were not prepared to negotiate in Iraq, but during their time there, they adapted and learned. Many already knew or learned effective lessons in Iraq; some seemed to learn the wrong lessons, diminishing their negotiating effectiveness.[64]

One officer noted the importance when negotiating in Iraq of "letting your counterpart know that you understand the dynamics of the situation. If he was trying to take advantage of you, it causes him to lose face because the deception is brought out into the open. All negotiations pose a risk of one party taking advantage of another poorly informed party."[65] All of the U.S. officers interviewed emphasized the importance of understanding the cultural differences that exist between U.S. soldiers and Iraqis. Several officers believed that personality was as likely to have as powerful an effect on a negotiation as culture.[66] The examples discussed above demonstrate the complex realities that soldiers face when they are deployed, and they have to negotiate with civilians outside their areas of expertise and training.[67]

Case Study Thirteen: "From Peddlers to Sheiks: A Contracting Case Study in Southern Baghdad." Verdon conducted this case study, deployed to Baghdad, Iraq, in 2007-2008 to serve as a cultural advisor and social researcher for the U.S. Army.

A sheik's (Tribal Leader) legacy, as defined by those Verdon interviewed in the field, depends on where he resides, how he becomes a sheik, and how much respect he has from his people.

> Referring to an incident involving the disappearance of a local Shi'ite, one Sunni sheik complimented coalition forces for allowing sheiks to handle the matter according to local customs. "It is best to allow tribes to settle problems," commented one sheik, who then added: "It is better that you allowed us to go on the patrol to seek the truth." Striking a balance between the mores of coalition forces and of Iraqi tribes is necessary. Sheiks generally prefer to resolve issues amongst themselves through consensus and by an informal "gentlemen's agreement."[68] One sheik commented, "Americans don't understand something: all people respect the sheiks and will follow him no matter what he says and regardless of where he resides.[69]

According to McFate, most U.S. soldiers are not trained to understand or operate in foreign cultures and societies. One U.S. Army captain in Iraq said, "I was never given classes on how to sit down with a sheik. . . He is giving me the traditional *dishdasha* and the entire outfit of a sheik because he claims that I am a new sheik in town so I must be dressed as one. I don't know if he is trying to gain favor with me because he wants something [or if it is] something good or something bad."[70]

A Marine commander stationed near Tall Afar noted that, without appreciating the culture, the nuances of cultural difference between Americans and Iraqis, and the role within Iraqi culture of the sheik and tribe, "you fail at whatever you need to do"[71] Cultural differences have sometimes created misunderstanding and even disgust on both sides of U.S.-Iraqi interactions. A civil-military relations officer assessing the general prerequisite of trust in Iraqi culture acknowledged that "[t]here is not a lot of trust between men in a place like Iraq. However, the appearance of trust (or the societal obligation to demonstrate trust) is almost as powerful as trust itself."[72]

Significant Changes of United States Military Procedures in Foreign Countries

"The military's reputation greatly depends on its past performance. Many of the mistakes that have been made in Iraq that are the consequence of cross-cultural misunderstanding have decreased trust in the military and have set a precedent for mistrust based on reputation."[73] Hudson and Warman analyze the current problems and difficulties reported to be occurring while attempting to combat irregular forces in non-Western environments.[74]

"Major General (Ret) Robert Scales argues that some of the problems the U.S. military is facing in places like Iraq and Afghanistan are the result of an over-reliance on technology, combined with a lack of cultural understanding of the local population motivation."[75] Moreover, according to Scales, "We need to be able to understand the non-military advantage, to read intentions, to build trust, to convert opinions, to manage perceptions—all tasks that demand an exceptional ability to understand people, their culture and their

motivation."[76] The U.S. military has engaged in combat operations in Iraq; this environment did not present a conventional battlefield.

[Editor's Comment: MG Bob Scales is a highly respected former Commandant of the U.S. Army War College in Carlisle Barracks, PA. During his distinguished military career and ever since retiring from the Army, he has been a prolific writer and researcher on military strategy and doctrine issues.]

The U.S. military usually receives little instruction as to the nuances of the local culture prior to its deployment. Although some information is provided, it usually consists of merely the basic statements in bullet form, such as: "avoid showing the bottom of your foot in mid-eastern countries," or "don't stare at women," and listing hand gestures that are considered taboo. Although these simple warnings are an effective way to get out the basic information and can be useful for soldiers who are traveling through a foreign country or region, they merely provide superficial sensitivity training, and their only aim is for soldiers to avoid offending the population.[77] In practice, it is difficult to translate such warnings into effective cross-cultural understanding, especially while conducting military operations for an extended period of time in varied combat conditions.

> An example of the difficulties faced when trying to translate cultural awareness statements into proper application of tactics in an operation is when soldiers in Iraq were using dogs to help search houses. Although soldiers might realize that the Iraqis didn't "like" dogs, what they might not realize is that the vast majority of Iraqis don't just "not like" dogs, but instead consider them an "unclean" animal and bringing them into houses was considered disgraceful. Another example of tactical difficulties based on a misunderstanding of culture is when American male soldiers search Iraqi women. Although tactically it might be necessary, it is considered a highly disrespectful action that violates the honor of a family and begs vengeance. These examples, as previously mentioned, indicate just some of the problems that can lead to further alienation of the population, and an additional erosion of trust. It is very difficult to trust someone, let alone an organization, that violated your family's honor or disgraced your home. As a result, United States military actions are eroding the trust of the Iraqi people in the Coalition.[78]

Recently, some changes in arrest techniques have been implemented by some units which incorporate an understanding that insulting or humiliating locals while arresting them has the tendency to do more harm than good. According to U.S. Army Major General Peter Chiarelli, then Commander of the 1st Cavalry Division stationed in Baghdad, "The worst thing in the world is to put him on the ground and put your boot on his head. Honor is so critical in this society. You don't take away a man's honor. Although some changes are being undertaken in some units, the argument can be made that too much damage has already been done"[7] [Editor's Note: After the war, Chiarelli rose to 4-star rank and served as Vice Chief of Staff of the Army prior to retiring. A quarter century earlier, this editor, at the time a MAJ, and then-CPT Chiarelli taught political science together to cadets at the U.S. Military Academy, where we did our best to try to instill an appreciation for cultural awareness.]

Case Study Fourteen: "DoD News Briefing from Iraq with Colonel Gregory Lusk, commander, 30th Heavy Brigade Combat Team, Multi-National Division." Colonel Lapan (director of Press Operations, DoD) interviewed COL Lusk via teleconference from Iraq.[80] COL Lusk explained the mission of U.S. troops: "Our mission here in Iraq is to secure the population of those that reside within our operating environment, in order to support and enhance the continued development of Iraqi civil capacity."[80] Lusk put a lot of emphasis on the importance of developing a good relationship with the local population of Iraq. "Despite the seemingly large numbers of security forces, the maintaining of hard-earned security gains would not be possible without the support of the people. Many have become our good friends and indeed they often invite us into their homes in order to share a meal, a cup of chai or just simply casual conversation."[81] "This fruitful and productive relationship with Iraqi security force partners has resulted in the reduction of capabilities for al Qaeda in Iraq operating within operating environment, as well as the reduction in capacity of former special groups and other rejectionists." "We have reduced the high-profile attacks throughout our operating environment."[82] "As long as we are here, we, in support of our Iraqi security force partners, will continue to take the fight to the enemy."[83]

Case Study Fifteen: "Army Transformation: Implications for the Future." Major General Robert Scales, USA (Ret). This study demonstrates the importance of cultural awareness for U.S. military members.[84]

"U.S. forces have spent billions to gain a few additional meters of precision, knots of speed or bits of bandwidth. Some of that money might be better spent in improving how well our military thinks and studies war in an effort to create a parallel transformational universe based on cognition and cultural awareness.[85] Implementing only a few of these initiatives will go a long way to creating an

environment conducive to fighting an enemy in this emerging era of culture-centric warfare. A military all too acculturated to solving war-fighting problems with technology alone should now begin to recognize that wars must be fought with intellect. Reflective senior officers returning from Iraq and Afghanistan have concluded that significant advantage can be achieved by out-thinking rather than out-equipping the enemy. This means that wars are won as much by creating alliances, leveraging non-military advantages, reading intentions, building trust, converting opinions and managing perceptions, all tasks that demand an exceptional ability to understand people, their culture, and their motivation.

A military all too acculturated to solving war-fighting problems with technology alone should now begin to recognize that wars must be fought with intellect.

Clearly, these imperatives place an increased premium on the ability of America's military to understand the nature and character of war as well as the cultural proclivities of the enemy. Yet, increasingly military leaders subordinate the importance of learning about war to the practical and more pressing demands of routine day-to-day operations. Today's military has become so overstretched that it may become too busy to learn at a time when the value of learning has never been greater.[86]

One division commander in Iraq told Scales that his greatest worry was that his soldiers comprised "an army of strangers in the midst of strangers." During the early months of occupation, cultural isolation in Iraq created a tragic barrier separating Iraqis of good will from the inherent goodness that American soldiers demonstrated so effectively during previous periods of occupation in such places as Korea, Japan, and Germany.[87]

Few members of the armed forces are familiar with the cultural traditions of the countries in which they operate. Yet, violation of local norms and beliefs can turn a welcoming population into a hostile mob. Iraqis arrested by U.S. troops have had their heads forced to the ground—a position forbidden by Islam except during prayers. This action offends detainees as well as bystanders.[88]

Tribal Economics and Corruption

Retired USAID officer Crandall raised some issues, including the level of corruption among the Iraqis, the error of the total exclusion of Baathists from the reform process, and the difficulty of recruiting the best officers to serve in Iraq due to security and career concerns.[89]

Verdon in 2007-2008 explored the social phenomena of Iraqis in regard to local customs, conflict resolution, economics, and political and kinship organization.[90] "This assignment required working directly with operational commanders to offer opinions and to make suggestions based on field observations, extensive experience in the Middle East, and prior military service. The goal was to provide an insider's view through the lens of social anthropology, analyzing data from a two-fold cultural perspective: U.S. military and Iraqi."[91] Because the BCT's priority was reconciliation, this research focuses on tribal behavior within this context, and it highlights reconciliation and an apparent economic upturn. Reconciliation is defined as a measured reduction in violence achieved through peaceful means, whereby security, political processes, humanitarian efforts, and infrastructure improvements can be transitioned to the Iraqis. "However, there is a causal relationship between reconciliation contracting and violence: good contracting decisions reduce violence and promote reconciliation; bad contracting decisions can have the opposite effect."

While in the field, Verdon asked the following questions:

- Are we challenging long-standing tribal power structure by contracting with the "wrong" tribe, brother, or cousin?
- Are our contracting decisions based on Western values that can cause long-term damage to the fragile elements of reconciliation?
- With whom do we form alliances to build a sustainable future?[92]

Verdon provided a detailed analysis to answer the above questions. She offered an Arabic idiom to reveal this dilemma: "My brother and I are against our cousin, but my cousin and I are against a stranger."[93] A result of this proverb is: eliminate the stranger through reconciliation. Then, cousins fight against one another when power, strongly connected to the values of honor and shame, is challenged. "Eliminating one threat may bring about another, which may jeopardize U.S. alliances with the sheiks."[94] If this occurs, a competitor or conspirator may vie for support from the tribes. She added the cooperation we share with the tribes should never be assumed to be absolute. To maintain strong relationships, it is vital that the U.S. military commanders understand the cultural, political, and economic contexts that influence Iraqi tribal behaviors.[95]

Tribal leaders or sheiks put heavy efforts into maintaining their power and prestige, especially within their own tribes. When U.S. military forces directly award contracts to lesser tribesmen, sheiks react swiftly to stop any challenge to their authority. Tribal leaders protect the foundations of their power as manifested through influence connection, or "wastah," and reputation, or "wasl." Sheiks feel they are

entitled to control the contracts awarded to members of their tribes. Controlling such resources secures the sheik's wasel and gives the sheik power; sheiks maintain their dominance by leveraging their wastah to diminish the threat of an opponent. The U.S. military should consider to whom contracts are rewarded so as to avoid any disruption to the tribal balances of power. Contracting agents who see the sheiks as corrupt individuals would prefer to deal with the more straightforward approach of a non-sheik. Often in tribal cultures, however, the more straightforward and transparent person engaging the coalition one-on-one is often a person with less power and influence in his community.[96]

The U.S. Marine Corps Center for Advanced Operational Culture Learning (CAOCL) ensures Marines are equipped with operationally relevant regional, culture, and language knowledge to allow them to plan and operate successfully in the joint and combined expeditionary environment, in any region of the world in current and potential operating conditions.[97] The U.S. Air Force also recognizes the need for its airmen to be culturally in tune with today's operating environment. The Air Force University Culture and Language Center supports the Expeditionary Air Force by providing airmen at all ranks with the best available understanding of foreign cultures and the competencies to communicate and collaborate effectively with members of foreign societies.[98]

INTERVIEW FINDINGS

Implementation of Cultural Understanding

The first thematic category was labeled implementation of cultural understanding. The thematic category pertained to the different methods of cultural understanding implementation to which the U.S. troops were exposed. The thematic category produced nine unique codes, with general pre-deployment training (ten out of fifteen participants, 67%) receiving the most responses from the sample. Table 1 contains all the codes that emerged from the data.

Table 1

Codes for Implementation of Cultural Understanding

Codes	# of participants to offer this experience	% of participants to offer this experience
General pre-deployment training	10	67%
Language training	2	13%
Combat experience	2	13%
Personal research	2	13%
Religion	1	7%
Culture	1	7%
Observation	1	7%
Psychology	1	7%
Mentorship	1	7%

Most of the participants reported that they were exposed to pre-deployment training, which covered general training about the culture of the country of interest. Participant 1 explained the different topics covered in the pre-deployment training:

> Implementation of Arabic Culture Awareness is conducted down to the lowest soldier level prior to deployment. This is accomplished by presentations made (usually by the unit's intelligence officer) that address the tribal factors prevalent in Arabic society, the relationships and importance of family in the Arab World, the history of the Arab World within the context of its relationship with Western interactions (e.g., the Crusades, trade, current events), and finally important facts to know about Islam (key dates, holidays, prominent figures, etc.). Every soldier is usually given a "Smart Card," A foldable brochure that can easily be carried in the pocket and highlights key phrases in Arabic plus highlights on culture, to include culturally-specific hand gestures.

Participant 2 reported that pre-deployment training usually covers broad topics such as the day-to-day practices that need to be familiarized; however, longer courses were available focusing on language. Participant 2 shared:

> Pre-deployment training covers aspects of the culture in a broad sense. The classes range from some key small phrases for interacting with the culture in a day-to-day basis, basic dos and don'ts, indigenous wildlife, etc. This training is at the operational level for military occupational specialties whose main mission is not interaction with the local population. Further training is provided for those who need a working understanding of the culture. Lengthier courses, which focus on language, also develop a clear understanding of the culture, its interactions, and its traditions from topics such as religion to cuisine.

Participant 13 explained the troops were exposed to minimal pre-deployment training about cultural awareness, which he believed was insufficient. Participant 13 explained:

> In my Army experience, there was no clear stepping-stone process for learning about the positive and negative aspects of the Arabic culture prior to deployment to Operation IRAQI FREEDOM. However, the Army did put my unit through training scenarios at the Joint Readiness Training Center at Fort Polk, and we were required to attend a short training session on cultural awareness prior to deployment to Iraq. There were no unit roles or was there a coordinated stepping-stone process into the learning of the Arabic culture prior to our departure

for Iraq. I will say that the training improved slightly, but was nowhere near where it should have been in my opinion after spending 26 months in Operation IRAQI FREEDOM.

Areas of Improvement

The second thematic category was labeled areas of improvement. The thematic category pertained to the areas of cultural awareness that were experienced negatively by the participants during deployment, suggesting that improvement might be necessary. Some of the responses include cultural communication (four out of fifteen participants, 27%) and cultural sensitivity (two out of fifteen participants, 13%). Table 2 contains all the codes that emerged from the thematic category of areas of improvement.

Table 2

Codes for Areas of Improvement

Codes	# of participants to offer this experience	% of participants to offer this experience
Cultural communication	4	27%
No response	3	20%
Cultural sensitivity	2	13%
Purpose of military	1	7%
Practices of the native	1	7%
Application	1	7%
Television	1	7%
Civilians	1	7%
Flexibility	1	7%

The results of the study indicated that cultural communication is an area relevant to cultural awareness that needs to be improved. Participant 1 spoke about further developing the cultural sensitivity of the troops, an area that he found still to be lacking,

I have seen the opposite of support in cultural sensitivity in other units. When this occurs, people have a tendency to brand others as liars, greedy, or insurgents. The Arab World is far too complex to paint such a general picture of someone who may exaggerate, ask for money, or have links to insurgent/criminal groups. Sadly, it is more the norm than the exception that military commanders fail to realize.

Participant 7 spoke about the benefits of formalization of cultural sensitivity training in schools:

> It should be taught in schools about different cultures. They teach in the language and the culture of a country we might be transferred to. So we know ahead how they live and how they dress. It's a whole different ball game.

CONCLUSIONS

This qualitative research, using case studies and interview data, proved to be the best for exploring the lessons learned by the U.S. military in an operational environment. The results indicate that the government policies that are not only designed appropriately, but also implemented properly, are key aspects in improving the cultural understanding programs for U.S. soldiers. The researcher recommends increased training in negotiation and offers practical recommendations for how officers can improve their negotiating outcomes and how military trainers can supplement pre-deployment training to ensure that military leaders deploy with the skills and practice they need for the 21st century operating environment. Dedicating more time during pre-deployment training to preparing these leaders to negotiate will allow for training in techniques, methods, and theory that are important for lasting effectiveness and mission success.[99]

The results of the case study analysis underscored the significance of cultural knowledge and awareness during deployment, an area that remains to be a weakness under U.S. policy. None of the elements of U.S. national power—diplomatic, military, intelligence, or economic—explicitly takes adversaries' culture into account in the formation or execution of policy. Failure in cultural awareness can manifest itself in terms of tactical failure endangering both the lives of the civilians and the troops.

The cultural awareness needs to be much more comprehensive because many countries are structurally diverse and complex. In Iraq, for instance, the underlying tribal structure of the country; the power wielded by traditional authority figures; the use of Islam as a political ideology; the competing interests of the Shia, the Sunni, and the Kurds; the psychological effects of totalitarianism; and the divide between urban and rural underscore the complexity of the culture. A general cultural training program does not take into consideration these inherent complexities. The civilians also play a role in a successful tactical mission, an area that is often missed in training policies and cultural awareness programs. Violations of local practices and norms could have repercussions for local relations.

The case study analysis showed that religion can be a key aspect in understanding the culture of one country, particularly in the Middle East. There is indication that the military is not yet equipped with the cultural knowledge to be fully operational in an Islamic state. Many U.S. soldiers are not trained to understand or operate in foreign cultures and societies, resulting in inadvertent forms of miscommunication.

The results of the interview component of the study seem to validate the results of the case study analysis. Even though tactical and strategic implications of cultural awareness were discussed by the participants in the interview as integral in the success of their missions, the participants also highlighted the importance of having relations with the civilians that are culturally sensitive. There seems to be a perception among the interview participants that the manner in which the troops relate with the locals is insufficient.

The current cultural awareness training programs are only effective in providing a brief overview of the culture...

The interview results also validated that the current pre-deployment training is superficial in nature, covering only basic cultural information. This kind of training often overlooks the complexity of what the country is really about from a cultural standpoint. The current cultural awareness training programs are only effective in providing a brief overview of the culture; however, the participants in the study seem to agree that more in-depth training needs to be implemented.

Learning the language and immersion strategies appears to be a suggestion that could help improve the cultural awareness of the troops. Cultural communication is a valuable aspect of the life of troops during deployment, and these two strategies would be able to improve the performance of the troops. The results of the case study and interviews revealed the significance of cultural knowledge during combat operations. It is the aspect of military operations that is often overlooked in favor of technological prowess.

NOTES

[1] Arcuri, A.P., & Ulrich, M.P. (2007). *The importance of cross-cultural awareness for today's operational environment*. Master's thesis, U.S. Army War College, Carlisle Barracks, PA.
[2] Ibid., 21.
[3] Ibid.
[4] Jandora, J.W. (2006). Military cultural awareness. *The Landpower Essay* 6(3), 1-8. Ladson, 3.
[5] Ibid.
[6] Ibid.
[7] Durlach. P.J., Wansbury, T.G., & Wilkinson, J.G. (2008). Cultural awareness and negotiation skills training: Evaluation of prototype semi-immersive system. Retrieved from DTIC website: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=AD A505896&Location=U2&doc=GetTRDoc.pdf.
[8] Edwards, D., Lenker, A., & Kahn, D. (2009). National language policies: Pragmatism, process, and products, joint national committee for languages, national council for languages and international studies. Retrieved from DocStoc.com website: http://www.docstoc.com/docs/93935378/NATIONAL-LANGUAGE-POLICIES-PRAGMATISM_-PROCESS_-AND-PRODUCTS.
[9] Albirini, A. (2009). Using technology, literature and guest speakers to raise the cultural awareness of Arabic language learners. *The International Journal of Language Society and Culture* 28, 1-15.
[10] Beckno, B.T. (2006). *Preparing the American soldier in a brigade combat team to conduct information operations in the contemporary operational environment*. Master's thesis, Fort Leavenworth, KS.
[11] Ibid.
[12] Ibid.
[13] Pai, S., & Adler, S. (2001). *Cultural foundations of education* (3rd ed.). Upper Saddle River, NJ: Prentice-Hall, Inc.
[14] Beckno, B.T. (2006). *Preparing the American solider in a brigade combat team to conduct information operations in the contemporary operational environment*.
[15] Ibid.
[16] Jandora, J. (2004). Military cultural awareness, 3.
[17] Center for Advanced Defense Studies (CADS) Staff. (2006). *Cultural intelligence and the United States military the center for advanced defense studies (CADS) staff*. Retrieved from CADS website: http://www.c4ads.org/files/cads_report_cultint_jul06.pdf.
[18] Hudson, J.D., & Warman, S.A. (2005). *Transformation of the American Soldier: Educating the Warrior-Diplomat*. Master's thesis, Naval Postgraduate School, Monterey, CA. Hussain, J.H. (2010). *Lessons for American companies in adapting to local cultures: A case study of education in Bahrain*. Doctoral dissertation, University of Northumbria, Newcastle, UK.
[19] Ibid.
[20] Scales, R. (2004). *Army transformation: Implications for the future, statement of Major General Robert Scales, USA (Ret)*. Retrieved from http://www.au.af.mil/au/awc/awcgate/congress/04-07-15scales.pdf, 20.
[21] Wong, L, Kolditz, T.A., Millen, R.A., & Potter, T.M. (2003). Why they fight: Combat motivation in the Iraq war. Retrieved from *Small Wars Journal* website: http://smallwarsjournal.com/documents/uckocoin.pdf.
[22] Hudson, J.D., & Warman, S.A. (2005). *Transformation of the American Soldier: Educating the warrior-diplomat*. Master's thesis, Naval Postgraduate School, Monterey, CA. Hussain, J.H. (2010). *Lessons for American companies in adapting to local culture cultures: A case study of education in Bahrain*.
[23] Ibid.
[24] Arcuri, A.P., & Ulrich, M.P. (2007). *The importance of cross-cultural awareness for today's operational environment*.
[25] Ibid.
[26] Ibid., 11
[27] Ibid.
[28] Bledsoe, E.E. (2005). *The use of culture in operational planning*. Master's thesis, Fort Leavenworth, KS.
[29] Ibid.
[30] McFate, M. (2004). The military utility of understanding adversary culture. *Joint Force Quarterly* 38, pp. 42-48.
[31] Ibid.
[32] Ibid.
[33] Ibid.
[34] Ibid.
[35] Plotkin, L. (2004). *United States institute of peace, association for diplomatic studies and training, Iraq experience project*. Retrieved from USIP website: http://www.usip.org/files/file/resources/collections/histories/iraq/crandall.pdf, on March 28, 2010, p. 10.
[36] Ibid.

