AMERICAN INTELLIGENCE JOURNAL

★ ★ ★ ★ ★ ★ ★

FOR INTELLIGENCE PROFESSIONALS

Intelligence Education, Training, and Professional Development

NMIF Publication
Vol. 42, No. 1, 2025

Vol. 42, No. 1, 2025

AMERICAN INTELLIGENCE JOURNAL

FOR INTELLIGENCE PROFESSIONALS SSN 0803-072X

NMIF Board of Directors

LTG (USA, Ret) Mary A. Legere, Chair
Maj Gen (USAF, Ret) Linda Urrutia-Varhall,Vice Chair
LTC (USA, Ret) Steve Iwicki, President
LTC (USA, Ret) Ken Diller, Vice President
CW3 (USA, Ret) Todd Robinson, Treasurer

Ms. Natalie Anderson-Wells, Director
CDR (USCG, Ret) Michael Bennett, Director
LtCol (USAF, Ret) James Eden, Director
Col (USAF, Ret) Michael Grebb, Director
CAPT (USN, Ret) Steven Horrell, Director

COL (USA, Ret) Jim Edwards, Director
CAPT (USNR) Rick Myllenbeck, Director
COL (USA, Ret) William C. Spracher, EdD, Director
LTC (USA, Ret) Christopher E. Bailey, SJD, Director
Major (USAF, Ret) David J. Kritz, DBA, Director

Editor - LTC (USA, Ret) Christopher E. Bailey, SJD
Assistant Editor - Maj (USAF, Ret) David Kritz, DBA
Editor Emeritus - COL (USA, Ret) William C. Spracher, EdD
Production Manager - Debra Hamby-Davis

Col (USAF, Ret) William R. Arnold, Director Emeritus
Brig Gen (USAF, Ret) Scott Bethel, Director Emeritus
CDR (USN, Ret) Calland Carnes, Director Emeritus
Col (USAF, Ret) John R. Clark, Director Emeritus
MajGen (USMC, Ret) Michael Ennis, Director Emeritus

COL (USA, Ret) Michael Ferguson, Director Emeritus
Dr. Forrest R. Frank, Director Emeritus
Col (USAF, Ret) Owen Greenblatt, Director Emeritus
Col (USAF, Ret) William Huntington, Director Emeritus
COL (USA, Ret) Gerald York, Director Emeritus

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

Authors interested in submitting an article to the ***Journal*** are encouraged to send an inquiry - with a short summary of the text-to the Editor by e-mail at <christopherbailey286@yahoo.com>. Articles and inquiries may also be submitted in hard copy to Editor, c/o NMIF, PO Box 494, Earlysville, Virginia 22936. Comments, suggestions, and observations on the editorial content of the ***Journal*** are welcomed. Questions concerning publications, 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, Member of Congress and their staffs, and university professors and libraries, as well as to NMIF associates, Journal recipients, and contributors. Contributors include Intelligence Community leaders and professionals as well as academicians, research fellows, students, and others with interesting and informative perspectives.

Copyright NMIF. Reprinting and copying by permission only. ISSN 3067-9672 (Online) ISSN 0883-072X (Print).

AMERICAN INTELLIGENCE JOURNAL

Table of Contents

"Intelligence Education, Training, and Professional Development"

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 in which the authors are employed.

PRESIDENT'S MESSAGE

This issue focuses on intelligence training and development during a turbulent time across the intelligence community (IC). Despite all the political shifts, the IC remains strong and dedicated to getting the right information to our leaders to protect our national security.

There has been a major shift in one critical part of our IC partners, and that is in law enforcement. Traditionally, law enforcement intelligence analysts were siloed to focus on forensic case building to enable trial convictions. That has dramatically shifted this year for a number of reasons.

First, the southern border is secured like never before, which has allowed our law enforcement agencies to focus on more than just the border or local criminal gangs. I recently attended two major border intelligence and security conferences and was amazed to hear the intel leaders of these agencies talking about predictive intelligence, patterns of life, and digital ISR. They all acknowledge that their intel analysts need significant training in analytical tradecraft and how to leverage all the information available in the IC.

Second, the majority of the law enforcement targets are inside the borders of the United States, where there is no traditional IC collection and support, so more capabilities are desperately needed. For example, the notorious MS13 gang was originally formed in California in 1980, thus representing 45 years of primarily U.S. citizen membership. This creates tremendous challenges for intelligence operations that regularly come across U.S. persons information.

Third, law enforcement intelligence capabilities are integrating data and information with the goal of creating a common operational picture (COP) and a common intelligence picture (CIP) that is shareable across the law enforcement enterprise. The Department of Defense (DoD) and the IC can greatly assist in replicating their capabilities into the law enforcement community at different classification levels, all the way down to unclassified/law enforcement sensitive.