[37] Ibid.
[38] Hudson, J.D., & Warman, S.A. (2005). *Transformation of the American Soldier: Educating the Warrior-Diplomat*. Master's thesis, Naval Postgraduate School, Monterey, CA. Hussain, J.H. (2010). *Lessons for American companies in adapting to local cultures: A case study of education in Bahrain*.
[39] Ibid.
[40] Arcuri, A.P., & Ulrich, M.P. (2007). *The importance of cross-cultural awareness for today's operational environment*, 15.
[41] Hudson & Warman, *Transformation of the American Soldier: Educating the Warrior-Diplomat*, 45.
[42] Ives, C.K. (2007). *Interview with LTC John A Nagl*. Retrieved from http://www.au.af.mil/au/awc/awcgate/army/csi_nagl_interview.pdf, 3.
[43] Ibid.
[44] Ibid.
[45] McFate, M. (2004.). The military utility of understanding adversary culture, 43.
[46] Ibid.
[47] Arcuri, A.P. & Ulrich, M.P. (2007). *The importance of cross-cultural awareness for today's operational environment*, 7.
[48] Ibid.
[49] Ibid.
[50] Hudson & Warman, *Transformation of the American Soldier: Educating the Warrior-Diplomat*.
[51] Ibid.
[52] Beckno, *Preparing the American solider in a brigade combat team to conduct information operations in the contemporary operational environment*, 2.
[53] Hudson & Warman, *Transformation of the American Soldier: Educating the Warrior-Diplomat*, 23.
[54] Ucko, D. (2008). *Innovation or inertia: The U.S. Military and the learning of counterinsurgency*. Retrieved from *Small Wars Journal* website: http://smallwarsjournal.com/documents/uckocoin.pdf, 290.
[55] Ibid.
[56] McFate, M. (2005). Anthropology and counterinsurgency: The strange story of their curious relationship, *Military Review*, 24.
[57] Center for Advanced Defense Studies, *Cultural intelligence and the United States Military, the Center for Advanced Defense Studies (CADS) staff*.
[58] Beckno, *Preparing the American solider in a brigade combat team to conduct information operations in the contemporary operational environment*, 46-47.
[59] Durlach, Wansbury, & Wilkinson, Cultural awareness and negotiation skills training: Evaluation of prototype semi-immersive system, 1.
[60] Ibid.
[61] Tressler, D.M. (2007). *Negotiation in the new strategic environment: Lessons from Iraq*. Retrieved from: Strategic Studies Institute website: http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB792.pdf.
[62] Ibid., 19.
[63] Ibid.
[64] Ibid.
[65] Ibid., 21.
[66] Ibid.
[67] Ibid.
[68] Verdon, L.A. (2009). From peddlers to sheiks: A contracting case study in Southern Baghdad, *Military Review*, 54-55.
[69] Ibid.
[70] McFate, Anthropology and counterinsurgency: The strange story of their curious relationship, *Military Review*, 25.
[71] Tressler, *Negotiation in the new strategic environment: Lessons from Iraq*, 25.
[72] Ibid.
[73] Hudson & Warman, *Transformation of the American Soldier: Educating the Warrior-Diplomat*, 30.
[74] Ibid.
[75] Ibid., 28.
[76] Ibid.
[77] Ibid., 1-2.
[78] Ibid., 29.
[79] Ibid., 31.
[80] Lapan, D. (2009). *DOD news briefing from Iraq with Col. Gregory Lusk, commander, 30th Heavy Brigade Combat Team, Multi-National Division – Baghdad*. Retrieved from http://dr15.ahp.dr1.us.army.mil/images/stories/Press_briefings/2009/november/091110lusk.pdf, 2.
[81] Ibid., 3.
[82] Ibid., 4.
[83] Ibid.
[84] Scales, R. (2004). *Army transformation: Implications for the future, statement of Major General Robert Scales, USA (Ret)*. Retrieved from http://www.au.af.mil/au/awc/awcgate/congress/04-07-15scales.pdf.
[85] Ibid., 2.
[86] Ibid.
[87] Ibid., 3.
[88] Arcuri, A.P., & Ulrich, M.P. (2007). *The importance of cross-cultural awareness for today's operational environment*, 7.
[89] Plotkin, L. (2004). *United States institute of peace, association for diplomatic studies and training, Iraq experience project*.
[90] Verdon, L.A. (2009). From peddlers to sheiks: A contracting case study in Southern Baghdad. *Military Review*.
[91] Ibid., 50.
[92] Ibid.
[92] Ibid.
[93] Ibid., 50-51.
[94] Ibid., 51.
[95] Ibid.
[96] Ibid.
[97] Arcuri, A.P., & Ulrich, M.P. (2007). *The importance of cross-cultural awareness for today's operational environment*, 15.
[98] Ibid.
[99] Tressler, *Negotiation in the new strategic environment: Lessons from Iraq*, 8.

Dr. Rad Malkawi has more than fourteen years teaching experience at several universities in the U.S. and in the Middle East, such as University of Wisconsin, University of Tennessee, Prince Mohamad University, and Jordan University of Science and Technology. He holds two doctoral degrees, one in Educational Leadership from Argosy University in San Francisco, CA, and the other in Archaeology and Art History from Kaslik University in Lebanon. He works as a trainer in leadership and soft skills for several academic institutions in Jordan and Saudi Arabia. Jordanian by birth, he is a U.S. citizen and taught Arabic for five years at the Defense Language Institute.

Imagining a National Intelligence Strategy for the Age of Information Warfare

by Zachary L. Young II

[Author's Note: The views and opinions expressed herein are those of the author alone, and do not necessarily reflect the official policy or position of the National Intelligence University, the Department of Defense, the U.S. Intelligence Community, or the U.S. Government.]

INTRODUCTION

Of the four elements in the traditional "DIME" model of national power, *information* is the least well understood. It lacks the formal structure of *diplomatic* power, the directness of *military* power, or the quantifiable nature of *economic* power. When used as an instrument of national power, the purpose of information is to influence foreign audiences or governments to act in ways that advance the interests of the United States. As with any other exercise of power, information power requires clear objectives, without which there can be no intentional action, and thus no strategy. With those objectives, it is possible to build a strategy using intelligence about ourselves, our audience, and the channels through which we communicate to employ properly the various means at our disposal. A failure to define objectives or specify means to achieve them is the hallmark of insufficient strategy.

The structure and mission priorities of the United States Intelligence Community (IC) reflect the *National Intelligence Strategy*, which provides a blueprint for how the IC will contribute to national security. The 2014 *National Intelligence Strategy* (NIS) was insufficient with respect to supporting national information power. This was due to a succession of *National Security Strategies* that were silent, incomplete, or misguided in their thinking, leading to a flawed strategic treatment of information power. The 2017 *National Security Strategy* (NSS) showed some improvement on this score. However, IC leaders failed to grasp the opportunity to improve the situation and build on the 2017 NSS with the 2019 NIS, which carries over the same structure and very similar language from the 2014 iteration. The current NIS, like the previous version, has four topical "mission objectives" that cut across the foundational intelligence missions of Strategic Intelligence, Anticipatory Intelligence, and intelligence support to Current Operations. Adding "Information Advantage" to the four topical missions could have positioned the IC to provide strategic and anticipatory intelligence that informs strategy and enhances current operations, such as they exist. Ideally, this new mission would build upon a *National Security Strategy* that recognized the value and necessity of Information as an instrument of national power. A reformed NIS might also provide guidance for structural reforms to enhance mission effectiveness. This is necessary because, as John Arquilla wrote in 2007, "Skillful information strategy is likely to prove the difference between victory and defeat."[1] By examining previous iterations of the NSS, lessons from the past reveal themselves and inform potential updates to both the NIS and NSS.

According to its own language, the NIS works "in support of" the NSS and is to be read alongside the National Intelligence Priorities Framework (NIPF) and the Unifying Intelligence Strategies (UIS).[2] This article examines the 2015 NSS under the assumption that its strategic framework has much in common with the 2014 NIS. It assumes a certain degree of continuity between the 2010 NSS and the 2015 version, with the 2014 NIS appearing toward the end of the period between the two. The article then looks back at the example provided by the very first NSS, released in 1987, which was crafted by an administration for which information power was a potent weapon of the Cold War. The treatment of information power in the 2017 NSS is examined to provide context for how the IC might support current strategic thinking in a new NIS. The NIS is updated every "four to five years," which means the next one is not due until 2023 or 2024.[3] Once the context provided by the previous NSSs is clear, this article identifies the problems of the 2014 NIS, which carried forward into 2019, and makes suggestions for how the next NIS could better support creation and use of national information power, including some ideas for IC structural reform.

INFORMATION POWER AND THE NATIONAL SECURITY STRATEGIES

The 2015 National Security Strategy

Both the 2014 NIS and the 2015 NSS bear the signs of what management professor Richard Rumelt called "bad strategy." In 2011 Rumelt described his four hallmarks of bad strategy as the following: failure to face the problem, mistaking goals for strategy, bad strategic objectives, and "fluff," or imprecise language used to avoid the hard work of thinking through problems. According to Rumelt, "Bad strategy covers up its failure to guide by embracing the language of broad goals, ambition, vision, and values."[4] Both the NIS and the NSS are, to varying degrees, guilty of using such fuzzy language throughout, but that is somewhat expected of political documents that surely go through dozens of rounds of coordination. When it comes to creating or employing national information power, both fail even to state objectives adequately and thus have no hopes of successfully strategizing. Douglas Borer described a more effective method of thinking strategically when he referred to the framework used by Colonel (Retired) Arthur Lykke, and adopted by the Army War College, that parses a strategy as a combination of objectives (or ends), ways, and means. According to Borer, "This tripartite framework illustrates how strategy is fundamentally a calculated relationship between ends and means."[5] With regard to use or support of information power, the 2015 NSS was missing every element.

After a brief introduction, the 2015 NSS identified the top strategic risks facing the United States. These included: "catastrophic attack on the U.S. homeland or critical infrastructure; threats or attacks against U.S. citizens abroad and our allies; global economic crisis or widespread economic slowdown; proliferation and/or use of weapons of mass destruction; severe global infectious disease outbreaks; climate change; major energy market disruptions; and significant security consequences associated with weak or failing states."[6] While each of these is a serious issue, the NSS omits any threat in the information environment or of an informational character, even cyberattacks.[7] In a section which specifically states that the U.S. will lead "with all instruments of national power," the NSS specifically mentions diplomacy, military power, and economic power. Curiously, the 2015 NSS completely omits informational power, the "I" in the traditional "DIME" model of national power. The closest it comes is an offhand mention of "people-to-people relationships," customarily termed "public diplomacy."[8]

Throughout the 2015 NSS there are sprinklings here and there that could potentially combine to create some informational strategy. The fact that they are scattered in placement and vague in language indicates that the author or authors did not consider the concept as a whole. In the "Security" chapter, there is a section titled "Assure Access to Shared Spaces" that mentions "cyber, space, air, and oceans" as global commons through which "goods, services, and ideas" flow.[9] This is analogous to the "physical" dimension of the information environment.[10] The subsection on cybersecurity mentions the need for " an open, secure, and reliable internet," but in this case "reliable" almost certainly refers to access to the Internet, not an Internet populated with content on which one can rely.[11] This section does not address the informational or cognitive dimensions of the information environment. The chapter on "Values" lists some goals that could be informational in nature, such as "promoting universal values," being a "champion" for vulnerable communities, or "supporting" democracies in transition, but there is very little there that could be called a "way" or a "means" for accomplishing these goals.[12]

There are two specific areas in which the 2015 NSS actually mentioned an information conflict. These were combatting Russian propaganda and countering terrorist narratives. In neither example was there any sense of a strategy to do either, or any stated role for intelligence. In the former example, the NSS stated that the U.S. would counter "Moscow's deceptive propaganda with the unvarnished truth."[13] It made no mention of how the U.S. would do this, what organs of the government would deliver the messages in which venues, what the "unvarnished truth" is, or whether it would be delivered as an overarching narrative or in an ad hoc fashion as the need arises. In the section on counterterrorism, there is a nod toward communications, but it uses a problematic "we say" versus "they do" phrasing: "in all our efforts, we aim to draw a stark contrast between what we stand for and the heinous deeds of the terrorists."[14] The statement does not specify to which audiences this "stark contrast" will be illustrated or to any process for determining that. Additionally, it ignores the fact that the terrorists themselves have a message, and that the U.S. has actions. Indeed, in many cases the terrorists' message is about U.S. actions. It is also unclear what the utility is of pointing out that terrorists use ugly and violent tactics. Various terrorist groups have disseminated videos of themselves beheading hostages for well over a decade.

The 1987 National Security Strategy

The difference between the muddled thinking exhibited by the 2015 NSS and the lucidity of the 1987 NSS promulgated by President Ronald Reagan could not be any clearer. As Daniel Kuehl described in 2000, the Reagan White House had a significant appreciation for information as an element of national power, and that administration viewed it as key to defeating the Soviet Union and securing the U.S.[15] The Reagan administration

developed and fully explained the overall philosophy in National Security Decision Directive 130 (NSDD 130), "U.S. International Information Policy," which was originally classified Secret and issued in March 1984. This directive is quite straightforward, with statements such as "international information is an integral and vital part of U.S. national security policy and strategy in the broad sense," and "the fundamental purpose of the U.S. international information program is to affect foreign audiences in ways favorable to U.S. national interests."[16] The directive described specific programs not only to deliver messages to foreign audiences, but also to learn about those audiences and thus craft better messages: "Research on public opinion, media reaction, and cultural factors needs to be substantially improved and more fully coordinated and applied to U.S. information activities. The proposed Foreign Opinion Research Advisory Group (FORA) is hereby approved and agencies should seek funding for it as required."[17]

It is in this context that the 1987 *National Security Strategy*, the first of its kind produced as required by the Goldwater-Nichols Act of 1986, included a section titled "Political and Informational Elements of National Power." In this document, the elements of strategy were all present. There was a charge: "This challenge is to fight the war of ideas and to help support the political infrastructure of world democracies." There was a way: "To accomplish this we must be as committed to the maintenance of our political defense as we are to our military defense." And there was a variety of means, including "traditional foreign policy agencies," "several less traditional participants," and private citizens and organizations. This short, seven-paragraph section also managed to describe a challenge of building a constituency for foreign policy at home, an effort to fight Soviet propaganda abroad, and a strategy of delivering messages to "the peoples of denied areas" using a variety of media. It did not make the mistake of referring to goals or vision as strategy. In fact, this section mentioned vision only in the close: "This is the vision of a nation which believes that a world of democracies is a safer world, and one where the respect for the dignity of all men has a better chance to be realized."[18]

The 2017 National Security Strategy

The 2017 NSS, while not as sharp or clear as the 1987 version, does show a greater appreciation for Information as an instrument of national power than the 2015 version it replaces. The document is structured around four "pillars": "Protect the American People, the Homeland, and the American Way of Life"; "Promote American Prosperity"; "Preserve Peace Through Strength"; and "Advance American Influence."[19] Each pillar has below it a number of subsections and "Priority Actions" describing ways to accomplish those items. From an information power standpoint, the closest item to the 1987 document's "Political and Informational Elements of National Power" section is the item in Pillar III on "Information Statecraft." There are many other references throughout the document that nod to the use of information power by the United States, its allies, and its adversaries, but this section provides the clearest guidance for what a new NIS would attempt to support.

As in 1987, the NSS begins with a description of the challenge: "America's competitors weaponized information to attack the values and institutions that underpin free societies, while shielding themselves from outside information. They exploit marketing techniques to target individuals based upon their activities, interests, opinions, and values. They disseminate misinformation and propaganda."[20] Written with the events of 2016 and 2017 clearly in mind, this section is substantially more focused than any similar references in the 2015 NSS. Unfortunately, the understanding of the problem demonstrated in the 2017 NSS is still incomplete. For example, in describing Russian information efforts, the 2017 NSS states, "Russia uses information operations as part of its offensive cyber efforts to influence public opinion across the globe. Its influence campaigns blend covert intelligence operations and false online personas with state-funded media, third-party intermediaries, and paid social media users or 'trolls.'"[21] In reality, this is backwards: Russia uses cyber operations as part of information operations, not the other way around. The type of operation referred to here would in Russian terms be considered "information-psychological," in which Russia understands its objective to be to affect the mind of a decision-maker—or many decision-makers, in the case of an election—rather than a particular piece of equipment.[22]

In terms of describing U.S. actions up to the present and in the future, the 2017 NSS continues to demonstrate an advance over the thinking in the 2015 document while still leaving substantial room for improvement. It correctly describes U.S. policies over the past several years as "tepid and fragmented," noting that they "lacked a sustained focus and have been hampered by the lack of properly trained professionals."[23] Unfortunately, the ways and means the NSS offers toward fixing the identified problems are somewhat scattered and thus highly unlikely to provide the "sustained focus" identified as a deficiency.

One of the Priority Actions does provide a clear role for the IC. The action "Prioritize the Competition" pledges to "improve our understanding of how adversaries gain informational and psychological advantages across all policies."[24] An IC enterprise aligned to the task should lead on this item. The action item goes on, however, to issue a

truly confusing statement, calling for the U.S. to "empower a true public diplomacy capability to compete effectively in this arena."[25] There is no explanation of what a "true" public diplomacy (PD) capability would be or what distinguishes this from the current, State Department-led effort.

The rest of this section shows a similar tendency toward vague and confusing statements. "Drive Effective Communications" calls for "coherent communications campaigns" but does not discuss what it means for something to be coherent.[26] Is it coherent to us, or coherent to the audience? Both? How do we know who the audience is and how to reach it? Then, how do we assess the effect? Who in the U.S. government is responsible for crafting these campaigns? How can any U.S. communications campaign be coherent in an age when "the tweet speaks for itself" and White House communications are not coherent from day to day?[27] This action talks about "ideological threats that emanate from radical Islamist groups and competitor nations," but makes no mention of whom the U.S. or competitor nations are attempting to communicate with or influence. The NSS states that campaigns run by the U.S. "will…expose adversary propaganda and disinformation," but shows no understanding or idea of how they would be distinguished by their target audiences as something other than propaganda, as if the mere fact that the U.S. says something means it must be true and therefore believed.[28]

A Priority Action describing the need to act with local elements makes mention of using the U.S. private sector, which "should lend its creativity and resources to promoting the values that inspire and grow a community of civilized groups and individuals."[29] The 1987 NSS also named private organizations as an element of national information power, but the world is very different 30 years later. Here, the private sector refers to "media and internet companies" that are multi-billion dollar international, publicly-traded corporations which conduct large amounts of business in Russia, China, and other countries with whom the U.S. has fundamental disagreements. The U.S. government would need some sort of formal mechanism to foster cooperation between itself and the private sector that does not hinder its elements as global brands. The U.S. risks killing the gaggle of geese currently laying golden eggs by attempting to leverage them for strategic purposes. There is space for cooperation, as the companies themselves have increasingly acknowledged their heightened responsibility in an age when they control so much of the domestic and international information environment.[30] This is a difficult problem that deserves careful, focused attention both inside the government and in the private sector.

INFORMATION POWER AND THE NATIONAL INTELLIGENCE STRATEGY

The 2014 National Intelligence Strategy

The 2014 NIS, which supported the 2010 and 2015 NSSs, defined the mission of the IC as follows: "Provide timely, insightful, objective, and relevant intelligence to inform decisions on national security issues and events." It was organized into sections on the "Strategic Environment," "Mission Objectives," "Enterprise Objectives," and "Implementing the Strategy."[31] The Strategic Environment section makes no explicit mention of an information component to that environment. It provides vague references to "influence," but nothing addressing information as an element of national power.

The mission objectives were divided between the functional (strategic intelligence, anticipatory intelligence, and intelligence support to current operations) and the topical (cybersecurity, counterterrorism, counterproliferation, and counterintelligence) in such a way that the functional objectives support each of the topical objectives. This illustrates the problem: the 2014 NIS did not support creation or use of national information power because none of the stated functional objectives of the IC is aligned to the problem. This largely reflects both the 2010 and 2015 NSS, neither of which found a place for intelligence in the strategic application of information power. The challenge and opportunity for the authors of the next NIS was to change this to reflect the greater awareness of information power demonstrated in the 2017 NSS and to support those openings it provides for the IC to contribute.

Like the 2015 NSS, the mission objectives of the 2014 NIS made only scattered mention of the communicative aspect of information power. These occurred in the counterterrorism objective, which directly foreshadowed the 2015 NSS, and fleetingly in the counterintelligence objective. The counterterrorism mission objective stated that "the IC supports the national whole-of-government effort to…counter the spread of violent extremist ideology that influences terrorist action…"[32] There was no specific mention of what form this support takes. There is a bulleted list claiming to explain how the IC will accomplish its goals, but it only says "provide insight to mitigate the spread of violent extremist ideology."[33] This is not only circular but represents muddled, non-strategic thinking, because it mistakes an objective for a course of action. It is unclear whether the aim is to counter the idea or the propagation of the idea, and the NIS proposes no means for accomplishing this. The 2015 NSS was not much better in this vein, promising only to support "alternatives to

extremist messaging." Unlike the NSS, the NIS did not mention Russian propaganda. The only thing at all close is in the counterintelligence section, which, in a list defining the term "foreign intelligence entity," mentions organizations, people, or groups which "unlawfully influence U.S. policy." It does not continue the thought into the discussion of the counterintelligence objective and how the IC plans to meet it.[34]

The potential effects of a vague NIS that suffers from the symptoms of "bad strategy" can be found in the section on "Implementing the Strategy." It stated that the DNI is the principal intelligence advisor to the president. If the DNI views his portfolio in a way reflected in the 2014 NIS, then he will be wholly unable to provide advice with respect to information power. The IC will produce no strategic or anticipatory intelligence, and it will have little or nothing to say about any current operations. The NIS made no mention of insight or support for military or diplomatic information efforts. If the IC does provide intelligence support, it will largely be the result of luck, happenstance, or an extraordinary effort instead of defined, executed strategy. The NIS shows no effort to characterize the information environment beyond cyberspace, and the support to countering terrorist messaging seems reactive and isolated, rather than part of a unified information strategy.

The "Implementing the Strategy" section stated that the NIS sets strategic priorities, budgets, and missions of the various elements of the IC. If this is the case, then information power will not appear on the list of priorities, at least not in any unified sense. Judging solely from their brief mention in the NIS, there would be an effort to understand terrorist narratives and ideology and, potentially, actions to thwart influence efforts conducted by foreign intelligence entities. However, there will be no intelligence support to a proactive effort to tell America's "story" in a way that counters those narratives or to craft the sort of "coherent" campaigns called for by the newest NSS. According to its own language, the NIS helps align the National Intelligence Program (NIP), which directs the budget for IC activities. Because information power as a concept appears nowhere in the NIS, it is likely that it is not specifically accounted for in the NIP either. Finally, "the mission and enterprise objectives in the NIS shall be incorporated and cascaded into IC elements…"[35] Because there is no mission objective for information power, it cannot be incorporated in any strategic way into the plans of the IC elements. The NIS specifically declares the need to measure progress against the objectives, but in the case of information power there are no stated objectives and thus there is nothing to measure. Hence, there is no opportunity for accountability.

LOOKING FORWARD TO A NEW NATIONAL INTELLIGENCE STRATEGY

"Information Advantage": A New Topical Mission Objective

The 2019 *National Intelligence Strategy*, released in January 2019, follows the same basic structure as the 2014 NIS. It has the same three functional mission objectives and the same four topical mission objectives. As such, it represents continuity. In many ways, that continuity was welcome in a turbulent time in American society and politics. However, the 2019 NIS largely failed to build on the progress evident in the 2017 NSS and its greater awareness of information power.

The next NIS could have improved substantially on the 2014 version simply by adding one more topical mission objective specifically designated to support creation and use of national information power. For the purposes of this article, the proposed objective will be referred to as "Information Advantage." The Information Advantage mission objective should be modeled on the NSDD 130 framework and updated for the modern era. This would drive the infrastructure and mechanisms of the IC in a way that supports and builds on the work of the 2017 NSS. Explicitly mentioning information power in the 2017 NSS underscored the need for intelligence support and at least provided some indication for how that support would contribute to national security. Including "Information Advantage" in the next NIS would have driven the need for collection and analysis that support political and diplomatic efforts as well as military information operations.

Both the 2014 and 2019 NIS include a "Cybersecurity" mission objective, and cyberspace is part of the information environment. Indeed, the 2017 NSS has an entire section titled "Keep America Safe in the Cyber Era," which stresses the dangers to critical infrastructure and financial networks.[36] However, for the purposes of the NIS and the NSS, "Information Advantage" and "Cybersecurity" should be treated separately. Over the past 25 years, cyber issues have tended to overshadow every other part of the broader information problem. As Arquilla noted in 2007, the cyber focus has "led to a concentration of effort on technological aspects of infrastructural warfare in cyberspace… This has led to a 'hollowing out' of capabilities for and sensitivities to the nuances of psychological operations and deception."[37] The past decade has seen no improvement on this score. As Christopher Paul explained in 2016, "Cybercapabilities are currently suspected to be over-resourced in relation to the absorptive capacity of organizations and command responsible for this area."[38] The ability of the IC to produce cyber threat intelligence, conduct computer network operations (CNO), and provide support to military CNO is important and should continue to expand, but it should be accompanied by a broader understanding of information power.

INFORMATION ADVANTAGE AND THE FUNCTIONAL MISSION OBJECTIVES

Strategic Intelligence

Adding a topical mission objective for Information Advantage would cut across the three functional mission objectives of strategic intelligence, anticipatory intelligence, and intelligence support to current operations. The 2014 NIS describes strategic intelligence as "the process and product of developing deep context, knowledge, and understanding to support national security decision-making," and the 2019 version uses broadly similar language.[39] Of course, understanding the strategic objectives of the U.S. government's information activities would help drive the production of strategic intelligence. The way the IC would produce strategic intelligence to support information activities would be, as described by the 2014 NIS, using "research, knowledge development, outreach, and tradecraft in order to provide deep context for a wide variety of policy and strategy communities." Actually, the 2017 NSS almost directly calls for better intelligence products that take all elements of national power and associated information into account. Specifically, it demands that the U.S. government "fuse our analysis of information derived from the diplomatic, information, military, and economic domains to compete more effectively on the geopolitical stage."[40]

Anticipatory Intelligence

The 2014 NIS defines anticipatory intelligence as "the product of intelligence collection and analysis focused on trends, events, and changing conditions to identify and characterize potential or imminent discontinuities, significant events, substantial opportunities, or threats to U.S. national interests."[41] Essentially, anticipatory intelligence forecasts and projects. The 2014 NIS called for the IC to "improve its ability to foresee, forecast, and alert the analytic community of potential issues of concern and convey early warning to national security customers to provide them with the best possible opportunity for action."[42]

It is clear that, since 2014, anticipatory intelligence is still a struggle for the IC, especially with regard to events having an informational character. A clear example was the failure to anticipate the Russian information campaign against the 2016 U.S. election. Because the IC had failed to envision this sort of information attack, decision-makers had little idea what the rules or implications of any of the potential courses of action would be and were essentially forced to make things up as they went along. The previous administration did not have a playbook for sustained, state-led information campaigns against a candidate for president.[43] A *National Intelligence Strategy* with a mission objective for Information Advantage may have been able to provide policymakers with some semblance of decision advantage in those situations. As it stood, most of the value provided by the IC was in attributing the attacks after they started and as they continued. The 2019 NIS relies on the same structures executing essentially the same strategy, albeit with the lessons of recent history as a guide.[44]

Current Operations

The 2014 NIS describes current operations intelligence as "characterized by the immediacy of the support provided. In addition to being responsive, this support also shapes future operations and investigations."[45] In order for the IC to produce intelligence that supports current operations in the information environment, it must be aware of them. The IC needs to be involved in the planning stages of activities conducted by civilian agencies. The 2017 NSS shows some areas where the IC could contribute to the execution and planning of operations in the information environment, though some are more explicit than others. A revised NIS could clarify this situation and provide for intelligence support to civilian agencies.

The IC must also be an active participant in military information operations (IO). The process of information operations intelligence integration (IOII) is described in the second chapter of the draft Marine Corps Information Operations Center's *Information Operations Planner's Handbook*. This chapter creates step-by-step instructions for IO planners to work with intelligence analysts in developing products that support IO. One item of note is that this chapter does not mention IC support. The IO planner and the intelligence analyst with whom he works in the field are largely on their own to create the products they need.[46] Given there is no mention of support to military information operations in either the 2014 or 2019 NIS and no mention of military information operations at all in the 2015 or 2017 NSS (other than cyber operations), this is not surprising. The IC needs to work with military leaders to develop collection requirements for IO planning, including public affairs, strategic communications, military deception (MILDEC), and military information support operations (MISO). The IC should specifically tailor products for these customers instead of expecting them to pull down and compile the information themselves from dozens of different databases and reports.

Despite the structural deficiencies of the 2014 NIS and 2015 NSS, the IC and military demonstrated what the integration of intelligence and military information operations can accomplish with the execution of cyber operations against ISIS by Joint Task Force (JTF) ARES.[47] Indeed, according to National Public Radio, the successes of JTF ARES provided the model for the Russia Small Group (RSG), which was developed to combat Russian influence efforts

against the 2018 midterm elections.[48] Building the concept of Information Advantage into the Intelligence Community in a robust, structural way by making it part of the NIS would provide the foundation for both civilian and military operations within the information environment. Both JTF ARES and RSG took advantage of the fact that the National Security Agency and U.S. Cyber Command share a director and headquarters. This likely made it easier to move people and resources to meet challenges. Other information operations, including ones that do not rely on computer network operations, do not have that same advantage.

INFORMATION ADVANTAGE AND THE ENTERPRISE OBJECTIVES

Advancing the IC's role in support of information power will, however, require investments in people and innovation. These are already enterprise objectives in the 2014 and 2019 NISs, but they could benefit somewhat from modification. Making advances in the use of information power will require innovation in the social sciences, as well as a better understanding of technological trends. Public opinion research is a moving target. It is advancing in response to challenges and, if the IC invests heavily in the space, it will have to move with that technology or be left with capabilities that will quickly become obsolete. One simple example would be the transition in the U.S. population from a landline-only group to a cell phone-only group. According to a study cited by Pew Research in 2016, the cell phone-only group grew from nearly 0% to 47% of adults between 2004 and 2016.[49] There are almost certainly similar trends occurring among overseas publics at a similar or greater speed. Additionally, applying traditional public opinion research methodologies to populations in less permissive areas which may live in cultural contexts that affect their responses will require constant innovation.

AN IDEA FOR STRUCTURAL REFORM

Operationally, the best way to provide strategic, anticipatory, and operational intelligence for the information mission may be to create a new organization or mission center. Currently, under the ODNI construct, the four topical mission objectives in the NIS map directly to the National Counterterrorism Center (NCTC), the National Counterproliferation Center (NCPC), the National Counterintelligence and Security Center (NCSC), and the Cyber Threat Intelligence Integration Center (CTIIC). Indeed, the 2019 NIS specifically notes that "mission-focused centers have proven effective in achieving" outcomes in a "flexible, responsive, and resilient" manner.[50]

One problem with following this model directly is that none of the current mission centers is charged with collection. Instead, they serve to coordinate activities taking place in other parts of the government, to varying degrees of effectiveness. The characteristics of the new organization should perhaps be more like the National Geospatial-Intelligence Agency (NGA), which provides geospatial intelligence (GEOINT) by synthesizing information from a variety of sources, which include classified, commercially acquired, and open source information. NGA does not "collect" GEOINT as much as it creates it. For the purposes of this article, the new construct would be called the Center for the Study of the Information Environment (CSIE). The difference between CSIE and NGA is that the former would actually generate public opinion research.[51]

The CSIE would consist of several elements, some of which already exist in the IC. The DNI could join the media analysis activities of the Open Source Enterprise (OSE) with the public opinion research currently conducted by the Office of Opinion Research (OPN) of the State Department's Bureau of Intelligence and Research Office (INR).[52] Alternatively, INR/OPN could be left where it is to focus on its current mission of supporting diplomacy, and the IC could build its own organization for its own purposes. INR/OPN analysts bring significant training, expertise, and experience to the areas they study. This expertise is critical and every effort should be made to maintain and increase that capacity. An independent mission center could add a cadre of data scientists to make increased use of public opinion data collected to identify underlying trends.

Intelligence in support of information activities should not entirely consist of OSINT or polling, however. CSIE analysts would add value to open sources by integrating insights from classified collection to produce all-source products. This "OSINT first" mentality is somewhat contrary to the way analysts now approach intelligence problems. Unlike the information that classified platforms collect, however, most of the relevant features of the information environment are not hidden.

CSIE would produce traditional strategic intelligence to support information activities by using "research, knowledge development, outreach, and tradecraft in order to provide deep context for a wide variety of policy and strategy communities."[53] In addition to the media content analysis and quantitative and qualitative opinion research functions, the CSIE could engage in further techniques to understand cultural and behavioral profiles of target audiences that would be integrated into a strategic intelligence picture.[54]

A new CSIE could take the lead in incorporating private sector techniques into the mission of understanding the modern information environment. Currently, the IC is not equipped

to understand what is happening on social media. An overreliance on classified collection has not helped. In truth, very few people, even in the private sector, actually have a grasp of the rapidly changing nature of social media. Though many vendors demonstrate proprietary solutions with backward-looking case studies, their effectiveness as anticipatory tools remains suspect. To remedy this problem, the CSIE should recruit and learn from Silicon Valley giants, such as Google, Twitter, and Facebook, which have poured substantial resources into studying and influencing behavior of social media and mobile application users worldwide.[55] If the U.S. government wishes to confront adversaries in those relatively new information arenas, it should use the natural advantage that they are American companies full of American citizens who have at times shown interest in serving their country.[56] Open source researchers have been able to track information operations in social media with sleuth work on specific Twitter users and networks of bots.[57] Marrying informed open source tradecraft with classified collection that reveals leadership intentions and operational sources and methods of foreign military or intelligence units could create powerful anticipatory intelligence.

CONCLUSION

A skeptic might view deep analysis of the various iterations of the *National Intelligence Strategy* and the *National Security Strategy* as inherently flawed. These are public documents that are inherently political. Indeed, Kuehl described how the public NSS "can become a subject of public controversy, whereby domestic and partisan political issues and positions come into play."[58] No further proof of this is needed than the fact that tax reform and climate policies appear in the 2017 NSS.[59] There is no reason to think the NIS is immune from such treatment. However, when examined in the context of actual investments, the actions of administrations in crisis situations, and the evolution of the strategies over time, both the NIS and NSS do provide insight into the strategic thinking of presidents and of the nation at large. For example, the fact that cybersecurity appears as a topical mission objective in the 2014 and 2019 NISs, but "information advantage" does not, really does reflect IC investments and focus. It is also clear that the scant treatment of information is also not itself some form of denial and deception, meant to bamboozle America's adversaries. The nation's slow, confused reactions to an increasing number of foreign information operations and its decades-long struggle to defeat terrorist messaging indicate the truth of the matter.

A *National Intelligence Strategy* that explicitly calls for support to national information power will not solve all the problems the U.S. government finds itself facing. Similarly, reorganizing or creating new bureaucracies certainly has the potential to hurt more than it helps. However, a continued failure by the U.S. government to use every instrument at its disposal will mean that achieving national goals and securing national interests will become more and more difficult as time goes by. Throughout the 20th century, the nation found itself faced with strong adversaries which pushed this country to the brink. Successful application of every element of national power brought the country through those times. Every one of our current IC organizations was created to address a specific set of challenges by gathering resources and expertise in a way that added value to the whole mission. We would do well to learn from that history. Looking back, we find clear-eyed, pragmatic, strategic thinking that helped maximize U.S. power potential. Applying that same philosophy to the *National Intelligence Strategy* in a way that builds upon the positive steps of the 2017 *National Security Strategy* will position the nation well for the 21st century.

NOTES

[1] John Arquilla, "Introduction: Thinking about Information Strategy," in *Information Strategy and Warfare*, eds. John Arquilla and Douglas A. Borer (New York: Routledge, 2007), 9.
[2] U.S. Director of National Intelligence (DNI), *The National Intelligence Strategy of the United States of America* (Washington, DC, September 2014) accessed November 5, 2017, https://www.dni.gov/files/documents/2014_NIS_Publication.pdf, 2.
[3] U.S. DNI, 2014, 2.
[4] Richard Rumelt, "The Perils of Bad Strategy," *The McKinsey Quarterly*, no. 1 (2011): 30, accessed November 7, 2017, https://search.proquest.com/docview/54051815?accountid=10504.
[5] Douglas A. Borer, "Conclusion: Why Is Information Strategy Difficult?" in *Information Strategy and Warfare*, eds. John Arquilla and Douglas A. Borer (New York: Routledge, 2007), 233.
[6] U.S. President, *National Security Strategy* (Washington, DC, February 6, 2015), accessed November 5, 2017, https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy.pdf, 2.
[7] Throughout this article, the definition of the information environment used is "the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information." The information environment is described as having a physical dimension (connectivity), an informational dimension (content), and a cognitive dimension. This definition is derived from DoD Joint Publication 3-13, the citation of which follows. Joint Chiefs of Staff, Joint Publication 3-13, *Information Operations*, November 2012 (incorporating Change 1 of November 20, 2014), ix-x.
[8] U.S. President, *National Security Strategy*, 2015, 4.
[9] U.S. President, *National Security Strategy*, 2015, 12-13.
[10] Joint Chiefs of Staff, ix-x.
[11] U.S. President, *National Security Strategy*, 2015, 12.
[12] U.S. President, *National Security Strategy*, 2015, 20-21.
[13] U.S. President, *National Security Strategy*, 2015, 25.
[14] U.S. President, *National Security Strategy*, 2015, 9.
[15] Daniel Kuehl, "The Information Component of Power and the National Security Strategy," in *Cyberwar 3.0: Human Factors in Information Operations and Future Conflict*, eds. A. Campen and D. Dearth, (Fairfax, VA: AFCEA Press, 2000), 277-278.

[16] Ronald Reagan, National Security Decision Directive 130, "US International Information Policy," National Security Decision Directives, Ronald Reagan Presidential Library & Museum (March 6, 1984), accessed November 6, 2017, https://reaganlibrary.archives.gov/archives/reference/Scanned%20NSDDS/NSDD130.pdf, 1.
[17] Reagan, 4.
[18] U.S. President, *The National Security Strategy of the United States* (Washington, DC, January 1987), accessed November 6, 2017, http://insidethecoldwar.org/sites/default/files/documents/National%20Security%20Strategy%20of%20the%20United%20States%201987_0.pdf, 13.
[19] U.S. President, *National Security Strategy* (Washington, DC, December 18, 2017), accessed December 19, 2017, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf, v-vi.
[20] U.S. President, *National Security Strategy*, 2017, 34.
[21] U.S. President, *National Security Strategy*, 2017, 35.
[22] Kier Giles, *Handbook of Russian Information Warfare* (Rome: NATO Defense College, 2016), 9.
[23] U.S. President, *National Security Strategy*, 2017, 35.
[24] U.S. President, *National Security Strategy*, 2017, 35.
[25] U.S. President, *National Security Strategy*, 2017, 35.
[26] U.S. President, *National Security Strategy*, 2017, 35.
[27] Noah Bierman, "'The tweet speaks for itself' could become a Trump administration motto," *The Los Angeles Times*, January 9, 2017, accessed July 16, 2018, http://www.latimes.com/politics/la-na-pol-trump-tweet-20170109-story.html.
[28] U.S. President, *National Security Strategy*, 2017, 35.
[29] U.S. President, *National Security Strategy*, 2017, 35.
[30] Emily Stewart, "Read: Mark Zuckerberg's prepared statement for congressional testimony," *Vox*, April 10, 2018, accessed July 24, 2018, https://www.vox.com/policy-and-politics/2018/4/9/17215640/mark-zuckerberg-congress-testimony-facebook.
[31] U.S. Director of National Intelligence, *The National Intelligence Strategy of the United States of America* (Washington, DC, September 2014), accessed November 5, 2017, https://www.dni.gov/files/documents/2014_NIS_Publication.pdf, 4.
[32] U.S. DNI, 2014, 9.
[33] U.S. DNI, 2014, 9.
[34] U.S. DNI, 2014, 10.
[35] U.S. DNI, 2014, 16.
[36] U.S. President, *National Security Strategy*, 2017, 12.
[37] Arquilla, 8.
[38] Christopher Paul, "Enhancing US Efforts to Inform, Influence, and Persuade," *Parameters* 46, no. 3 (Autumn 2016): 96.
[39] U.S. DNI, 2014, 7; U.S. Director of National Intelligence, *National Intelligence Strategy of the United States of America* (Washington, DC, January 2019), accessed October 13, 2019, https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf, 8.
[40] U.S. President, *National Security Strategy*, 2017, 32.
[41] U.S. DNI, 2014, 7.
[42] U.S. DNI, 2014, 7.
[43] Ellen Nakashima, "NSA and Cyber Command to coordinate actions to counter Russian election interference in 2018 amid absence of White House guidance," *The Washington Post*, July 17, 2018, accessed July 24, 2018, https://www.washingtonpost.com/world/national-security/nsa-and-cyber-command-to-coordinate-actions-to-counter-russian-election-interference-in-2018-amid-absence-of-white-house-guidance/2018/07/17/baac95b2-8900-11e8-85ae-511bc1146b0b_story.html?utm_term=.f1a20e451b9e.
[44] U.S. DNI, 2019, 9.
[45] U.S. DNI, 2014, 8.
[46] Marine Corps Information Operations Center, *IO Planner's Handbook* (2d draft), June 2012, 2-1, 2-2.
[47] Dina Temple-Raston, "How the U.S. Hacked ISIS," National Public Radio, September 26, 2019, accessed October 13, 2019, https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis.
[48] Temple-Raston.
[49] Kyley McGeeney, "Pew Research Center will call 75% cellphones for surveys in 2016," Pew Research Center Fact Tank, January 5, 2016, accessed November 7, 2017, http://www.pewresearch.org/fact-tank/2016/01/05/pew-research-center-will-call-75-cellphones-for-surveys-in-2016/.
[50] U.S. DNI, 2019, 18.
[51] A new organization like this would likely require legislation, but the political and budget implications are beyond the scope of this article.
[52] U.S. Department of State, "Offices Within the Bureau of Intelligence and Research," accessed November 8, 2017, https://www.state.gov/s/inr/owb/index.htm.
[53] U.S. DNI, 2014, 7.
[54] Jeannie L. Johnson and Matthew T. Berrett, "Cultural Topography: A New Research Tool for Intelligence Analysis," *Studies in Intelligence* 55, no. 2 (June 2011): 3.
[55] Samuel Gibbs, "Facebook apologises for psychological experiments on users," *The Guardian*, July 2, 2014, last modified November 30, 2017, accessed July 24, 2018, https://www.theguardian.com/technology/2014/jul/02/facebook-apologises-psychological-experiments-on-users. See also Avery Hartman, "These are the sneaky ways apps like Instagram, Facebook, Tinder lure you in and get you 'addicted'," *Business Insider*, February 17, 2018, accessed July 24, 2018, https://www.businessinsider.com/how-app-developers-keep-us-addicted-to-our-smartphones-2018-1.
[56] Michael D. Shear, "White House Picks Engineer from Google to Fix Sites," *The New York Times*, August 11, 2014, accessed October 28, 2017, https://www.nytimes.com/2014/08/12/us/politics/ex-google-engineer-to-lead-fix-it-team-for-government-websites.html?_r=0.
[57] Jarred Prier, "Commanding the Trend: Social Media as Information Warfare," *Strategic Studies Quarterly* 11, no. 4 (Winter 2017): 66-75.
[58] Kuehl, 276.
[59] U.S. President, *National Security Strategy*, 2017, 18.