Lastly, our senior leaders serving across the Department of Homeland Security (DHS) and law enforcement agencies have a detailed long-term intelligence objective. They understand the intelligence fight needs to be expanded in depth and detail well beyond both sides of our borders and throughout our nation's interior. They have the same need as the DoD: how do we get the right information to the front-line agents, so it is actionable but generally unclassified? This challenge is similar to the IC when we write for release, protecting sources and methods.

The IC can and should contribute to not only mission success, but also in training and educating our law enforcement intelligence analysts on data analysis, fusion, and information sharing.

LOOKING AHEAD TO THE 2025 NIGHT OF HEROES

This year's annual Night of Heroes Gala will be on Thursday, November 20, at the Crystal City Gateway Marriott in Arlington, Virginia. We will begin the evening with our happy hour reception starting at 1800 hours. Please consider attending as we honor 18 outstanding awardees from across the military services, the Defense Intelligence Agency, the National Geospatial-Intelligence Agency, the National Reconnaissance Office, and DHS. We will also be awarding scholarships to some amazing undergraduate and graduate students studying for careers supporting our nation's national security.

LTC(R) Stephen Iwicki, USA
President NMIF

EDITOR'S DESK

Welcome to the spring edition of the American Intelligence Journal. I'm pleased to introduce this edition on "Intelligence Education, Training, and Professional Development," a subject worthy of consideration with recent changes in the intelligence community (IC) brought about by the new Trump administration over the past several months. We certainly have much to think about with the streamlining of government and the need to meet emerging national security requirements. This edition offers several interesting perspectives on issues involving the professional development of new and experienced intelligence practitioners. Now, I'd like to highlight some of the fine contributions from intelligence practitioners, scholars, and students.

We have many interesting and provocative articles. First, we have an introduction by Dr. Stephen Marrin, an accomplished educator and professor at James Madison University. We greatly appreciate his perspectives. Dr. Marrin's introduction is followed by several thematic articles that examine important broad issues in intelligence studies: Dr. David Kritz, a professor at American Military University, examines grounded theory and its implications for intelligence practitioners and academics; Dr. Valerie Davis, also at American Military University, considers the need for adapting intelligence education to emerging threats; and two Greek scholars argue for a redefinition of intelligence studies. Each article offers ideas about past efforts and what can be done to improve the work of the ODNI/U.S. intelligence community.

Second, we have five articles that illustrate varied research and teaching methodologies. Dr. John Bustria, formerly a fellow at the National Intelligence University (NIU), has authored a useful article that illustrates the use of Alternative Futures Analysis (scenario development). Next, we have three NIU graduates—with differing work backgrounds—who have provided short pieces illustrating a "best practices" teaching methodology used in the NIU core course MCR 608 (Leadership and Management in the Intelligence Community). In the 608 course, students are typically tasked to prepare an 8-10 page paper to evaluate a private sector or government best practice that addresses a practice involving leadership, management, transformation, or organizational cultural problem that might have utility for the IC. A fourth NIU graduate, Eitan Jay Sayag, examines a case study using the external environment analysis model, known as PEST (political, economic, social, and technological). It's worth noting that this analysis originates in Eitan's thesis and has been refined through a peer-review process that included scholars/practitioners in a "Bear Pit" session organized by the International Association for Intelligence Education (IAFIE).

Next, we have a series of articles on emerging issues for intelligence practitioners. We have four articles authored by students in the NIU-led Intelligence Studies Consortium (ISC). In 2019, the NIU started the ISC to bring together faculty and students in the undergraduate and graduate-level intelligence programs in the Greater Washington, DC area. The ISC has focused on promoting intelligence as an academic discipline and has helped intelligence students present and publish original research. The ISC has sponsored five annual student-oriented conferences; in November 2023, the ISC held a virtual symposium for students and faculty with the editors of intelligence journals on how to get published in the field. The original handful of schools has now expanded to nearly a dozen, including an expansion to include schools from the IC Centers of Academic Excellence. I'm pleased that we can showcase some of that work here. Finally, we have two articles on human intelligence (HUMINT); one article, by two Brazilian authors, highlights the ancient origins of modern espionage practices, and the second article is about Cold War collection in Europe.

We have two opinion pieces. The first is by Dr. Bill Spracher, a past editor of and frequent contributor to this journal. Dr. Spracher helps clarify the distinction between intelligence education and intelligence studies, especially because these two terms seem to be used almost interchangeably in much of the literature. The second is by James Carlini, a frequent contributor to the journal. Mr. Carlini argues that the United States needs a modernized educational framework for military personnel to address the evolving demands of 21st-century warfare, particularly in the cognitive and electronic domains. It emphasizes the necessity for a diverse and advanced skill set beyond traditional training

methods. It also examines the emerging importance of Cognitive Competitiveness (CC) and Cognitive Warfare (CW) and addresses why we need an urgent shift in military training priorities.