Zachary L. Young II is a National Security Agency employee with experience serving as a target analyst, dealing with election protection issues, and working both the offensive and defensive sides of the cyber mission. In 2018 Zach earned a Master of Science and Technology Intelligence (MSTI) degree from the Anthony G. Oettinger School of Science and Technology Intelligence, National Intelligence University, and in 2004 a bachelor's degree in Applied Mathematics from Harvard University.

The Many Ways Writing Can Help and Hinder Your Career and Business

by Col (USAF, Ret) Carla D. Bass

[Editor's Note: This article, which differs radically from the usual *AIJ* format, is based on a radio interview by Mark Amtower, host of "Amtower Off Center," conducted on Federal News Network with Carla Bass, NMIF board member and author of the award-winning book *Write to Influence!* I have taken the liberty to edit slightly for grammar, punctuation, and other problems that naturally arise with a transcribed verbal piece.]

- Quick! Snag the Reader's Attention … and Keep It!
- Frame a Winning Argument – Influence the Financial "Bottom Line"
- "Strategize Your Way to Success" – Job Interviews, Performance Reviews, and Resumes
- "You're Speaking My Language!" – Strategies to Resonate with Your Audience
- Make Each Word Count – Four Tips to Do Just That
- What Do I Bring to the Game? Self-Empowerment

QUICK! SNAG THE READER'S ATTENTION … AND KEEP IT!

Mark: I'm here with a returning guest, retired Air Force Colonel Carla D. Bass, author of the multiple award-winning book *Write to Influence!* … now in its second edition. Before we begin, you teach workshops, yes? Where can people find information about you?

Carla: I teach workshops to government, corporate, private business, and NGO clients across the country and locally, of course. The book is available online at several commercial retailers. My website is www.writetoinfluence.net.

Mark: Carla's on the show because we agree on the concept of concise and precise communication. Carla once presented a workshop to my graduate-level class at George Washington University. I had tasked my 15 students to compose an essay no longer than 400 words; however, only three succeeded. The others submitted two pages of worthless verbiage.

Carla: You're correct. The academic system—and no ding on teachers—produces students who write "fat" and not "skinny," a handicap when entering the fast-paced business world in which every second counts.

Mark: Let's discuss short attention spans. Research indicates the attention span is shrinking for humans in general and Americans in particular. Some say it can be as short as eight seconds. Now, pair this fact with the concept of the word-per-idea ratio, which emphasizes using the fewest possible words to convey a message. Thus, two opposing forces converge: the short attention span and the need to communicate with audiences.

Carla: Yes, the *Write to Influence!* methodology addresses precisely that. We're going to play "Knock, knock." Ready? "Knock, knock."

Mark: "Who's there?"

Carla: Wrong answer! The correct response in today's busy world is, "What do you want?" Everyone is so busy that you must make your point quickly and get off the stage. Thus, writers are constrained by two things: the audience's time (counted in seconds) and space, such as above-the-fold on a web page, demarcated areas on government forms, or an allocated word count.

Brevity and conciseness are essential for impactful communication. Imagine a white rectangle six inches wide and one inch tall. Impose on that shape the word "OPPORTUNITY" in big, bold letters. My point? The author who best leverages time and space to make a case often wins.

Mark: You also see this in the above-the-fold on LinkedIn, that opening screen shot. You've got the background graphic, but the most important verbal real estate is your headline—the 200 characters where you explain who you are, what you do, and for whom you do it.

FRAME A WINNING ARGUMENT – INFLUENCE THE FINANCIAL "BOTTOM LINE"

Mark: Let's discuss framing arguments.

Carla: An argument is actually a form of warfare and the weapon of choice is words. For example, the goal in debates is to subdue the opposition through the persuasiveness of your own argument.

Developing an outline is a fundamental first step people often skip. The product suffers as a result.

The outline offers four major benefits. First, it enables the author to predetermine key points—stepping-stones—that guide the reader to the intended conclusion and leverages that time and space we just discussed. Second, it keeps the author on track while developing the draft. Third, when the draft is complete, it serves as a checklist to verify that you did, in fact, address the intended points. Finally, it highlights information in the completed draft *not* identified in the outline. The author must then confirm that these data advance the message.

A builder wouldn't undertake a major construction project without an architectural drawing. A family wouldn't embark on a cross-country trip without a roadmap. Similarly, the astute author shouldn't write without an outline.

I offer four additional tips to frame a winning argument:

(1) Define the issue and its impact in precise, objective, and factual terms.
(2) Present alternate courses of action, addressing pros and cons equitably to enhance your credibility.
(3) Recommend the preferred course of action, explaining the rationale and who will benefit.
(4) Learn as much as possible about opposing views and neutralize them as you present the preferred solution.

Mark: Let's discuss the powers of persuasion as they impact the business. We're entering another continuing resolution … no new projects … and many organizations face diminishing funds. So, how does one defend an operating budget when called into corporate headquarters or Congress?

Carla: Consider using this structure: Problem, impact, solution, result.

Problem: An organization approached me because its staff couldn't write effectively.

Impact: It couldn't relate to higher headquarters the value and operational impact of its many noteworthy accomplishments. As a result, its budget was cut.

Solution: The staff learned to write with precision and banish bureaucratic blather. They also developed the ability to infuse messages with detail, essential when writing persuasively.

Result: The organization became more proficient in defending its budget.

Let me emphasize the importance of including detail in a message. It adds contour, depth, and dimension, and provides the reader a mental yardstick to grasp the significance of the story. Consider this example from a resume. The first version is flat; the second pops with the significance of the individual's achievement—detail makes the difference.

BEFORE: Supervised a team studying an aging logistics system. Sent recommendations to the CEO.

AFTER: Supervised a 6-person team conducting a 5-week study of an aging logistics system. Made four recommendations, all accepted by the CEO. Saved the company $800K.

Mark: When companies face revenue shortfalls, marketing is usually the first department cut.

Carla: Strategic communications is precisely the *wrong* place to cut! Leveraging success stories is an opportunity people often miss. This affords tremendous marketing material for brochures, web sites, press releases, or other products. People like to associate with winning companies. So when you hit those home runs, you need a marketing department to publicize and claim credit for them.

Mark: For some contractors, this information must remain internal to the government customer, predicated on who that might be.

Carla: True, but the affected government agency can leverage that information, as needed, such as defending operational budgets or justifying and expanded mission.

Mark: I want to present a scenario. A small company (50 people) is exceptionally well-qualified as a subject matter expert on cybersecurity. It competes against larger firms performing similar services but not so well. How would you enunciate this in a strategic communications campaign that positions this company as the one to select?

Carla: I'd determine advantages my company offers that a larger company can't: my strengths, e.g., uniquely talented employees; current and former clients; problems I've solved; essentially, factors that make me unique.

"STRATEGIZE YOUR WAY TO SUCCESS" – JOB INTERVIEWS, PERFORMANCE REVIEWS, AND RESUMES

Mark: You composed an article, "Strategize Your Way to Success," that the Military Officers Association of America published in its magazine. Can you summarize that for us?

Carla: Sure, this again refers to leveraging time and space. You should always have three messages in your hip pocket. Prior to a job interview, determine what facts you want to resonate after you've departed … a skill set, specific accomplishment, or something else … and purposefully work these into the conversation. Senior leaders should be prepared to identify three items upon which they could spend funds, should that opportunity suddenly arise. When briefing a senior-level individual, be able to adjust should that 30-minute meeting be curtailed to five—triage your points, identifying the top three in advance.

Mark: How do you apply this writing methodology to promotion endorsements and performance reviews, especially your own?

Carla: Consider your performance expectations based on your most recent discussion with your supervisor. How did you perform contrasted with those expectations?

If the boss asks you to submit input to your performance review, provide information that highlights the impact of your accomplishments, including detail to set the context. People consider this an onerous task because it seems like bragging. Now is *not* the time for humility. I offer five tips:

(1) Pretend you are making a case to promote a deserving subordinate.
(2) Keep a job journal and be precise in recording what you did, for whom, and the impact.
(3) Submit input to weekly activity reports (include detailed impact).
(4) Document and retain compliments from supervisors, clients, others—annotate the originator and date. Consider including short quotations from these in your submission; such words can be golden.
(5) Don't inadvertently convey a partial story, e.g., "Top 1 percent of my staff," but out of how many?

Mark: The job journal can help if you keep it up to date.

Carla: Oh, sure! Record accomplishments as they occur. People who don't keep track of what they've done, their impacts, and compliments received hurt themselves professionally. Nuances of your achievements are often lost in the flurry of having to review your previous year's activities—and usually doing so when rushing to meet a deadline.

Mark: These tips also apply to building a resume.

Carla: Absolutely. An employer will often miss the opportunity to hire the perfect applicant due to a poorly composed resume—a lose/lose situation. Avoid this by strategizing the presentation of your accomplishments and honing the text to leverage that limited space and convey their importance.

The opening two lines on a resume are critical. Express "Here's how I can help the employer," not "Here's my skill set." Then begin bullets with hard-hitting verbs such as "led," "organized," "implemented," "initiated," and "developed."

A major mistake people make in resumes is mixing the opening words in listed items. I'm going to read a list of opening words that I extracted from sequential bullets in a resume. Try to detect the inconsistencies: "responsible for," "supported," "co-led," "provide coordination," "skilled communicator," "coordinates," and "monitor." They snag like a car's engine struggling to shift gears. This distracts the reader from your message. Don't mix nouns and verbs. When using verbs, maintain the same tense.

Mark: How do you explain your contribution when you are a team member?

Carla: State "member of a XX-person team that …" and explain what that team accomplished. Then identify your contributions. Examined from another perspective, determine what that team would *not* have accomplished without you. That's how you distill your achievements from that of the group.

"YOU'RE SPEAKING MY LANGUAGE!" – STRATEGIES TO CONNECT WITH YOUR AUDIENCE

Mark: What do you mean when referring to strategic messaging?

Carla: I teach people to approach powerful writing from the perspective of an inverted triangle. Located at the top half of the triangle are strategies to develop your main message. Word Sculpting Tools to hone the message and make every word count are at the bottom half, culminating in the pointy end. Here are three of many strategies presented in Part 1 of the book:

First, "Know Your Audience" is the cardinal rule in any communication. You must recognize:

(1) The audience's background and familiarity with the information.
(2) What that audience hopes to gain from your communication.
(3) Equally important, what you hope to gain from communicating with the audience. Based on this information, you have a greater likelihood of leading the audience to your desired conclusion.

The **second** strategy is, "Resonate with Your Audience." Compose your message from the audience's perspective. Think empathetically. Here are three examples:

(1) When communicating with a potential employer, explain how you can help the company, correlating your skills and experience to its business needs. Don't approach the communication from the perspective of "Hire me because I'm great at …"
(2) If competing for a grant, explain how your project can further the grantmaker's mission rather than "I've got a great idea."
(3) If promoting a book, the approach should be, "With this book, you'll learn to …" and not "Buy this book; it won many awards."

The **third** strategy is writing to elicit this response, "By golly, you're speaking my language!" When addressing a specialized audience, jargon related to that audience is appropriate. For example, I helped a friend edit an article for a baseball journal. His article included the term "strike out the side"; I had no idea what this meant being unfamiliar with the nuances of the sport. However, the intended audience did! Conversely, if lobbying Congress for funds for an IT system, don't make your case based on processing capacity and storage space; instead, explain how it will benefit the taxpayer using terms Congressional decision-makers understand.

MAKE EACH WORD COUNT – HERE'S HOW

Mark: Describe the next part of your book.

Carla: Part 2, *Word Sculpting* (the bottom half of the inverted triangle), demonstrates how to hone the draft—

sentence by sentence—to make each word count and every second of the reader's time play to *your* advantage. Let me share four of my ten Word Sculpting Tools:

(1) **Avoid "verb-icide."** Don't smother the verb in useless words. For example, "make a determination" equates to "determine," "hold a discussion" equates to "discuss," and "say specifically" equates to "specify."
(2) **Purge redundancies**. These encumber your message. Consider "malicious computer virus." What "computer virus" is not "malicious"?
(3) **Eliminate useless words**. This is the most fundamental of my tools. We revise, "If there is a disagreement between the parties" to "If the parties disagree," thus saving time and space, and not inflicting the reader with horrible writing.
(4) **Revise, edit, and proofread**. Each is a distinct and critical step for successful messaging. After completing the first draft, set it down and revisit it later, propelled with a fresh perspective and new ideas.

Mark: Let's discuss that second set of eyes; we've touched on this a couple of times. When reading the completed draft, it ostensibly conveys precisely what you intended. However, if you read the draft aloud, you can hear nuanced mistakes and identify needed refinements.

Carla: A second set of eyes is invaluable in reviewing the first and even subsequent drafts and will identify items unapparent to the author, who is by this time too close to the material. Regarding your other point, I'm a huge proponent of reading a draft aloud. You can hear how it flows ... or doesn't … and detect overused or repetitious words that might otherwise slip into the final product.

Mark: People often ghost-write items for a senior manager's signature. However, even talented ghost-writers can unintentionally infuse their own opinion and skew the message. The signatory should thoroughly edit these products to ensure they reflect the proper voice and convey the intended message. Do you edit other people's products in your current position working with the federal government?

Carla: Yes, and I address the difficulties of editing in an appendix in *Write to Influence!* One must proceed carefully when editing another's work. The key to a successful partnership is determining how much help the author wants—a light touch for grammatical correction or a major facelift, if required. I once considered a poorly written product "red meat" and gleefully began to edit, alienating—even angering—the author in the process. The kinder, gentler approach is definitely more effective and enjoyable.

WHAT DO I BRING TO THE GAME? SELF-EMPOWERMENT

Mark: Carla, you are a business owner. How do you position yourself? Your book is the quintessential business card.

Carla: Yes, the second edition, published this summer, contains new chapters on writing grants, essays for college applications, elevator speeches, framing a paper, knowing your audience—psychology of the catch, and much more.

With 40 years' experience writing for Congress, the White House, generals, and ambassadors, I position myself as an expert in composing impactful messages and banishing bureaucratic blather. I share my techniques in workshops that are fun, engaging, and effective. This empowers others to capitalize on opportunity by leveraging the strength of their own words.

Mark: We met two years ago via phone call. I predicate interviews on my show based on the individual's ability to speak. You are very precise about what you say and how you say it.

Carla: That's because precise communication has become instinctive; it can become instinctive for others, as well.

Mark: OK. Final thoughts?

Carla: Learning to write to influence is a skill that will open doors for a lifetime. I adore helping others acquire this capability!

Mark: Thank you for coming … find Carla on LinkedIn and www.writetoinfluence.net.

Colonel (USAF, Ret) Carla D. Bass, author of the multiple award-winning book Write to Influence! *(2nd edition published in July 2019), served 30 years' active duty and 12 years for the Office of the Director of National Intelligence. Throughout this time, she composed products for Congress, the White House, ambassadors, and generals. She developed and taught her writing methodology to thousands of Air Force members for 15 years. Carla now teaches highly acclaimed workshops to corporations, private business, government agencies, and NGOs. Her assignments included Washington, DC; Germany; Korea; and Bulgaria, as the U.S. Defense Attaché. Carla is a valued member of the NMIF board of directors.*

Lieutenant Colonel Carol S. Bessette: NMIA President

by Col (USAF, Ret) John R. Clark

Carol Schoeller Bessette, former President of the National Military Intelligence Association, passed away on May 29, 2018, at the age of 79 in her home, after a long struggle with brain cancer. She was a dedicated member of NMIA, the predecessor of NMIF, and led it through some difficult times during the early 1990s. Carol and her husband both served tours in the Defense Intelligence Agency, and both were dedicated intelligence professionals who strongly advocated intelligence studies and professional careers in that field.

Carol was born in northern New Jersey in 1938 to Theobald Herman (Ted) Schoeller and Evelyn Lucitt Schoeller. She entered College Misericordia in Dallas, Pennsylvania, in 1956 and graduated four years later with a BA degree in Social Studies. She then entered the U.S. Air Force upon commissioning from Officer Training School in September 1960. While at OTS she tried to enter the intelligence career field but was told that "girls can't do intelligence." She knew better; hence, at Langley Air Force Base, Virginia (her next assignment), she discovered a path to intelligence if she earned a master's degree in International Relations via the Air Force. Selected for this program, she did indeed enter the intelligence career field with an assignment to HQ, U.S. Air Forces in Europe (USAFE). After three years at Ramstein Airbase with her new husband John (whom she had married in 1964), she was selected for an intelligence billet at HQ, Seventh Air Force, at Tan Son Nhut Airbase, Vietnam.

She arrived at Tan Son Nhut in May 1968, just in time for the Viet Cong's May Offensive. Having survived those rocket attacks, and many others over the next 13 months, she was then sent as a student to the Defense Intelligence School (now National Intelligence University) in Washington, DC, where she and John became students in the same class. Then ensued three years serving as an analyst in DIA, specializing in the Laotian component of the Southeast Asia conflict. She subsequently returned to USAFE HQ in Germany and headed a branch of its analysis division. After returning to the United States in 1978, she became a dean in what was soon to become the expanded Defense Intelligence College. She was selected next for a prestigious position on the Intelligence Community Staff, the pinnacle of the U.S. Intelligence Community at the time headed by the Director of Central Intelligence.

Carol retired from the Air Force as a lieutenant colonel in 1985 and spent a few years as a defense contractor. However, she soon found a very satisfactory niche as a museum guide, then a tour guide, in the national capital area. She found her best calling in teaching classes and leading "Washington Spy Sites" tour groups throughout the region. She melded her extensive historical knowledge, ability to lead, and skill at teaching to thrive in this environment.

In the early 1990s, she became a board member of NMIA. During her tenure, there arose an organizational crisis threatening NMIA's very existence. With the backing of Lt Gen Eugene Tighe (former DIA Director), LTG James Williams (former DIA Director and NMIA Chairman), and others, Carol effectively rescued the organization and put it on the road to recovery as President. Across the breadth of the intelligence disciplines, she was very supportive of intelligence careers (a current NMIF focus), and especially supportive of women working in such sensitive positions.

During her military career, Lt Col Bessette earned the following awards and medals:

- Bronze Star Medal
- Defense Meritorious Service Medal
- Joint Service Commendation Medal
- Air Force Outstanding Unit Award with Valor and 2 Oak Leaf Clusters
- National Defense Service Medal
- Vietnam Service Medal
- Air Force Longevity Service Ribbon with Silver Oak Leaf Cluster
- Republic of Vietnam Gallantry Cross with Palm
- Republic of Vietnam Campaign Medal

In 2000 she became aware of the Tan Son Nhut Association (TSNA) and joined up. In 2009 she volunteered to become TSNA's treasurer, a position she held right up until her passing. Her leadership skills were valuable wherever she went, and TSNA became her special venue, as NMIA had been earlier. She always loved the annual reunions, her last one in 2017 in Colorado Springs. Carol will be missed greatly, not only by her husband John, but also by anyone who ever crossed her path.

Tactical Intelligence Failures from Vietnam to Afghanistan and Iraq: "Same Old Song"

by Luke A. Holloman

In Vietnam, there were clear deficiencies in tactical information. However, Vietnam was the first case in which, regardless of modern collection assets such as new surveillance and reconnaissance equipment utilizing airborne infrared, chemical, and radar sensors, a variety of night vision aids and devices, signals intelligence equipment, unattended ground sensors, and ground surveillance radars, the terrain and environment presented unprecedented challenges to all collection efforts. Tactical commanders faced issues not just in collection, but in evaluation and dissemination of intelligence as well. The main issues were not with the amount of information, but with varying armed service doctrine on how to centralize collection efforts in a way that could be integrated to inform operational planning. Additionally, security requirements needed to access certain intelligence information subsystems, and the lack of trained and experience intelligence personnel in-theater contributed greatly to deficiencies.