We have nine great book reviews on a range of thematic, historical, and emerging topical issues. We have one important comparative review, authored by a well-qualified doctoral candidate, involving two leading books involving Open Source Intelligence (OSINT). We have several books that examine emerging issues in intelligence practice, such as unmanned systems, artificial intelligence, and microchips, as well as some interesting topics in military intelligence history. I remain an unabashed fan of spy fiction, not just for its entertainment value, but also as an andrological tool to promote a well-balanced moral/ethical education for NIU students. I encourage interested AIJ readers to contribute their own reviews on recently published intelligence topics, whether non-fiction or fiction.

As a reminder, for the fall 2025 edition, we'll focus on "Professional Stewardship." We have had some authors express interest in an article written through the use of AI/ChatGPT. While I would agree that such tools have value in brainstorming or writing a first draft, I would remind everyone that authors are responsible for all content and for ensuring the quality/validity of all sourcing. You can also check online for the proper means of citing work prepared by Chat/GPT (https://apastyle.apa.org/blog/how-to-cite-chatgpt). We're committed to a high-quality publication. As always, we welcome articles, opinion pieces, and book reviews both on and off theme.

Dr. Christopher E. Bailey
Editor

NMIF Corporate Partners

Thank-you to NMIF's
2024 Night of Heroes
Corporate Sponsors

SOSi
CHALLENGE ACCEPTED

BEYOND IDENTITY

Google

SMX

FENIXPYRE

Intelligence Education:
Bridging the Gap between Intelligence Studies and Intelligence Practice

by **Dr Stephen Marrin**

This special issue of the American Intelligence Journal, addressing "Intelligence Education, Training, and Professional Development," is on the important topic of how intelligence professionals should acquire the knowledge and skills they need to succeed. Ensuring that intelligence professionals are prepared for the challenges they will face is crucial for the effective functioning of the intelligence community (and enterprise) well into the future.

A key question—and a theme running through the special issue—is "how should the relationship between academia and government best be managed to accomplish these goals?" As a pracademic … a former practitioner turned academic … I've been studying intelligence now for over 30 years. After spending five years as an analyst at the Central Intelligence Agency (CIA) and the Congressional Government Accountability Office, I spent more than 20 years researching and writing about intelligence analysis and teaching in a variety of academic programs. These writings contribute to the intelligence studies literature, which is the body of knowledge about intelligence as a function of government.[1] The question, how to best integrate intelligence studies knowledge into intelligence practice, is an ongoing challenge that can best be accomplished using an educational framework.

There is a noted gap between theory and practice in many fields—including foreign policy, as political scientist Alexander George has argued—reflecting major differences in purposes between academia and government.[2] Academic institutions focus on building the body of knowledge—to include theory—because that is their purpose … to help society know and understand. Meanwhile, the government is an action arm of society, for implementing activities that are in the national interest … for "we the people."[3] An effective partnership between academia and government would ensure that the knowledge developed by academia is then used to best effect by government in the best interest of society.

Bridging the gap between academia and government in the space of intelligence studies and intelligence practice requires implementing ways to ensure the transmission of knowledge between these institutions with equally important but very different purposes. As I've suggested elsewhere, this includes encouraging experts—who bring a lot of knowledge with them—to transition between government and academia (people who Joseph Nye calls "in-and-outers"), shifting the emphasis on practical relevance from traditional academic departments to public policy schools or interdisciplinary undergraduate programs that offer degrees relevant to intelligence practice, and develop or support academic research-oriented intelligence studies centers.[4] Doing more of this would increase the flow of intelligence studies knowledge into intelligence practice.

An example of how this works can be found in the way in which the IC reached out to intelligence studies scholars when developing the first national intelligence strategy. The subsequent conversations became known as the "intelligence theory" contributions to the intelligence studies literature.[5] For example, in those conversations, Jennifer Sims pointed out that the goal of intelligence is to help achieve decision advantage.[6] This framing was subsequently adopted by the Director of National Intelligence (DNI) and ODNI as the stated mission of the IC.[7] But others in the intelligence theory literature have also suggested alternative frameworks … that the goal of intelligence is to optimize the application of power or the use of resources.[8] Or, as some have suggested, the purpose of intelligence is to reduce the uncertainty or the ignorance of decision makers.[9] Or as some have said, its purpose could—conversely—be to challenge decision makers or even *increase* their uncertainty, presumably to provide the best opportunity to ensure that the best decisions are made … optimizing the application of power, the use of resources, and the achievement of decision advantage.[10]

To achieve these goals, intelligence organizations implement many different kinds of activities. And the professionals who implement those activities within those organizations require a combination of knowledge and skill so that they can do their jobs to the best of their abilities. What kind of knowledge or skill they

require depends on what kinds of activities they are implementing, so there is no universal best answer to the question "what does an intelligence professional need to be able to know or do?" Instead, there are many different kinds of answers to that question, with the best one being "it depends."