Service doctrine saw U.S. military units in advisory roles throughout the initial parts of the war. Information flowed well at first, through both South Vietnamese and U.S. channels. However, South Vietnamese battalions were decimated and the U.S. advisors assigned to them were lacking critical information. U.S. forces were lacking sufficient detailed information to plan operations, and even intelligence gathered by Special Forces proved inadequate. The United States took a more cooperative approach to combining intelligence operations systems with those of the South Vietnamese. However, language and cultural differences proved to be significant obstacles preventing the success of melding collection, processing, analysis, and dissemination methods of intelligence. Different perceptions of needs, priorities, and political constraints kept the U.S. respecting international boundary lines while the lines held no significance to the enemy. The rate at which a command could accept requests and apply additional intelligence assets limited availability for time-sensitive tasking.

Special security programs, such as signals intelligence (SIGINT), performed less than satisfactorily in the eyes of tactical commanders in Vietnam. The issue was never the lack of units or equipment, but rather the releasability of collected SIGINT to tactical commanders. Security clearance procedures were rigorously followed to the point where battalion commanders were routinely denied access to timely readouts of SIGINT intercepts.

New arrivals came to Vietnam each day, but they were undertrained and woefully lacking in experience. The impact of these initial shortcomings were felt at every level of command.

The U.S. Army's Military Intelligence branch was not formally established until 1962. A quick inventory of personnel revealed that only a modest number of specialists and very few officers were fully qualified to conduct G2-level duties. The output of personnel was increased over time, but they were unable to respond directly to special joint and combined operational requirements. The training curriculum at that time still focused on the CONUS counterintelligence mission and European threat collection needs. New arrivals came to Vietnam each day, but they were undertrained and woefully lacking in experience. The impact of these initial shortcomings were felt at every level of command. In particular, surveyed commanders felt this impact in the earlier campaigns of the war.

Moving to Afghanistan, during the initial planning phases of Operation ANACONDA, the Intelligence Community could not come to a consensus on the number of enemy fighters and their capabilities. Estimates ranged from high to low but, ultimately based on little current data, the assessment was that Al Qaeda and the Taliban would not put up staunch resistance. Additionally, it was believed that the enemy fighters remained in mountain villages and were never deployed in the surrounding mountainsides. Another commonly held belief was that they would flee the valley while facing overwhelming odds. If they were cornered, it was assessed that most fighters would surrender. Reflecting on these decisions and how the operation actually occurred, a majority of these assessments came from CENTCOM HQ at

MacDill Air Force Base, Florida. Thousands of miles away from Afghanistan, intelligence professionals created assessments based on older data and did not seek to deploy human intelligence (HUMINT) intelligence assets to develop knowledge of the local area where the operation would occur, nor did they seek to understand the current mindset of the enemy force.

Once the Operation ANACONDA plan failed at the very beginning of execution, a multi-headed command structure squabbled and could not determine the responsibilities of joint commanders. General Franklin Hagenbeck, named as commander of the Coalition and Joint Task Force (CJTF), would have command and control authority over those involved in the operation. However, he did not have command over air component forces or friendly Afghan forces. This limited his ability to make decisions based on incoming intelligence from SOF forces in Task Force Dagger (TFD), which assisted the Afghan forces on the ground. The ability to respond to erroneous intelligence estimates and develop decisions and assessments based on incoming data from Special Forces did not allow joint forces in the fight to react quickly.

An issue with the Iraq War was the reuse of intelligence from Operations DESERT FOX, STORM, and SHIELD operations plans (OPLANs) that focused on the defense of Kuwait. To develop an offensive plan rather than a defensive plan, CENTCOM reused the same data, but approached the analysis of the enemy in Iraq in a linear, militaristic manner. Hardly any analysts expected the insurgency to swell to the degree it did in the initial years of the Iraq War. The National Intelligence Estimate used to flesh out the war planning relied heavily on existing products in the Intelligence Community.

As security presented an impediment in Vietnam, so too did Iraq War planning face similar hurdles. The OPLAN for the invasion of Iraq was compartmented to such a degree that only a few people at CENTCOM HQ worked on developing it. Steady leaks to the press about the nature of plans being developed at CENTCOM increased security pressures even more. Additionally, methods to cut corners for the sake of brevity such as Microsoft PowerPoint abbreviated operations planning points and took away most of the deliberative and cognitive process required to read, understand, and inform senior decision-makers. Additionally, as in Operation ANACONDA, there were debates on the amount of resources and number of troops required. These estimations were built on the understanding of Iraqi military capability and performance. They did not, however, factor in insurgency or any other variables that would extend the campaign

A lack of tactical intelligence was not what plagued the intelligence constructs of the Vietnam, Afghanistan, or Iraq Wars. Instead, when studying the issues across the span of decades, it becomes apparent that organizational structure, compartmented information access, and analytical complacency seemed to be the prime factors in what caused intelligence strife. In Vietnam, few were experienced enough to conduct intelligence analysis or collection on Vietnamese culture, and officers capable of being a theater G2 were in short supply. In Afghanistan, a distant CENTCOM HQ created and planned Operation ANACONDA around assessments that relied upon outdated data. Additionally, the multi-headed coalition and joint command structure inhibited the ability to process and plan on newly received intelligence after the initial plan failed. During the Iraq War, security restrictions prevented a wider audience from analyzing the OPLAN to search for previously unobserved intelligence gaps. Additionally, Iraq War estimates on the appropriate quantity of troops and supplies needed for the operation were severely low due to the preconception of a traditional military conflict without weighing unknowns such as insurgency.

References:

Hooker, Gregory. “Shaping the Plan for Operation Iraqi Freedom.” The Washington Institute for Near East Policy, No. 4, 1-132.

Johnson, John, et al. 1976. “Analysis of Tactical Intelligence Experience in Southeast Asia.” General Research Corporation, 1-27, 33-86.

Kugler, Richard. 2007. Operation Anaconda in Afghanistan: A Case Study in Adaptation in Battle. Office of the Deputy Assistant Secretary of Defense.

Luke Holloman is a U.S. Navy Veteran and former enlisted Intelligence Specialist. He has a BA degree in Intelligence Studies with a concentration in Geospatial Intelligence (GEOINT). His previous experience includes serving as an imagery instructor for Navy special operators, as well as an operational intelligence analyst, imagery analyst, and targeting planner. After the service, he provided near-real-time full motion video analysis for MQ-1 Predator and MQ-9 Reaper remotely-piloted aircraft missions vital to counterterrorism operations abroad. He then moved to a Defense Intelligence Agency contractor position at the Office of Naval Intelligence (ONI), where he analyzed intelligence production gaps and manning issues focused primarily on Navy acquisition mission data needs. Currently, Luke is an employee of the Department of the Navy supporting fleet intelligence engagements and analyzing key fleet intelligence man, train, and equip (MTE) issues on the N2 staff at ONI.

Strategic Intelligence for Escalating Security Issues: Its Time Has Come

by Dr. (CAPT, USN, Ret) David D. Belt

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

Two recent U.S. strategic-level strikes on Iran that many experts view as acts of war—neither of them urgently necessary, nor approved by Congress, nor subject to national debate—have significantly escalated the 40-year cold war between the U.S. and the Islamic republic, and precipitated second- and third-order implications that appear to make the U.S. and the region less secure. This article briefly examines the strategic risks that the nation incurred with only the most recent and far less consequential of these two foreign policies, and then outlines a new escalation-phase strategic intelligence analysis process whereby the U.S. Intelligence Community can better serve the sitting administration, the Congress, and the American public.

[Editor's Note: For those wondering how events occurring in January 2020 could be covered in a journal reflecting a 2019 date, during the unavoidable delay in getting all the other articles cleared, this provocative essay, which was already cleared, was submitted. I made the decision that these current, high-visibility events merited immediate coverage and could not wait for the next time a non-student could publish in *AIJ*, i.e., late 2020.]

RECENT FOREIGN POLICY AND THE RISKS INCURRED

The first strategic strike on Iran was an unparalleled regime of economic sanctions that the administration of President Donald Trump describes as its "maximum pressure" campaign, but what many security professionals view so severe as to constitute an economic blockade of this country of 80 million, with whom we are not at war. Even preventing Iran from importing crucially important food and over $3 billion in life-saving medicines, this economic form of warfare promises to kill more people and be more destructive generally than a major military bombing campaign of its coastal cities might have been. The many consequences of this strike promise to negatively impact U.S. national security significantly. The strike occurred when longtime Iran watchers were hopeful that the new economic success and foreign direct investment would advance the societal trend of wider cosmopolitanism and the economic trend of increasing compliance with international norms of transparency, rule of law, and so on. These unwritten international economic order rules—what popular *New York Times* journalist Thomas Friedman called "the golden straight jacket"— moderate even the most rogue of regimes, if they are allowed to join the system. This strike ignores the 40 years of sanctions which hindered that process and proved to be an abysmal failure in dislodging the hardliners in favor of reformists.

The second strategic-level strike was the dual assassination of the region's two most popular counterterrorist military leaders—Iran's Islamic Revolutionary Guard Corps (IRGC) Qods Force (special operations) commander General Qasem Soleimani and Iraq's Shiite militias deputy leader Abu Mahdi al-Muhandis—after Soleimani arrived via a commercial airliner at Baghdad's commercial airport at the request of Iraq's prime minister. Soleimani was Iran's modern-day military savior-figure—a kind of Douglas MacArthur—whose name will forever be enshrined in Iran for his defeat of the Islamic State group, or ISIS, and whom many experts believed would be the country's next Supreme Leader. A University of Maryland survey in 2019 revealed that Soleimani was more popular than anyone in the country, with 82 percent of Iranians holding a positive view of him and 59 percent a highly positive view. Similarly, Muhandis was a revered figure among Iraqi Shia for his ability to meld Iraq's disparate militias into a force that would eventually beat ISIS. Consequently, the U.S. assassination of both of them in the capital of Iraq was fraught with risks, as we will soon see.

The problem with these two war-like strategic strikes is that, by all insider accounts, they occurred outside of and without the assistance of the broader national security establishment. The latter strike—again, by all insider accounts—seemed particularly hurried, and took place

without supporting national intelligence estimates, without notification of Congress, and even without the minimalist check of notifying the Congressional bipartisan "gang of eight" as required by 50 U.S.C. § 3093(c)(2), who have otherwise been privy to urgent strikes of opportunity against pre-approved targets such as key leaders of non-state actors like al-Qaeda and ISIS.

The latter of these two strikes better reveals the vulnerability gap in our national security apparatus. It reveals how major decisions with reasonably probable significant consequence to national security can be made without the necessary checks and balances. Before we examine a simple, low-cost opportunity to improve the process, however, it is helpful to examine briefly just three of the latter strike's consequences for national security—risks that even the narrowest, least-informed elements of our national security enterprise were prevented from considering.

Demobilizing Gradual Reformist Movement in Iran

A first big risk of this latter strategic strike was that of demobilizing the Iranian peoples' growing reform movement against the Islamic Revolutionary regime in Iran. We should not forget the context in which both of these strategic strikes were launched. Despite the early regime's gains of Islamization of society, the bulk of Iran's populace is not nearly as susceptible to indoctrination into the much narrower Khomeinist paradigm as those who suffered under the U.S.-backed Shah and went through the revolution and the war. The major societal and cultural megatrend in the world since that time has been toward individualism or liberalism—catalyzed by globalization of business, popular consumer products, fashion, music, literature, and major films, which are themselves catalyzed by international satellite television, the Internet, YouTube, and other social media. Because of the nature of Persian culture, Iran is not immune to these profound inter-cultural forces, and might be even more susceptible to them than any nation remotely near it. Urbanized, educated youth are the most susceptible to countercultural revolutions or worldview changes, and 60 percent of Iranians are under 30 years old, 50 percent more urbanized, vastly more educated, and have assimilated globally-available identities and more universalist governmentalities. Perhaps most of the 75 percent of Iranians living in cities are increasingly resisting government restrictions through underground culture and subtle forms of protest. Instead of public piety driven by an inward sincere worldview, religiosity in Iran is increasingly more pragmatic and self-sanctions driven merely by the desire to avoid the consequences of Iran's religious police and law.

The Iranian people—while anti-American due to U.S. foreign policy and discourse which they interpret as hostile to Muslims—increasingly prefer a more historical, Persian-based nationalist pragmatism and interaction with the international community over the more hardline or principalist urges of Islamist "resistance." President Hasan Rouhani's decisive 2017 victory over fundamentalist and isolationist Ibrahim al-Raisi illustrates precisely that. Intimidated and politically quiet since the crackdown on the Green Movement in 2009, the past three years have witnessed a respectable gradual movement that vocally opposed not just certain policies of the regime, but opposed the very continued existence of Khomeinism's innovative clerical rule. Using social media, the protesters were rebelling by posting everything from religious texts to nude photos to political commentary, and over half of all Iranians are using these social media platforms like Telegraph.

These trends, therefore, are by far the biggest threat to the Islamic revolution, and it is in this vein that General Soleimani complained about how seminary enrollment had plummeted and how the Western cultural invasion was destroying the Islamic fervor and piety of Iran's youth. Moreover, it was these trends that explain the hardliners' resistance to the JCPOA, or nuclear deal—which flung wide open Iran's gates that kept the world and its values out, and loaded rocket fuel into Iran's ongoing second revolution—or its counterrevolution—toward a more politically secular and liberal Persian nationalist state.

The more hardline regime led by the old guard realizes that these social megatrends are against it, but it is nevertheless a case of both being faithful to their religious principles by resisting this tide—as an act of obedience and worship—and being more pragmatic in hoping to stave off a destructive Gorbachev-like moment. Observing the Soviet demise, the old guardians of the Islamic revolution in Iran seem careful to avoid the catastrophe we witnessed when that primarily revolutionary ideological regime rapidly fell back to the more pragmatic earth.

Although the regime was resisting this ongoing counterrevolution at the cultural level, it had also been changing in subtle ways up to the point of the U.S. strategic strike. Apart from its public discourse, which was a kind of separate realm, the regime was becoming more materialistic and less revolutionary. Moving away from the ideological foundation of the guardianship of the Islamic jurist, Iran's regime has been slowly moving toward the more materialistic foundation of the guardianship of the deep state military, under the leadership of the Revolutionary Guard. Khomeini's famous quip that—from the Islamists' view—the revolution was not about the price of melons is no longer true. Today's regime is comprised of several structures which have been taking full advantage of the economic structure to advance its individual interests. These are the guardians of the system that produces their golden egg, but seem to care less about faithful obedience or *taqlid,* and thumb their noses at

the Supreme Leader when he subtly begs them to undertake the necessary economic structural reforms. Khamenei himself is a hypocrite who owns vast swaths of the Iranian economy, with the Revolutionary Guard controlling up to 30 or 40 percent of it.

...the vast majority of Iranians do not want an outside-forced regime change. They and the world know that both Iran and its regime are changing, and it should have been clear that all the U.S. had to do was follow the Hippocratic Oath and "first do no harm," thereby gradually winning back the street's hearts and minds.

As this more materialist trend in the regime meets the counterrevolution outside of it, the most logical next evolutionary leap might be a soft, unwritten handover of the supervision of Iran's Islamic democracy to the military, the Artesh, with the IRGC as "the Power" behind the scenes, following the pattern of Algeria and Egypt. That is a logical step to another more incremental phase of increasing liberal democracy, even though it remains technically illiberal, with an Islamist judiciary and a Supreme Leader who functions much like Iranian-born Ayatollah Sistani does in Iraq, under a more technocratic form of governmentality, or *veleyat-e-umma*.

Watching all of this and knowing that time is on its side, Iran's next generation has pragmatically been biding that time, moving slowly—not wanting to risk the country's demise by another destructive revolution, like that in Syria, in Iraq, in Yemen, and in Libya. It is in this context that recent polling shows that the vast majority of Iranians do not want an outside-forced regime change. They and the world know that both Iran and its regime are changing, and it should have been clear that all the U.S. had to do was follow the Hippocratic Oath and "first do no harm," thereby gradually winning back the street's hearts and minds.

In that mode of thinking, there was a range of options that could have kept us in the "do no harm" realm. Political movements in Iran to this point have succeeded only when they built on mass anger against foreign interference, such as the anti-British tobacco movement in 1891, the anti-American and anti-British nationalist movements in the 1940s-50s, and the anti-American and pro-Islamic movements leading to the 1979 revolution. The reformist protests in recent years have been different in that they were the people uniting against their own government's interference and ineptness. Surely, all the U.S. had to do was nothing to take the movement's eye off the domestic enemy.

Another strategy option available with Iran prior to the recent strategic strike plays on the basic axiom of warfare and statecraft—in Sun Tzu's words: "When [your enemy] is united, divide him." Here we might think of a range of ways to advance the reformist narrative and counter the hardliner narrative, by acting in ways that legitimize the former and delegitimize the latter. However, some attacks on a regime—whether kinetic, or discursive, as was the case with President Bush's "axis of evil" statement—can have the opposite effect and unite a weak and divided regime. The U.S. saw this with 9/11 and, in this vein, when Saddam Hussein launched the war on Iran, Ayatollah Khomeini famously quipped how it was "a divine blessing" because it demobilized the regime's opposition. The assassination of Soleimani was a similar and easily predictable divine blessing for the hardliners in the regime. Even the most critical of the regime—2009 Green Movement opposition leaders, novelists, former political prisoners, and even Western-based journalists—joined with the millions of others, to include the regime's hardliners and allies, to protest.

President Trump followed up with a message on Twitter that the U.S. would hit 52 important Iranian sites, even cultural sites, if the regime retaliated. Here again, this unites the people behind the regime because this great nation's cultural sites do not belong to the Islamic revolutionary regime; they belong to the Iranian and Persian peoples—past, present, and future. These places are in their history books and in their songs, and are key identifiers for them.

Even though Soleimani's assassination was a strategic blow mainly to Iran's young reformers and to U.S. national interests, it probably will set back the ongoing revolution for only a few years. The removal of any individual from the battlefield of ideas has never threatened the ideas themselves, and here the global megatrends are in the reformists' favor.

Demobilizing the Iraqi Nationalist, Reformist Revolution

A second big risk of the dual assassination of Iran's and Iraq's more popular anti-ISIS heroes was that of demobilizing Iraq's own reformist movement. The world has watched over the past three months as mostly young Shia protesters across the country—at a cost of over 500 dead and over 20,000 injured—demanded an end to corruption, a more representative and effective government, economic development for jobs, freedom of speech and the press, and—something entirely lost on the advocates of this strike—a rollback of Iranian suzerainty over Iraq. Anti-Iran, nationalist sentiment in Iraq had skyrocketed during this time, and the revolution's momentum was gaining, resulting first in the resignation of the Iran-brokered Prime Minister, and then the important backing and even protection of nationalist

Shia cleric and militia leader Muqtada al-Sadr. With this kind of momentum, President Barham Salih had the political opportunity to heed the protester demands and reject the two candidates for prime minister put forward by the pro-Iran Fatah parliamentary bloc. Given that momentum, some Iraqi elites were willing to compromise with the protesters, against the will of the more corrupt and pro-Iran elite. Two-hundred thousand U.S. troops, and a trillion dollars of bribes, could not have achieved this strategic gain.

...this strategic strike has demobilized the protest movement and forced the national debate from the internal self-critical governance reform to an outward focus on those who violate Iraq's sovereignty.

The fact that it is a Shia-led movement trying to evict Iran from Iraq is crucial. Sometimes we forget that the Iraq which the U.S. liberated was majority Shia, and—given Iran's support during the cold war between Saddam's Baathist minority and its Shia majority—no small segment of them looked to Iran as their fictive kin and to Khomeinism as their own doctrine. Thus, U.S. policy from the start should have been carefully supportive of the rising nationalist Sadrist movement, even though it was equally hostile to U.S. occupation. In other words, a staunch Shia nationalist, Al-Sadr—although equally opposed to U.S. occupation of his country—was the greatest force up until the Shia protest movement for checking Iranian satrapy. Yet, the U.S. from the beginning tried to destroy al-Sadr and his movement by backing his pro-Iran rivals.

The dual assassination of the two leaders credited by most Iraqis as defeating ISIS has predictably forced al-Sadr to withdraw his support from the reform movement, to tilt his geopolitical framework from nationalism to pan-Shiism, and to join the pro-Iran camp to evict the U.S. presence from Iraq and the region. President Trump's staff obviously had not conveyed the strategic security environment in Iraq—evidenced by his tweeting that Iraq, not Iran, would experience the most severe sanctions ever if it did not allow the U.S. military to stay. Most members of Iraq's Council of Representatives remember the U.S. sanctions regime that forced Saddam to narrow his patronage tightly among Sunnis from his hometown area, thereby causing more sectarianism and producing 500,000 to one million deaths—25 to 54 times the U.S. casualties in Vietnam on a per capita basis. It is in this context that al-Sadr ordered his supporters and militia to stop protecting these anti-Iran Iraqi nationalist protesters.

Thus, this strategic strike has demobilized the protest movement and forced the national debate from the internal self-critical governance reform to an outward focus on those who violate Iraq's sovereignty. This means that political elites like al-Sadr who were key to the reform movement are now forced to fall in line behind the broader movement to defend the nation's sovereignty against what most Iraqis view as their distant enemy. The crowds that protested the assassination were different from the reformist protesters in Tahrir Square; they were part of the 90 percent of Iraqis who—according to a 2016 poll—see the U.S. as an enemy.

It also means that the U.S. will lose its bases in Iraq, or once again become an occupier in the minds of the many who might thereby become influenced by the narrative of pan-Shiist resistance. More like prisoners than trainers, U.S. troops will be under high risk of "fragging" by the very Iraqi troops whom they are there to assist in the fight against a resurgent ISIS.

Strengthening Pan-Shiist Resistance and Iranian Soft Power in Iraq

A third big risk in the dual assassination of Iran's and Iraq's most popular anti-ISIS heroes is that of strengthening the wider pro-Iran, pan-Shiist Islamist movement in Iraq, and thus increasing Iran's influence or soft power in that country, across the spectrum of political, military, economic, and cultural relationships at the elite and street levels.

The Iranian revolution has, since the Islamist coup in 1979 and 1980, been a pan-Islamist, pan-Shiist, resistance-minded religious revolution, aimed at eliminating Western influence. Because of pan-Shia nationalism in the face of a rising tide of Sunni Shia-hating extremism, or *takfirism*, Iran has functioned as the ideological hub of a confederation of like-minded Shia Islamist movements with their own militias. To the degree that pan-Shiism across Iraq is strong is the degree that Iraqi nationalism and the ability of the state to resist Iranian satrapy will be weak. With the rise of al-Sadr and the millions of ordinary Shia who had been the base of pan-Shiism, and who now were protesting for reform and the eviction of Iran, Iran's influence has been in serious decline.

Nevertheless, the dual assassination reversed this course significantly. Soleimani and Muhandis were both what Eric Hoffer called "the true believer" in his book by that name. They were staunch defenders of the Islamic revolution and its inherent pan-Shiist project, and they worked to demobilize the more nationalist opposition to it, as seen in the killings of Iraqi protesters by their militias. By assassinating these wildly popular Shia Islamist leaders like we did, however, we have erased much of their ugly baggage, and created larger-than-life symbols who can do

far more in death for the ideological cause of the virtual pan-Shiist Islamic state than they could in life—inspiring tens of thousands of other true believers to rise and take their place. Seeing the vast opportunity created when the pan-Shiists in Iraq learned that their two icons had been martyred, an official from the pro-Iran Iraqi militia Kataib Hezbollah tweeted a call for "opening the door to registration for those who love martyrdom, to carry out martyrdom operations against the foreign crusaders."

Thus, just when we were starting to see meaningful revolution of Shia toward a new social contract and a secular or non-consociationalist constitution, this single strategic strike tends to push Iraq into strategic alliance with Iran and to shift its political culture toward a more pan-Shiist, anti-American identity.

THE OPPORTUNITY FOR ESCALATION-PHASE STRATEGIC INTELLIGENCE

The fact that our nation can so readily be subjected to strategic-level consequences like these without broader participation by the national security apparatus and even public debate demonstrates a critical vulnerability. We said that, in this case, the second strategic-level strike was enacted by sidelining Congress and even the gang of eight, as well as other parts of the national intelligence and security apparatus, leaving this huge decision with immense consequences to the whims of *a single* individual and his closest like-minded appointed advisors. The checks and balances that the framers set in place with the institution of the legislative branch are insufficient in the Information Age. The Internet's saturation of the globe has effectively rebuilt the proverbial Tower of Babel. In the era of instantaneous worldwide media, events move at light speed, and this environment is exacerbated because the U.S. military is continually omnipresent and poised to deliver strategic-level strikes—blatant acts of war—anywhere in the world on a moment's notice at the whim of the Commander-in-Chief. Therefore, the present national security infrastructure of checks and balances on the single chief executive comes far too late in this environment. In this case, it was a full six weeks after the strategic strike before the Republican-controlled Senate could overcome the bureaucracy and pass bipartisan legislation to curb the President's ability to escalate further.

That this is a systemic vulnerability can be seen in the previous two administrations when strategic-level decisions that harmed national security were left to an elected executive and a small cabal of his staff—without the checks of the legislative branch, the main parts of the national security apparatus, and public opinion. It was in this mode that the Bush administration ramrodded through the invasion of Iraq, and the Obama administration leaped headlong into regime change in Libya. Hence, rather than a one-off anomaly, this is a recurring threat to national security, and the structure of the system guarantees that it will happen again, perhaps orchestrated by the next president. In the tyranny of the urgent—in the absence of specific strategic-level knowledge or intelligence on the issues confronting them—presidents tend to bypass the more collaborative decision-making and research and follow their gut instincts.

The solution, therefore, is to check this demonstrated need or propensity to govern by gut instinct by saturating the decision space across the entire national security enterprise with strategic-level intelligence. In other words, this case demonstrates how we need a national intelligence estimate process that shifts into a kind of Defense Condition (DEFCON) One during even seemingly benign phases of conflict escalation. The goal of this mobilization is to ensure that a Commander-in-Chief, his or her unofficial and official advisors, the National Security Council, the State Department, the Department of Defense, both the Senate and the House of Representatives, and the broader national media have all of the best analysis possible during the more rapid escalatory phase of a national security issue.

What, specifically, are we talking about here? In this escalatory phase with Iran, some U.S. intelligence agencies with the Iran and broader Middle East portfolio stood up special crisis cells *after* this latest strategic strike in an effort to be ready for Iran's reaction, and to answer the harried questions from legislators who had been caught off guard. In a similar vein, the $80 billion a year U.S. Intelligence Community could be required by law to mobilize during the slightest hint that escalation of a security issue is likely to produce official strategic-level (as opposed to tactical) intelligence on the broader strategic environment surrounding the issue and the full range of reasonable shifts and scenarios, along with the full range of opportunities to act, and the range of risks associated with each policy consideration. The opportunities for action could be prioritized to give the Chief Executive and his or her staff a menu of actions that would always be helpful to our security interests, and with little risk. That is what the intelligence apparatus and its mission area of strategic intelligence is for—to prevent the nation from stumbling ill-informed into unnecessary and counterproductive wars like Iraq, or counterproductive attempts at regime change such as in Libya and Syria; to get us out of the counterproductive wars like Afghanistan; to refrain from other policy predispositions where the risks far outweigh the likely benefits; and to seize upon all opportunities to advance our interests with little risk in the short or long term.

One way to mobilize the Intelligence Community for this purpose is to task by law the National Intelligence Council (NIC), CIA, and DIA with standing up an emergency "strategic intel cell," or peer-reviewed team of experts for every security issue for which there is a potential for near-term escalation with significant consequences to national security. The three strategic intelligence cells would proactively and constantly issue analysis on the following categories: (1) the risks or consequences of a range of anticipated policies or actions; (2) a current map of the strategic environment or context in which the potential escalation is embedded; (3) the elements of the environment that are working in our favor, and thus should be preserved by any action; and (4) opportunities to shape the events into achieving our interests, including increasing our moral bank account, or soft power.

In this case, we knew that three structures in the strategic environment of the cold war with Iran were working in our favor. First, we knew that the Iranian regime was on its heels with its own reform movement, which had gained impressive strength in the previous three months. Second, we knew that the highly influential cleric and politician Muqtada al-Sadr and a broad swath of Iraqi Shia had allied into a surprisingly formidable nationalist movement, intent on severely rolling back Iranian satrapy in their country. Third, we knew that the pan-Shiist confederacy was in serious decline, due in no small part to the first and second structures. Consequently, the intelligence apparatus should have already offered a range of possible options for increasing pressure on Iran—if that was also something that strategic intelligence suggested as value-added at this stage—that did not negatively affect these elements which were working in our favor. Saturated with this kind of intelligence, the Commander-in-Chief could understand why these are on the table, and why others—however enticing in the short run—would harm U.S. national security.

Still, for more than just the President's consumption, these official strategic intelligence cells would constantly pump their updated assessments and estimates—along with minority or dissenting opinion, when it exists—into the system for everyone. By simultaneously informing not only the White House but also the wider national security apparatus, the strategic *knowledge itself* would hold all parties accountable. In other words, the published strategic intelligence—the knowledge of a security issue, including the red-cell-like analysis of different scenarios and like responses—would provide the checks and balances *and* best inform the Commander-in-Chief on the best course of action for any given situation or opportunity. It would be politically unfeasible for a president and his or her party to ignore the official intelligence that all branches of the government, including Congress, are receiving simultaneously.

It would be politically unfeasible for a president and his or her party to ignore the official intelligence that all branches of the government, including Congress, are receiving simultaneously.

During the escalation phase, most of this kind of security knowledge—including the range of options to deter or weaken the opposing regime or movement—can be unclassified. All parts of the strategic environment in Iran just discussed are common knowledge among experts on Iran, and among the Iranian regime elites and their opponents. Thus, by publishing as much of this strategic intelligence as possible in unclassified products, it can be continually and instantaneously socialized across a range of stakeholders and the national media, to shape the discourse at home, inside the opposing regime or movement elite, and among their international partners.

This addition of escalation-phase strategic intelligence is a simple and low-cost proposition for an enterprise with $80 billion in annual resources. Senior intelligence officers are constantly complaining that their present structure does not allow for the production of this kind of strategic intelligence. This low-cost strategy adds to the nation's defense in depth, and promises to enhance the Intelligence Community with respect to the larger foreign policy and grand strategy decisions.

Dr. David D. Belt has been a full-time faculty member at National Intelligence University since 2008. He has led courses and mentored thesis research involving the social analysis of security issues emerging from Muslim communities worldwide. Prior to coming to NIU, he served as Assistant Professor, National Security Studies, National Defense University, Washington, DC, where he also developed and led the global community of interest and the course "Containing Al-Qaedaism." In his military career, Captain Belt served 26 years on active duty with the U.S. Navy's Special Operations community. His article, "An Interpretive Sociological Framework for the Analysis of Threats," appeared in AIJ, *Vol. 32, No. 1, 2015, and his article, "Countering Violent Extremism with 'The Washington Playbook': How a Former Intelligence Chief Reaches for Anachronistic Scripts in His Bestselling Book," appeared in* AIJ, *Vol. 33, No. 2, 2016.*

NMIF Bookshelf

RADICAL INCLUSION: WHAT THE POST-9/11 WORLD SHOULD HAVE TAUGHT US ABOUT LEADERSHIP.

Martin E. Dempsey and Ori Brafman.
Missionday. 2018.
175 pages.

Reviewed by Todd A. Kushner, a contracted assistant professor teaching leadership and management courses in the Department of Intelligence Enterprise, College of Strategic Intelligence, National Intelligence University. He previously served with the State Department for 31 years as a Foreign Service Officer, including in the Office of the Counterterrorism Coordinator. Overseas assignments included Nigeria, Yugoslavia, Malaysia, and the Netherlands. He was detailed to the U.S. Senate Immigration Subcommittee and to Special Forces elements in Iraq. Todd holds an MS degree from the Industrial College of the Armed Forces, an MA from the University of Virginia, and a BS/BA from Southern Methodist University.

Leadership books often fall into one of three categories: (1) academic studies, (2) celebrity leaders' first-person accounts, or (3) business consultants proffering best practices. *Radical Inclusion* by University of California-Berkeley professor Ori Brafman and former Chairman of the Joint Chiefs of Staff GEN (USA, Ret) Martin Dempsey is a thought-provoking and readable work that is firmly grounded in academic research yet illustrated through compelling stories. The authors aim to "provide leaders with a theory to help them prevail in what has become a very challenging environment" (p. 160). The essence of that theory—*radical inclusion*—asserts that modern leadership is not manifested by those in authority exerting power. In the 21st century, they argue, leadership consists of creating the conditions that encourage everyone in an organization to share enthusiastically in the ownership and implementation of decisions and contribute to the organization's persistent learning. Assigned leaders in this environment do not so much command their followers but provide inspiration and make sense of things for them.

Radical Inclusion's core theory echoes sentiments offered by other recent leadership authors. The importance of understanding and exploiting the characteristics of networks, for example, was powerfully set out in GEN (USA, Ret) Stanley McChrystal's *Team of Teams*. Seth Godin (in *Tribes*, for example) described how leadership is exerted throughout all levels of an organization. Deloitte ("Diversity's New Frontier," https://www2.deloitte.com/insights/us/en/topics/talent/diversitys-new-frontier.html) research concludes that organizations need to nurture a diversity of thought internally to generate new insights and avoid groupthink. The RAND Corporation has written about the diminishing influence of facts in policymaking and, as a result, the increased power of opinion and personal experience (RAND, https://www.rand.org/research/projects/truth-decay.html). NIU's Josh Kerbel ("The Complexity Challenge," https://nationalinterest.org/feature/the-complexity-challenge-the-us-governments-struggle-keep-13698) and Debora Pfaff ("Boxed In," https://warontherocks.com/2018/11/boxed-in-the-bad-side-of-best-practices-in-intelligence/) have written about the need for new approaches to analysis and decision-making in a complex, chaotic, interconnected world.

Where Brafman and Dempsey excel is synthesizing these and other elements into concrete leadership tools punctuated by narrative case studies illustrating each one. The power of the *digital echo*—"information originating from unreliable sources…quickly amplified by being retweeted, reposted, and repeated to the point where it appear[s] legitimate" (p. 14), often abetted by confirmation bias—is illustrated by relating the competing (and somewhat mistaken) narratives spun on social media that exacerbated 2017 political violence on the UC Berkeley campus. The importance of including all employees in decision-making is illustrated by the instance of a hospital custodian who supplied the key insight that led to a reduction of antibiotic-resistant staph infections. The case studies make the offered leadership tools memorable and vivid. Employees who want to apply them should be able to understand easily how the tools can be utilized in their own workplaces.

Radical Inclusion is a quick and interesting read. Its cogent narrative often has the feel and power of a novel. Yet, there is no doubt that the book has sound scholarship and practical experience at its basis. Anyone with an interest in modern leadership should include it on his/her reading list.

BATTLING THE BUREAUCRACY: THE ROUGH ROAD TO REBUILDING THE U.S. SPECIAL OPERATIONS FORCE CAPABILITIES 1976-1989.

Richard M. Lovelace, Jr., with Rod Lenahan
and Keith Nightingale.
Sigma Press, 2016.
313 pages.

Reviewed by CTI1 (USN) Jeffrey L. Kleppe, a Middle East and North Africa languages analyst. He holds an MS of Strategic Intelligence degree from National Intelligence University and a bachelor's degree from Iowa State University. He is a career Special Operations Forces enabler and has served with Navy and Joint SOF during deployments in support of Operations IRAQI FREEDOM, ENDURING FREEDOM, and INHERENT RESOLVE. He is fluent in Arabic and Pashto.

Describing an ill-conceived meeting between Congressman Dan Daniel, Secretary of Defense Caspar Weinberger, and Admiral William Crowe, author Richard M. Lovelace, Jr., wrote: "This was an 'in the weeds' briefing and the level of detail was very unsettling to the audience" (p. 215). Regrettably, the same could be said about this book.

Despite the timeline outlined in the subtitle, Lovelace actually intended his book to cover the period bracketed by the failure of Operation EAGLE CLAW in 1980 to the overwhelming success of Operation JUST CAUSE in 1989, thereby filling what he perceived to be a significant gap in the literature of modern American military history. Lovelace's failure to achieve his objective may be attributed to three categories of errors which both harmed the book's credibility and stretched the audience's credulity—history, terminology, and sourcing.

History Errors

Battling the Bureaucracy is replete with historical inaccuracies, ranging from mild misinterpretations to broad overstatements to outright falsehoods. An example of the first is the following assertion: "Islam represented the greatest military power on earth—its armies had successfully invaded Europe and Africa, India and China" (p. 245). However, the armies of the expanding Arab Empire *never* invaded China, successfully or otherwise. The closest the Arabs came was when they defeated the forces of the Chinese Tang Dynasty at the strategically unimportant Battle of Talas River in Transoxiana in 751 CE.

Next, Lovelace pronounced the Goldwater-Nichols Act and Nunn-Cohen Amendment (which he frustratingly and repeatedly referred to as the "Cohen-Nunn Amendment") the "two most important pieces of transformative Defense Legislation in the previous sixty years" (p. 204). How either of these pieces of legislation can be viewed as more "important" and "transformative" than the National Security Act of 1947, which created the Department of Defense, the United States Air Force, the National Security Council, the National Security Council, and the Central Intelligence Agency, is left as an exercise for the reader.

In Chapter 12 (an otherwise independent and unnecessary "Primer on Islam and ISIS"), Lovelace sought to summarize the genesis of the rift between Sunni and Shia Muslims by boldly asserting that "in 656 Ali's Shiites killed the Sunni Caliph ['Uthman ibn 'Affan]." This is, as the late Justice Antonin Scalia would have said, "pure applesauce." Not only were Shiites not responsible for 'Uthman's death, Shiite and Sunni historians alike agree that Ali's sons Hasan and Husayn were present at 'Uthman's besieged compound and attempted to defend the caliph from the rebels who would ultimately assassinate him.

Other notable historical inaccuracies included stating that the 23rd Air Force was headquartered at Scott Field in Illinois in 1985 (Scott Field had become Scott Air Force Base over 37 years earlier) (p. 178); writing that Iraq and Syria were part of the Ottoman Empire "as late as 1848" (the Ottomans retained control of that territory for 70 years longer) (p. 256); and saying that "SOF forces [*sic*] were the lead elements in the successful invasion of Iraq in 1993," during which the operators were presumably inserted via cruise missile (p. 242).

The worst historical injustices, though, are the treatments the author gave to Operations EARNEST WILL and JUST CAUSE. The former—despite being the first tactical operation of United States Special Operations Command ("USSOCOM" in the real world, "USSOC" in the book)—is not mentioned at all. The latter received a paltry *six sentences* of coverage, even though it was one of Lovelace's own self-determined bookends.

Terminology Errors

Although it is not apparent who the book's intended audience is, it is safe to say that if it were aimed at readers with even a passing familiarity with military or other national security topics they would be turned off quickly by its clumsy grasp of common terminology. A non-exhaustive list of terminology errors follows:

Lovelace named the capitals of Iraq, Iran, and Somalia as "Bagdad" (p. 7), "Teheran" (throughout), and "Mogadischu (p. 34), respectively. He referenced heretofore unknown places such as the "Russian Federal Republic" (p. 259),

"Peoples [*sic*] Republic of Korea" (p. 260), and the "Parcels" (p. 260). He also occasionally mixed up Iraq and Iran, leading to humorous results (e.g., p. 256).[1]

Consistency with terms was likewise lacking. "SEAL" in one paragraph would become "Seal" in another. "DELTA" was used interchangeably with "Delta," as were "DOD" with "DoD," "Qur'an" with "Koran," and "Muslim" with "Moslem" and even "Muslin." Times were represented using an impressive variety of conventions, liberally peppered throughout: 7:00 a.m., 3:00 A.M., 3 p.m., 5:00 AM, 10:00 p.m., 0445, six o'clock, and four thirty were all encountered. Dates were recorded with similar abandon. One remarkable sentence read "[General] Secord described Reza Pahlavi, the leader of Iran, from 19 September 1941 to February 11, 1979" as "The Shah" [*sic*] (p. 52).[2] The list of Theater Special Operations Commands ("TSOCs" in the real world, "SOCs" in the book) was missing SOCNORTH and SOCAFRICA but did include SOCACOM, which was disestablished in 1999.[33] The author stubbornly insists that SOCACOM is currently a subordinate unified command of U.S. Atlantic Command and headquartered in Norfolk, Virginia, writing that "SOCACOM is responsible for planning and conducting joint/multinational special operations throughout USACOM" (p. 286).

Lovelace used both "stol" and "stoll" in place of "STOL" throughout the book, such as when he renamed the XFC-130H "Super STOL" the "Super Stoll C-130" (p. 281).[4] He repeatedly rendered MacDill Air Force Base, home of USSOCOM, as "Mac Dill" (p. 7 and throughout), defined CONPLAN as "Concept Plan" (p. 7), and confused Fatah with the Palestinian Liberation Organization on the very first page of the book.

Sourcing Problems

In the acknowledgments section, Lovelace wrote, "normally recognition for ideas and words borrowed from another or another's writings are accorded only footnote or suffix recognition" (p. 263). Despite this clear admission, *Battling the Bureaucracy* is utterly devoid of any footnotes or endnotes, leaving readers to wonder where the author discovered some of the book's more outlandish claims.[5]

Lovelace also insisted that he "[drew] from a large collection of written works about the topics contained in [*Battling the Bureaucracy*]," but his bibliography has only 21 entries—and only 15 related to Special Operations topics (p. 275). Additionally, despite flatly asserting that "the bulk of this information in this book is based on interviews with the participants," the bibliography cites only a single interviewee (p. 275). Finally, through the author's own admission he reached out only to officers from the Army, Air Force, and Marine Corps for assistance with his book. Perhaps this explains the aforementioned absence of EARNEST WILL, a Navy-centric operation that one would reasonably have expected to find in a book purporting to examine the history of American Special Operations in the 1980s.

Lovelace, an attorney, one-time Army officer, and author of such tomes as *Dealing with Women: A Survivor's Guide*, had lofty ambitions for *Battling the Bureaucracy*. Unfortunately, whichever "gap" he apprehended in the literature and which prompted his pen has only broadened as a consequence of his failure.

[Reviewer's Note: The views presented here are my own and do not necessarily represent those of the *AIJ*, the United States Navy, or the U.S. government.]

[Editor's Note: This journal does not normally publish such negative reviews of books, operating on the concept that if one cannot say something nice one should probably not say anything at all. However, this book had such egregious errors—astutely pointed out by a former NIU student—despite being about such an appealing subject, that I felt it necessary to get the word out. This subject will likely appeal to many *AIJ* readers, who may want to read the book anyway. That is understandable, but they should be forewarned there are many distractions due to obviously terrible editing. I believe this publisher, whose website does not even indicate where it is located, must be one of those vanity publishers which tend not to maintain the same high standards that professional publishing houses take seriously.]

NOTES

[1] Other (probably unintentionally) humorous moments include referring to GSG 9 as Germany's "in-extremist" [*sic*] force (p. 5), stating that a problem had the complexity of an "eight-sided Rubik's Cube" (p. 250) and the appearance of "high-jackings" throughout.

[2] One cannot help but wonder if anyone other than General Secord ever described Reza Pahlavi as "Shah."

[3] The author stubbornly insists that SOCACOM is currently a subordinate unified command of U.S. Atlantic Command and headquartered in Norfolk, Virginia, writing that "SOCACOM is responsible for planning and conducting joint/multinational special operations throughout USACOM" (p. 286).

[4] It is also worth mentioning that the author conflated the XFC-130H development project (Credible Sport) with the aircraft itself (p. 281).

[5] While the book likewise lacks an index, it does include a glossary, albeit one in which the terms are not in alphabetical order.

STRATEGIC INTELLIGENCE–COMMUNITY SECURITY PARTNERSHIPS: MOLDING PARTNERSHIPS IN CONFLICT-PRONE REGIONS.

Maiwa'azi Dandaura-Samu.
Lanham, MD, Lexington Books. 2018.
318 pages.

Reviewed by Dr. Duane C. Young, a retired Army officer with two decades of experience in Armor/Cavalry and MI branches. He is currently Director of the Master of Science of Strategic Intelligence (MSSI) degree program in the College of Strategic Intelligence at the National Intelligence University, where he has taught since 2004. When not directing NIU graduate student research, he engages in private research and writing on defense strategy and security topics, including terrorism and asymmetries in conflicts, and also focuses on military transformation and modernization.

Maiwa'azi Dandaura-Samu, the author of the reviewed work, *Strategic Intelligence–Community Security Partnerships*, received his PhD in Conflict Analysis with specialization in Security and Intelligence Design from Nova Southeastern University, and is a consultant in conflict, security, and intelligence with the Justice and Human Security Initiative (JUHSI) USA.[1] His research interests include "Conflict, Trauma, and Resilience Research" and "Preventive Counterterrorism for Sustainable Peacebuilding," focusing on a case study of Nigeria and Boko Haram.[2] He is also the author of *Strategic Security Public Protection*, as well as a number of articles and short pieces posted to social media sites, and to open-access academic sites such as Academia.edu.[3] The work under review takes its place in the wider milieu of studies of the increasingly complex global security environment of the early 21st century, alongside works such as David Omand's *Securing the State*; the edited volume by Leslie Kennedy and Edmund McGarrell, *Crime and Terrorism Risk: Studies in Criminology and Criminal Justice*; and John Robb's *Brave New War: The Next Stage of Terrorism and the End of Globalization*.[4] Indeed, this is a global environment that former U.S. President Barack Obama once described as having "always been messy."[5]

The title of Dr. Dandaura-Samu's book does not adequately begin to suggest the variegated and nuanced topics contained within. In his book, the author examines what he sees as the need to bridge a gap between the functions of those agencies of a government charged with the creation of strategic intelligence for national security and the need for interaction by those agencies with their own societies in what he terms "community collaboration."[6] As a consequence, and undoubtedly as a result of his first-hand experiences as a native of Nigeria, Dandaura-Samu sets out in this work to explore the relation between intelligence collection and analysis, and the conduct of security operations in conflicts, with special focus on the ongoing insurgency in Nigeria waged against the government by the Islamist terrorist insurgency known colloquially as Boko Haram (to give it its full name, *Jama'atu Ahlis-Sunna Lidda'Awati Wal-Jihad* or, in Arabic, "People Committed to the Prophet's Teachings for Propagation and Jihad").[7] In the author's view, that conflict has been characterized by the Nigerian government's and its security forces' "dysfunctional intelligence collection and processing system," with resultant "colossal failures of intelligence" in what he terms "the Boko Haram war."[8] In this book, Dandaura-Samu argues that the problems he asserts regarding the Nigerian government's efforts can be solved through "community collaboration."

An interesting perspective taken by the author in advancing his argument is to elaborate on the nexus of intelligence collection and academic research, noting their similarities of approach in discussing the role of information gathering and intelligence production supporting security operations. Dandaura-Samu notes how analysts and academicians alike use analytical frameworks, process theories, must demonstrate critical thinking, and use pragmatic approaches in data analysis to provide a seamless end-product for effective decision making, regardless of the ultimate consumer of their work, whether policymakers, businessmen and women, or military strategists. Regarding security operations and forces, Dandaura-Samu insists that the opinion of and perceptions of those entities by the public matters. Therefore, government leaders must shape the public's views by using collected information and intelligence generated by cooperation with and from the community to better protect the community from harm at the hands of terrorists and insurgents. However, he warns that the intelligence/community collaboration will succeed only where security forces and intelligence agencies successfully frame public opinion.[9]

The book is divided into an introduction and ten chapters, the latter varying in length from as few as eight to as many as 78 pages. Two of the early chapters present the reader with a synopsis of the intelligence cycle. Chapter One, "Strategic Intelligence, the Community, and the Crime," relates the cycle to the community, especially because of the "gaps [that] existed in the community-security agencies' two-way collaboration in the fight against BH" (Boko Haram).[10] Chapter Three, in contrast, reads very much like a basic primer for junior intelligence analysts and for "cops on the beat" in how the intelligence cycle relates to processing collected crime data.[11] Subsequent chapters begin to get at the heart of his argument in favor of "community collaboration."

For this reviewer, the two most interesting chapters, which included the longest, encompassed the heart of Dandaura-Samu's research. Chapters Four and Five presented a series of case studies built on the narratives of Boko Haram operatives. In the first of these, short case narratives review details of the Boko Haram personnel engaged in intelligence gathering against the Nigerian government, security forces, and people.[12] In the second are cases concerning Boko Haram operatives who were engaged in attacks on the Nigerian security forces and people.[13] The penultimate chapters outline the steps based on creative thinking that in the author's view are required to reform the intelligence apparatus in states, such as Nigeria, suffering from a lack of public trust in the security forces, and a lack of a proper intelligence apparatus to support the security forces. These steps lead the reader through developing a security strategy applied to the complex contemporary Nigerian security challenges, but with application more widely and regionally.[14] The book ends with the author's proposal for the establishment of a specific mechanism that he labels "Citizens Police Project" (CPP). The CPP would be supported by intelligence derived from a combination of community-based information gathering and academic research, subjected to rigorous analytical frameworks.[15]

Dr. Dandaura-Samu's work is a fairly "easy read," although delving into his text can in a few instances be tedious for someone not keenly interested in an introductory tutorial on the intelligence cycle, for example. Nonetheless, on the whole he labors successfully to present a cogent and well-documented elaboration of this important topic. On balance, I would recommend the addition of his work both for the personal as well as for academic libraries of persons and institutions with an interest in how states can adapt intelligence gathering and security policy for better integration with their communities in the ongoing struggle with terrorists and insurgents, whether Islamists or otherwise.

NOTES

[1] "Maiwa'azi Dandaura Samu," https://independent.academia.edu/MaiwaaziDandauraSamu.

[2] See for example, Maiwa'azi Dandaura-Samu, *Boko Haram Conflict Research/Analysis & Management; Preventive Counterterrorism and Sustainable Peacebuilding: Nigeria and Boko Haram Case Study* (Lancaster, PA: Center for Justice and Peacebuilding, Eastern Mennonite University, 2012).

[3] Maiwa'azi Dandaura-Samu, *Strategic Security Public Protection*: *Implications of the Boko Haram Conflict for Creating Active Security & Intelligence DNA-Architecture for Conflict-Torn Societies* (Lanham, MD; Lexington Books, an imprint of Rowman & Littlefield Publishers, 2016). Examples of the author's work include "De-Modernization, De-Westernization, De-Secularization and Takeover of the International Systems and World Order by Islamic Thawra Al-Alamiyya," *The Bridge International*, http://www.bridgeinternational.org/page/19/wordfence_logHuman=1&hid=C943C451033CF8D95C46C899B7E81C85; "Development-Conflict-Insecurity-Poverty Gridlock & Sustainable Peacebuilding Tools," https://www.academia.edu/16276053/DEVELOPMENT-CONFLICT-INSECURITY-POVERTY_GRIDLOCK_and_SUSTAINABLE_PEACEBUILDING_TOOLS; and "Frameworks for Engaging Terrorism & Ethno-Religious Violence," https://www.academia.edu/6778009/FRAMEWORKS_FOR_ENGAGING_TERRORISM_and_ETHNO-RELIGIOUS_VIOLENCE.

[4] David Omand, *Securing the State* (Oxford, UK: Oxford University Press, 2015); Leslie W. Kennedy and Edmund F. McGarrell, eds., *Crime and Terrorism Risk: Studies in Criminology and Criminal Justice* (New York: Routledge, 2011); and John Robb, *Brave New War: The Next Stage of Terrorism and the End of Globalization* (Hoboken, NJ: John Wiley & Sons, 2007).

[5] Justin Sink, "Obama: Media Makes You Think 'World Is Falling Apart'," *The Hill*, August 29, 2014, http://thehill.com/homenews/administration/216281-media-makes-you-think-world-is-falling-apart, accessed October 31, 2019.

[6] Maiwa'azi Dandaura-Samu, *Strategic Intelligence–Community Security Partnerships: Molding Partnerships in Conflict-Prone Regions* (Lanham, MD; Lexington Books, 2018), viii.

[7] *United Nations Security Council*, "JAMA'ATU AHLIS-SUNNA LIDDA'AWATI WAL-JIHAD (BOKO HARAM)," https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list/summaries/entity/jama%27atu-ahlis-sunna-lidda%27awati-wal-jihad-%28boko, accessed November 11, 2019.

[8] Dandaura-Samu, *Strategic Intelligence–Community Security Partnerships*, vii.

[9] Dandaura-Samu, *Strategic Intelligence–Community Security Partnerships*, 239-248.

[10] Dandaura-Samu, *Strategic Intelligence–Community Security Partnerships*, 31.

[11] Dandaura-Samu, Chapter Three, "Intelligence Analysis, Crime Data Analysis, the Analytic Process, and the Workforce," *Strategic Intelligence–Community Security Partnerships*, 55-79.

[12] Dandaura-Samu, Chapter Four, "Terrorist Pre-War and War Covert Intelligence Operations," *Strategic Intelligence–Community Security Partnerships*, 81-94.

[13] Dandaura-Samu, Chapter Five, "Narratives of Extremist and Fundamentalist Attack Incidents and Relations," *Strategic Intelligence–Community Security Partnerships*, 95-171.

[14] Dandaura-Samu, Chapter Six, "Collaborative Intelligence: Community Essentials"; Chapter Seven, "Sustainable Culture of Peace, Strategic Peace Building, and Peacetime Intelligence Operations"; and Chapter Eight, "War Theater Public Safety Strategic Community Intelligence Operations," *Strategic Intelligence–Community Security Partnerships*, 173-194, 195-210, 211-260.

[15] Dandaura-Samu, Chapter Ten, "Citizens Police Project," *Strategic Intelligence–Community Security Partnerships*, 277-289.

INSPECTOR OLDFIELD AND THE BLACK HAND SOCIETY: AMERICA'S ORIGINAL GANGSTERS AND THE U.S. POSTAL DETECTIVE WHO BROUGHT THEM TO JUSTICE.

William Oldfield and Victoria Bruce.
New York, Touchstone. 2018.
336 pages.

Reviewed by Dr. Robert D. Gay, Jr., who is a federally-contracted Associate Professor in the College of Strategic Intelligence, National Intelligence University, in Bethesda, MD, where he teaches both international political economy and international relations. He holds an MA degree in Economics from the University of Oklahoma and a DBA in Business Administration (Finance) from Nova Southeastern University. Prior to his teaching career, Bob served in the U.S. Air Force and in 2016 retired following 20 years as a special agent with the FBI.

When I first read the title of this book, I could not help being reminded of the short story authored by Sir Arthur Conan Doyle concerning the characters Sherlock Holmes and Dr. John H. Watson titled "The Adventure of the Red Circle," named after a secret Italy-based criminal organization. However, unlike the short story, this book outlines what could be the first investigation in the United States of Mafia-like organizations long before the Prohibition Era. [Editor's Note: Readers who are Sherlock Holmes aficionados are urged also to read the article by MAJ (USA, Ret) John W. Davis, "Can Sherlock Save Counterintelligence?" in *AIJ*, Vol. 35, No. 2, 2018, pp. 153-156.]

This book begins like those movies, in which an event is shown in the present, and then a flashback to the past occurs before returning to the present. However, in this case, the present event is a murder committed in 1908 and the flashbacks go all the way back to the mid-1700s, and then to the late 1800s. The former flashback is to provide background into the foundation of the U.S. Postal Service and its Office of Inspector General (then the premier law enforcement agency in the United States—the FBI was not formally established until July 1908). The latter flashback is to give the reader an appreciation of the early life and political intrigue of the main character, U.S Postal Inspector J. Frank Oldfield.

Similarly, Inspector Oldfield did not work alone, much like Holmes was not without Watson. Instead, joining the inspector was an adept and enterprising Pinkerton undercover operative known as "The Raven," as well as a host of postal inspectors and administrative/translation support to investigate and take down a Sicilian criminal organization whose roots begin in New Orleans, Louisiana, and relocate to Ohio (due to their implication and following adverse consequences in the murder of a prominent law enforcement officer and police chief), before spreading its tentacles to the Great Lakes, New York, Pennsylvania, West Virginia, Chicago, Illinois, and Oregon. The organization was widely known as *La Mano Negra* or Black Hand Society, which was headed by a Sicilian collective calling itself The Society of the Bananas. Just as "The Godfather" movie character Vito Corleone began an olive oil business to conduct his nefarious activities, so the Society members were each involved in the commercial shipping, distribution, and selling of fruits and vegetables. In addition, most of their victims were small businesses in the same economic sector, which were seen as competition by the Society, and needed to be incorporated or merged with those of the Society.

By the time Oldfield is asked to investigate the Society, he has already earned a reputation for getting the job done, and for using unconventional and unsanctioned methods to do so, in busting train robbers, safe crackers, and embezzlers. These experiences are what he and his "Watson" use to take down the Society's intricate web of operatives and their unique manner of transmitting extortion and death threats via the U.S. Mail. In the end, through use of an ingenious manner of marking the envelopes being used only by Society members to transmit and convey their extortion attempts, Oldfield and his team successfully investigate and gain prosecution of eleven members of the Society in the first national organized crime conviction in the United States. At the time of their arrest, one of the eleven was living in the residence of the man murdered in the first chapter, who had received extortion and death threats from the Society and was romantically involved with one of his daughters. In another ironic twist, at the beginning of their investigation, Inspector Oldfield and other postal inspectors conduct an overnight surveillance of a meeting of the Society, where the organization draws up its sixteen articles later used to prosecute its members. This is reminiscent of the 1957 Apalachin Meeting of about 100 members of the *Mafioso* or Mafia members in southern New York, which confirmed the existence of a nationwide criminal conspiracy and organization, the presence of which was being denied. This was much the situation Oldfield and his team were running into as, until the conclusion of the investigation and subsequent trial, the existence of the Society was also being denied.

Nevertheless, the investigation and trial were not easy for Oldfield and his team. In addition to obtaining evidence "beyond a reasonable doubt" required for prosecution, they also had to overcome the threats of *Omertà* (which

literally means "manhood" and is a code of honor referring to dealing with one's own problems without the assistance of law enforcement, and observing a code of silence when questioned by authorities) made against potential extortion victims and witnesses, as well as threats to Inspector Oldfield, his team, and their respective families. These threats were not to be taken lightly, as the Society was known for backing them up with murders and bombings.

Without the survival of one of six leather trunks containing investigative notes, photographs, newspaper articles, and other supporting documents kept by the Oldfield family throughout the decades, this story more than likely would have been lost to the ages. In addition, fearing possible retaliation from descendants of the Society's *Mafioso*, who are prominent community members near where the descendants of the Oldfield family reside, was another consideration to take into account. However, this treasure of information passed down through history, regarding the first successful investigation and conviction of Sicilian Mafia members in the U.S., is a must-read for those interested in criminal history.

• •

THE WEST POINT HISTORY OF WORLD WAR II (VOL. II).

Clifford J. Rogers, Ty Seidule, and Steve R. Waddell.
New York, NY, Simon & Schuster. 2016.
370 pages.

Reviewed by Chief Petty Officer (USN) Jason T. Weber, analyst for the U.S. Navy and the Defense Intelligence Agency. He holds a degree in History from Thomas Edison University and earned his post-graduate degree in Historical Studies from the University of Oxford, UK. He is presently working on a second master's degree (MSSI) in the National Intelligence University's Monthly Executive Program. He has served as a Geopolitical Analyst for most of his military career across a broad spectrum of commands. Jason publishes the science fiction series *Major Chronicles* (CreateSpace 2016, 2017).

The editors of this continuous in-depth survey of World War II begin the book just as the Allies turn the tide in both the Atlantic and Pacific Theaters. A compilation of separate authors' points of view on the events, the book does an adequate job approaching both theaters of war simultaneously, taking the reader from one event to the next relatively seamlessly. The style of the text embodies the same treatment of this broad subject presented to those studying at the U.S. Military Academy at West Point, with enough archival material, graphics, and maps to please even the most skeptical fans of history. Each of the authors more than lives up to his academic credentials of being a preeminent military historian, without intimidating the reader as to his approaches being digestible. West Point's reputation for being a hallowed hall of military history is more than substantiated in this new tackling of what can be an unwieldy subject for even the most skilled author.

FORMAT AND APPROACH

The book's six thematically organized chapters chronologically proceed from the turning point for the Allies in 1942 through the end of the conflict, to include demobilization after total Allied victory, which provides excellent closure to the topic by including this often omitted period. The book's graphics and maps keep the reader on the path of the given section author's train of thought while not being so overbearing as to rob the work of its textual value. The oversized 8½ x 11-inch format lends itself to the two-column format, with the large central column bearing the dominant themes, and the second marginal column providing amplifying information, trivia, and details on relevant artwork or maps, the majority of which are in full, high-resolution color. Such a layout lends itself to an expansive topic by maximizing opportunity for text, without becoming textually unwieldy or distracting.

This reviewer is aware of only one book in English on topics related to West Point's work that have been published since 2016: Craig L. Symonds, *World War II at Sea: A Global History* (Oxford University Press, 2018). That so few additional books having the scope, skill, and breadth have been published highlights the tendency for authors to focus on one single element, theater, subject, or campaign. Only the aforementioned book approaches the tenacious attention to detail and is able to tackle the conflict spanning two theaters at the same time. All authors put forth logical and engaging narratives that walk the reader through the conflict, spanning both the Atlantic and Pacific land campaigns.

The generous inclusion of historical photos, maps, and portraits in *The West Point History of World War II* (Vol. II), combined with the colorful narratives, introduce the reader to both the scale and depth of that conflict in a comprehensive manner, with maps being one of the true gems of this work—overlaying strategic movements over terrain, supplemented with marginal call-outs and further points of note. The authors have created a coffee table-sized book that one could only have wished he/she had going through secondary school with material and content pleasing to both the ardent student of history and the amateur armchair general alike.

CONTENT

By 1942, the Empire of Japan had exhausted its momentum, and the ease with which it swallowed up territory in the Indo-Pacific region had begun to wane. Likewise, the Axis powers of Europe began to slow. Though the global conflict would continue on both fronts for over two years, the vast industrial complex that the United States brought to the Allied table, coupled with a more unified European command structure, began to have a positive effect. The Germans would continue to attempt to regain their edge and press back against Allied forces (pp. 9-10) but would not enjoy the same dominance they had capitalized upon from 1939 to 1941. The Germans' drive into Russia opens the narrative providing excellent maps outlining military strength and position for which West Point histories are so noted. Most historians and students of World War II are familiar with the Third Reich's push into Russia, and the devastating effect such tactics have had throughout history on any attempting such a maneuver. The authors, however, paint a picture easily digestible by even the newest student to the subject, placing additional shaded call-out boxes to provide amplifying context to a given event, such as the Soviet defense of Stalingrad (p. 25), while simultaneously providing a human lens through which the reader can peer, such as Russian General Chuikov having to hurl poorly equipped, barely trained solders at the very heavily armed and more experienced German Panzer Corps.

The authors make it a point to include various propaganda posters seen throughout the war on multiple fronts that give an added insight into efforts to influence populations (pp. 27, 50, 54, 74, 76, 152, 172, 253, etc.), and provide a useful bonus to those interested in the subject. Also included in the text as the authors walk chronologically forward are shaded call-outs of key military leaders that provide additional context. In the first chapter, the reader is introduced to British Field Marshal Bernard Montgomery (p. 31). Just as the Axis powers were finding frustration on the Russian front, so too were they finding problems in North Africa at El Alamein. From those conflicts, the narrative shifts to the Pacific to maintain chronological pace with the events in Europe, featuring more cartographical representations outlining military strategy, though those are more nautical in nature given the theater.

The book next moves to Chapter Two discussing the strategic implications of air and sea power (p. 45), with a shaded call-out giving biographical information on Admiral Dönitz (p. 52). This chapter does not include as many pages as some of the following chapters but still provides good context and summary to such areas as the U-boat war and the American industrial complex (p. 64), which ultimately overcame the Axis' submarine advantage. Starting in the middle of the chapter, the author begins to focus on the strategic air component of Europe (pp. 71-95) with details on desired effects, and the evolution in both the quantity of ordnance dropped and the delivery platforms painting a vivid account of the conflict's escalation. Following a succinct section, more pages are dedicated to Chapter Three, "Waging a Global War" (p. 98). Opening with the narrative that, by 1943, the Allies were squarely on the winning side, the author does an adequate job providing insights on different leaders' perspectives regarding the war and the direction they wished to take in the conflict, though more space could have been provided at the outset for their opinions without detracting from the flow of the narrative. Europe takes focus at the outset of the chapter, illustrating Germany's danger at being encircled by the Russian Army near the Sea of Azov (p. 103). The chapter then flows to the outlying European conflicts, such as the invasion of Italy, and next moves to events occurring in June-August 1943 (p. 139) in the Solomons, central to the Pacific campaign. The author's selection of sketches for inclusion made by those in the conflict on Tarawa provide a surreal scene filling an otherwise void of photographs (p. 145). The conclusion of the chapter achieves the aim of highlighting the global nature the conflict had now assumed and the various unique ways it was impacting each theater.

Midway through the book, the reader comes to the "Victory in Europe." The final two years of the war (1943-45) saw loss of life on a scale the world had never seen, with destruction on the continent being felt by those from all walks of life. Charts highlight the sacrifice and wholesale slaughter the Soviet Army faced (p. 154) with a myriad of military maps, some spanning two pages, to walk the reader through the conflict which, understandably, is challenging to follow though made much easier by their inclusion by the author. The chapter concludes discussing the war on the German-Russian Front and then transitions to the conflict in the West, which receives the majority of pages in the chapter. Starting with Operation OVERLORD (D-Day and the invasion of Normandy), the author discusses the various elements and tactics involved in the operation and the successive conflicts.

Though substantive pages are devoted to the section, it still gives a high-altitude look at the operation (pp. 169-198). In spite of the plethora of tactical maps, this section of the chapter feels rushed and compacted. More documents, testimonies, and biographies of those involved could have been included without sacrificing the pacing and catering to a period of events in which the majority of students and aficionados of World War II

history are most interested. Quantity of coverage aside, the quality of the narrative within the conclusion of the European theater is superb and in keeping with the preceding chapters, with a deluxe 2-page foldout chart in the succeeding chapter (p. 210a).

Chapter Five focuses on the defeat of Japan (p. 199) in keeping with the chronological style adopted by the authors. As the defeat of Japan within the Pacific relied heavily on maritime conflict and actions, it bears noting the author of this chapter is Robert W. Love, Jr., a preeminent historian with whose books on naval history (*History of the United States Navy*, Vols. 1 & 2, Stackpole Books, 1992) the reviewer is intimately familiar. The author highlights the differences in training the Japanese forces went through, as compared to those of the U.S. (p. 208), leading to an event referred to as "The Great Marianas Turkey Shoot." The chapter moves through various conflicts and does a succinct job of marrying the land aspects of the Pacific campaign to defeat Japan with the naval, drawing out implicitly, if not explicitly, the criticality of joint operations and the influence on sea lines of communication. In themes first seen earlier in the book involving strategic airpower, the author highlights both narratively and graphically (p. 239) the influence of bombing campaigns within the Pacific Theater and their contributions to ultimate victory over Japanese forces. Another deluxe foldout chart is present toward the end of the chapter, this one being three pages, and highlights Allied manpower in June 1944, nicely setting up the impacts and necessities of drawdown (as discussed in the next chapter).

Wrapping up the chapter, using only a few pages, is the atomic bombing of Japan. There is little discussion of the Manhattan Project, nor of the Army's organization and execution of the operation, to include the joint requirements to bring the Project and mission to a successful conclusion. That so little is devoted to this keystone event is the only shortcoming this reviewer encountered in the narrative.

The narrative concludes with Chapter Six, involving demobilization and victory assessment (p. 259). In addition to the major themes, the author weaves in ever so subtly the foundations for the coming Cold War between the Western Allies and Stalin (p. 265). The author highlights the political complications that came with denazification of Germany and briefly touches on the impact of the Holocaust and the extermination of peoples by the Nazi regime (p. 268). Moving next to Japan, the narrative details the myriad problems faced by the U.S. as it worked to govern a conquered nation. The chapter ends with an abbreviated summary of the war tribunals and lastly a "lessons learned" as a conclusion to the entire narrative—well thought-out, well-argued, and succinctly made leaving few if any elements not discussed or touched upon.

CONTRIBUTION AND CONTEXT

The authors and editors accomplish their objective of providing a *West Point History of World War II* with myriad high-quality graphics, several multi-page foldouts, and enough artwork and pictures to hold the interest of the reader. Additionally, they manage to transition from theater to theater in a manner that is not jarring or confusing. At no point is the reader lost in context or unsure of where he/she is in a given battle or front. The historians selected to author their assigned chapters do so admirably, and the editors have done a commendable job weaving them together into a succinct narrative.

The book also benefits from the shaded boxes calling out details, from the biographies of major individuals of importance, and lastly from the lavish battle maps outlining what took place and where. The photographs and artwork selected cannot be construed as superfluous and add a dimension of quality to the understanding of the conflict. The book itself mentions that it had been decades since such a narrative had been undertaken and published, and to anyone tackling the subject it is not difficult to see why. Each author judiciously selected the battles and conflicts most pertinent to his given section, though at times for a given element pages had to be sacrificed and, for some of those elements, quality and depth were sacrificed—occasionally in areas the reviewer felt were inappropriate. This by no means is an indication of faulty editing or research labor, but more of a historian's bias as to what warrants more coverage and what does not.

One walks away from the book with a holistic appreciation for the gravity of the conflict and the various challenges faced by both Axis and Allied powers waging war. The only aspect the narrative could do more with is page count and coverage, though to do so, if every battle and every element were covered in such depth, it would make the book unwieldy, as a quick perusal of books available pertaining to World War II quickly shows that a reader's library could be inundated with every manner of topic. The book maintains high academic standards within the strategic arena and also features exhaustive endnotes with supplemental references for the truly hungry aficionado. All these observations aside, this reviewer would heartily recommend the book to the budding tactician and the retired strategist alike, with everyone in between able to gain something, as it is unlikely such a skillful and succinct narrative of World War II is likely to emerge again anytime soon.

STONE THROWING AND THE U.S. CYBER COMMAND: INCREASED AUTHORITY TO CONDUCT OFFENSIVE OPERATIONS

Herbert Lin and Amy Zegart, eds.
Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations. Washington, DC, Brookings Institution, 2018.
424 pages.

Reviewed by Dr. (LTC, USAR) Christopher E. Bailey, an Associate Professor in the Intelligence Enterprise Department, College of Strategic Intelligence at the National Intelligence University, specializing in national security law, international law, and professional ethics. He is also an adjunct instructor in the Master of Science in Cyber Security Program at the University of Charleston (West Virginia). He serves as a staff editor for the *Journal of Law & Cyber Warfare*. Dr. Bailey is licensed to practice law in California and the District of Columbia, and is a member of the American Society of International Law. He has an LLM degree in National Security and U.S. Foreign Relations Law, as well as an SJD degree in International and Comparative Law from the George Washington University School of Law. He has published extensively on national security and international law issues, to include a forthcoming article on "Offensive Cyberspace Operations: A Gray Area in Congressional Oversight," in 38 Boston University Int'l Law Journal (2020).

[Editor's Note: Dr. Bailey graduated from NIU's Monthly Reserve Program in 2007 with a Master of Science of Strategic Intelligence degree. He enthusiastically joined me as a co-editor of *AIJ*, Vol. 33, No. 1, 2016, the theme of which was "Intelligence Ethics and Leadership," and has been a frequent contributor to the *Journal* over the last decade. In 2018, I nominated Chris to be a director on the NMIF board, and he now assists me on the Publications Committee, proving most helpful with pre-publication review issues.]

Offensive cyber operations, whether acknowledged or unacknowledged, are becoming an increasingly important—and worrisome—issue for the international community. Indeed, the under-regulated cyber domain creates opportunities, as well as risks, for state and non-state cyber actors alike. On one hand, the prospects for a meaningful international treaty that can regulate the domain in positive manner are likely to remain a distant dream given the range of conflicting state interests. On the other hand, this also suggests that cyber-capable states should be reticent to engage in unilateral operations that risk undermining international peace and stability. Indeed, one writer aptly describes the "Glass House" dilemma for cyber-dependent countries. He argues, "Paradoxically, the more a society relies on its cyber capabilities, the more it becomes vulnerable to malicious cyber operations. On the offensive side, cyber powers may thus prefer permissive rules [of international law] that would leave some leeway for stone-throwing. But on defense, those same states desperately need restrictive rules to protect the elaborate glass houses they are sitting in."[1] Thus, one is left with questions about whether and how the United States should use its cyber stones, as well as whether and how it should support the progressive development of international law *lex ferenda*.

In general terms, this raises important issues about how policymakers conceptualize offensive cyber operations as an instrument of national security policy. Policymakers must consider whether and how cyber operations should serve as an instrument of coercion in situations short of the "use of force" threshold under the Charter of the United Nations,[2] perhaps violating the international law principle of nonintervention in other countries with an internationally wrongful act or perhaps serving as an escalatory act during an existing crisis. What strategic considerations should guide the development and employment of offensive cyber operations? What intelligence capabilities are required to support effective cyber forces? Is there a role for the private sector in cyber conflict? This leaves important questions for the United States: Where is the country headed with the new statutory authorities that have been extended to the Department of Defense (DoD) and the U.S. Cyber Command (CYBERCOM), which removed the prior legal constraints on offensive cyber operations?[3] Will an increase in offensive cyber operations undermine international peace and security, or will an increase have a deterrent effect on cyber space adversaries?

Herbert Lin and Amy Zegart are both well-known international security experts in the Center for International Security and Cooperation at the Hoover Institution on War, Revolution, and Peace located at Stanford University. Initially, in March 2016, Lin and Zegart convened a two-day workshop that brought together distinguished academics and experienced national security practitioners from DoD and the Intelligence Community (IC) for an unclassified and in-depth consideration of the strategic issues raised by offensive cyber operations. The conferees debated papers and presentations on cyber operations. The group addressed conceptual issues, to include current U.S. cyber doctrine, operational assumptions, intelligence requirements, the roles and missions of CYBERCOM, escalation dynamics, and the role of the private sector.

Now, as co-editors of this well-researched and well-argued volume dedicated to the men and women of CYBERCOM, Lin and Zegart offer a range of 16 essays

that examine some of the strategic issues involving military intelligence, surveillance, and reconnaissance in the cyber domain; the development of U.S. cyber doctrine and practice, both offensive and defensive; issues in deterrence and escalation control; and various important cyber scenarios, such as hacking a nation's missile development program, cyber terrorism, a China-U.S. military confrontation, and the role of the private sector. While I found this book to be very informative in understanding some of the strategic issues in the cyber domain, I am unsettled by what is suggested by the book, as well as recent changes in statutory law, about emerging U.S. practice with respect to offensive cyber operations. In other words, we will act to assert our national interests because we can, but while also lowering some of the important barriers on uses of force in domestic law and sacrificing some level of democratic accountability. This normative turn—namely, assertive state practice absent a sense of obligation (*opinio juris*)—can only undermine international peace and security, as well as the progressive application of international law to new and emerging areas of international conflict.

Offensive cyber operations will—undoubtedly—remain an important means and method in international relations over the coming decades. Cyber warfare offers an attacker important advantages, to include remote operations, with the victim having problems characterizing the event as either a violation of domestic or international law and untangling the complex intelligence involving source attribution. Most important, if the victim cannot properly characterize the event or identify the perpetrators, then the attacker can achieve discrete strategic objectives without risking a retaliatory response. Both clandestine and covert cyber actions can, therefore, perform a useful role in furthering U.S. national security interests, provided that such actions comply with relevant domestic law to include appropriate executive and congressional oversight, are conducted consistent with fundamental principles of international law, and fall below a certain level of severity based upon either the nature of the target or the degree of harm caused.

Offensive cyber operations can range from the relatively benign exploitation of a zero day vulnerability that enables a Distributed Denial of Service (DDoS) attack (e.g., a shutdown of certain systems or services for a demonstrative effect), to a more active—perhaps even a false flag—operation that involves the use of disinformation/propaganda to hide its origin or even discredit a third country,[4] and to a clear use of force operation that involves destructive acts against a targeted country's nuclear power, SCADA,[5] critical infrastructure,[6] or air defense systems. The gravity of the situation has also been highlighted by the White House and senior Russian leaders; both countries see the need for stronger cyber defenses to protect against cyber-attack from foreign state and non-state actors.[7] Indeed, the likely Russian interference in the 2016 U.S. presidential elections indicates that the international community faces a pernicious security threat with the use of social media platforms for the employment of state-supported, albeit eminently deniable, mercenaries.

Accordingly, the 2018 comprehensive strategy rolled out by the Trump administration indicates that the United States will undertake offensive cyber operations against foreign adversaries.[8] Initially, President Donald Trump signed the 2019 National Defense Authorization Act (NDAA) into law on August 13, 2018; this act further militarizes cyberspace by authorizing DoD to conduct a range of clandestine military cyber operations—short of hostilities or in areas in which hostilities are not occurring—as a "traditional military activity" pursuant to the covert action statute.[9] President Trump then rescinded PPD-20, the interagency legal and policy process that had been initiated by President Barack Obama, for "green-lighting" cyber-attacks.[10] Indeed, the House of Representatives conference report noted that DoD had faced interagency problems in obtaining mission approval for cyber operations. The report found that DoD had been challenged by "the perceived ambiguity as to whether clandestine military activities and operations, even those short of cyber-attacks, qualify as traditional military activities as distinct from covert actions requiring a Presidential Finding."[11] Thus, Congress has authorized an increased range of offensive cyber operations, no doubt "unleashing" CYBERCOM from its defensive shackles to conduct a broader range of defensive and offensive operations.[12]

Nonetheless, this broad affirmation of authority from Congress in the Secretary of Defense leaves many questions unanswered about the reach of its new operational authority, as well as involving presidential and congressional oversight. First, one must distinguish among clandestine collection, cyber exploitation, sensitive military cyber operations (SMCO),[13] and covert operations. This problem, not clarified by either the 2019 or the 2020 NDAA, cannot be overstated; many cyber activities elude characterization under the definitions typically applied to physical activities. Second, the new statutory authorities raise questions about the nature of presidential and congressional oversight. The new statutory authorization allows for a range of offensive cyber operations that could be properly characterized as a covert action based upon the nature and extent of damage to foreign computers, information or communications systems, or computer networks, but without the executive

oversight required by the need for a presidential finding and Memorandum of Notification to the congressional intelligence committees.[14] In other words, DoD and CYBERCOM can now conduct a broader range of offensive cyber operations, some of which can be construed by an adversary as hostile or wrongful acts in violation of international law, but the Secretary of Defense is no longer constrained by the need for a presidential finding,[15] either prior or contemporaneous reporting to Congress,[16] or even reporting to the senior congressional leadership.

The traditional controls on use of force, whether involving covert actions or armed conflict, exist to ensure executive/congressional oversight and democratic accountability in the conduct of U.S. foreign policy. There is, however, a distinct difference between purely defensive actions, either responding against an ongoing attack on friendly systems or preparing capabilities for prospective conflict, and offensive operations that could initiate or escalate a crisis. Arguably, there is considerable merit to the concern that DoD has experienced difficulties in obtaining mission approval within the executive branch for peacetime cyber operations involving something more than intelligence collection or responding to an ongoing attack. Nevertheless, strong presidential control and prior congressional notification also perform an important function: they ensure that this country uses unacknowledged force only in pursuit of "identifiable foreign policy objectives of the United States and is important to the national security of the United States."[17] Indeed, the need to inhibit unintended escalation with a foreign adversary mandates high-quality intelligence to minimize the risk of misattribution and collateral damage, as well as provide tight political control. Now, however, DoD can conduct a range of offensive cyber operations (i.e., "defend forward" through "persistent engagement"[18]) independent of any explicit finding to that effect. In short, the DoD has the authority to conduct a broad range of activities that it may consider "short of hostilities,"[19] but ones that an adversary may consider as a hostile or internationally wrongful act.

It is important, therefore, to consider how offensive cyber operations are regulated under domestic and international law—with special emphasis on how cyber actions present special challenges for policymakers and practitioners alike. Arguably, the 2019 NDAA has clarified the relatively innocuous notion that military intelligence collection activities—whether styled as clandestine, preparation of the environment, or information operations—are exempted from the covert action statute as a traditional military activity (TMA).[20] The 2020 NDAA has, however, amended the definition of a SMCO with language that allows for a broader range of "defensive operations" by eliminating from its ambit operations that the military considers to be low risk. Still, both the 2019 NDAA and the 2020 NDAA leave unanswered questions involving cyber collection activities, SMCO, and cyber covert actions. In effect, CYBERCOM is now preauthorized to executive cyberspace operations that could be perceived as internationally wrongful acts with an attendant risk to U.S. foreign policy objectives and national security interests, without prior interagency coordination or presidential approval, provided that such acts are "short of hostilities"—at least in DoD's opinion. This lack of clarity is problematic with the ambiguity that is inherent in characterizing cyber activities. In other words, offensive cyber operations, not intended by the United States as a hostile act, could be readily viewed as such by a foreign adversary and could, therefore, lead to unintended and unwanted consequences.

Lin and Herbert have authored an important work for policymakers, national security practitioners, scholars, and the informed public. As a domain through which the nation can exercise its national power, offensive cyber operations offer a range of strategic opportunities and risks—yet many important strategic issues have been understudied, or perhaps underappreciated. This volume helps readers understand some of the strategic issues involved in cyber operations, offering ideas about how existing strategic theory, doctrine, and practice, some of which originated in the Nuclear Age, can be adapted for this new field of interstate conflict. I recommend this book as a means to help understand some of the strategic issues that we face with the diversity of state and non-state actors which threaten our national interests. However, I remain concerned about the loosened executive and congressional oversight over offensive cyber operations and what that suggests regarding the possible range of future U.S. cyber operations.

NOTES

[1] Kubo Macak, *On the Shelf, But Close at Hand: The Contribution of Non-State Initiatives to International Cyber Law*, 113 Am. Journal of Int'l Law 81, at 83 (2019).

[2] United Nations Charter, art. 2(4).

[3] The Department of Defense defines offensive cyberspace operations as "[m]issions intended to project power in and through cyberspace," Joint Publication (JP) 3-12, *Cyberspace Operations*, June 8, 2018, at GL-5, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf (accessed August 7, 2019).

[4] Tim Maurer, Cyber Mercenaries: The State, Hackers, and Power 23-24 (2018). I recommend this book by Tim Maurer, the Co-Director of the Cyber Policy Initiative at the Carnegie Endowment for International Peace. Maurer provides an excellent analysis of how states can use non-state hacker groups—21st century mercenaries—to conduct covert cyber operations while maintaining plausible deniability. Maurer reaches several important findings: that the projection of coercive power through cyberspace is not limited to state actors; that states have been using cyber proxies for a broad range of purposes, to include data collection, the targeting of dissidents, and support to law enforcement agencies and military forces; that categorizing proxies based upon

intent is not helpful; that states have had three types of relationships with proxy groups, including delegation, orchestration, and sanctioning; and that all states face a similar problem with proxy groups in terms of the costs of the relationship and the increased risk of conflict escalation. *Id*. at 151-153. He argues that the traditional methods of arms control have limited utility for intangible code, leaving the international community with difficult problems in how to control such groups.

[5] The term "SCADA" refers to the supervisory control and data acquisition systems used in modern industrial control systems that are controlled by computers and automate many, if not all, management processes. An attack against such a system could have a major crippling impact on public utilities over large areas, with severe second- and third-order effects resulting from an interruption of services. Michael N. Schmitt, ed., TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 567 (2d ed., 2017).

[6] The term "critical infrastructure" is defined in U.S. law as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Critical Infrastructures Protection Act of 2001, 42 U.S.C. § 5195c (e) (2001). *See also* Exec. Order No. 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," 82 *Fed. Reg*. 22,391 (May 16, 2017).

[7] U.S. President, *Cyberspace Policy Review* (2018), https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (accessed July 23, 2019); U.S. President, *International Strategy of Cyberspace* (2011); Sergei Ptichkin, *Russia Building a Unified System to Defend Against Cyber Attacks*, RUSSIA BEYOND THE HEADLINES, November 26, 2014, http://rbth.com/science_and_tech/2014/11/26/russia_building_a_unified_system_to_defend_against_cyber_att_41719.html. The 2017 U.S. *National Security Strategy* recognizes the importance of cybersecurity and the need to defend ourselves "within the framework of international law." *Id*. at 41.

[8] U.S. President, *National Cyber Strategy of the United States of America* (Sept. 2018), at 20-21. *See also* Dan Lohrmann, *New National Cyber Strategy Message: Deterrence through U.S. Strength*, GOVERNMENT TECHNOLOGY, September 29, 2018, https://www.govtech.com/blogs/lohrmann-on-cybersecurity/new-national-cyber-strategy-message-deterrence-through-us-strength.html (accessed July 23, 2019). This is also supported by DoD's 2018 *Cyber Strategy*, publicly-available currently only in an official summary document. This strategy focuses on five—primarily defensive—cyberspace objectives with five supporting lines of effort. This document states that DoD "will conduct cyberspace operations to collect intelligence and prepare military cyber capabilities to be used in the event of crisis or conflict. We will *defend forward* to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict." *Id*. at 1 (emphasis added).

[9] 10 U.S.C § 394(c).

[10] Sean Lyngaas, *PPD-20 Elimination Opens Arguments over How U.S. Should Conduct Cyber Hacking Operations*, CYBERSCOOP, August 16, 2018, https://www.cyberscoop.com/ppd-20-eliminated-cyber-war-donald-trump-mike-rounds/ (accessed July 31, 2019). PPD-20 has apparently been replaced by a new process outlined in a recently prepared, but not publicly-available, national security presidential memorandum. Dustin Volz, *White House Confirms It Has Relaxed Rules on U.S. Use of Cyberweapons*, THE WALL STREET JOURNAL, September 20, 2018, https://www.wsj.com/articles/white-house-confirms-it-has-relaxed-rules-on-u-s-use-of-cyber-weapons-1537476729 (accessed July 31, 2019).

[11] H.R. Report 115-874, at 1049 (2018).

[12] According to the U.S. Cyber Command, "Adversaries operate continuously below the threshold of armed conflict to weaken our institutions and gain strategic advantages." U.S. Cyber Command, "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," at 3 (April 2018), https://www.cybercom.mil/About/Mission-and-Vision/ (accessed July 25, 2018). The Command Vision seeks persistent, global engagement against adversaries: "We sustain strategic advantage by increasing resiliency, defending forward, and continuously engaging our adversaries." *Id*. at 6. In other words, DoD is pursuing cyber adversaries on a proactive global basis as a military activity.

[13] A SMCO has been defined in 10 U.S. Code § 395 (b); this language has been amended in the 2020 NDAA, signed into law by President Trump on December 20, 2019. This amended definition narrows the statutory notification requirements for a SMCO by adding certain risk and risk-threshold requirements, 2020 NDAA, §1632.

[14] 50 U.S.C. § 3093 (a).

[15] 50 U.S.C. § 3093 (a) (1).

[16] 50 U.S.C. § 3093 (a) (2) provides: "Except as permitted by paragraph (1), a finding may not authorize or sanction a covert action, or any aspect of any such action, which already has occurred."

[17] 50 U.S.C. § 3093 (a).

[18] DoD, 2018 *Cyber Strategy*, *supra* note 8, at 1. *See also* U.S. Cyber Command, Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," *supra* note 12, at 6.

[19] 10 U.S.C. § 394 (b).

[20] 10 U.S.C. § 394 (c).

National Military Intelligence Foundation
PO Box 683
Charlotte Court House, Virginia 23923