Yet, of all the ways that knowledge or skill can be acquired, education is the most important way to ensure that intelligence professionals are prepared for the challenges of the future. As has been highlighted by the faculty members at National Intelligence University, education is intrinsically challenging, designed to ensure improvement in the learning orientation of the students.[11] Education provides the opportunity to revise and update not only the knowledge and/or skills of the student, but more fundamentally, the strategies that the student uses for knowing and understanding. Education harnesses the students' passions and strengths, helping to ensure they do the work necessary to develop their capacities. The best education is that which is productively disruptive conceptually, ensuring that the student remains constantly curious, challenging, questioning, and reflective.

Education provides the current or prospective practitioner with knowledge and skill, geared to provide a foundation for a critical, questioning, evaluative orientation to lifelong learning. Education is to enable the recipient to develop their approaches to emerging issues and challenges. Its value is in the long term, with a potentially long shelf life.

Training, on the other hand, supplements education as it is oriented to skills development and proficiency, with value more in the short term than the long term.[12] Training is important as well, but the intelligence profession is changing so rapidly, and technology is affecting it to such a degree that it is not clear what the needs of the future practitioner will be. Artificial Intelligence (AI) looks to be both an enabler of intelligence products and a disruptor of intelligence processes at the same time. But can the outputs of AI be trusted? How and in what ways will AI facilitate—and then complicate—information acquisition, aggregation, and knowledge development? Due to technological advances in AI, we don't know what knowledge or skills will be required of the future intelligence practitioner … as Yogi Berra said, "It's tough to make predictions, especially about the future."

Yet, we know that the analytic skills of the future will require technological proficiency of some sort. As intelligence professionals look ahead to the requirements of the future, some suggest that the expert analyst will continue to provide knowledge and context, using technology to support knowledge production, emphasizing continuity.[13] Others flip the script, emphasizing change, and suggest that the role of the generalist analyst in the future will be—essentially—to engage with technology, facilitate the AI process, and curate the results.[14] To address this need for technology, some academic programs are preparing their graduates to be multidisciplinary analysts of the future by embracing the integration of technology into analytic processes.[15]

Also, in terms of the transition from student to intelligence professional, intelligence organizations should more effectively manage the integration of new personnel into the ranks and get them up to speed through a professional development process that identifies what kind of knowledge or skill is needed at various stages of one's career. There have been sociological studies focusing on the culture and mindset of working intelligence professionals and what is needed for an effective transition into the intelligence community, including pre-employment socialization.[16] But much more work could be done of an ethnographic variety to understand the unique acculturation process required to work in the intelligence sector.

Finally, in looking to the future, there is both a challenge and an opportunity. The challenge is in how to reconcile ourselves to the uncertainty, not knowing which of the old ways will continue to work for a new future. The opportunity is in how we orient ourselves to the potential of that future, to find better ways to achieve the immutable goals of intelligence.

One opportunity could be in government sponsorship of intelligence research—either the funding of it generally, or providing venues for its sharing and dissemination—to help facilitate knowledge production and bridge the gap between academia (theory or scholarship) and practice. This would also help build up and out the policy-relevant aspects of the intelligence studies literature, and help develop it as a multidisciplinary field serving as a professional body of knowledge for working intelligence professionals.[17] National Intelligence University's recent March 2025 hosting of an Intelligence Studies Summit to solicit and then present research about intelligence as a function of government is a good step in this direction. More could be done.

Another opportunity could be in developing and then institutionalizing collaborative infrastructures for the sharing of knowledge and perspectives to bridge the gap

between academia and government. Many intelligence studies scholars and intelligence professionals—such as those writing the articles in this issue—are reflecting on what "best practices" look like both today and into the future. Due to differences in their respective missions, academics tend to be more conceptual and theoretical, with intelligence professionals more practical and applied. These differences—while sometimes framed as competition or conflict—can more effectively be framed as complementary and optimally collaborative.[18] Collaboration can be a way to optimize the integration of theory and practice and—hopefully—produce an output that has relevance and utility in improving the knowledge and skill of future intelligence professionals.

As intelligence continues to professionalize, the formalization and institutionalization of organizations and associations to develop and share best practices will also help ensure that working intelligence professionals of the future have the knowledge and skills they need to succeed at their respective missions. Professional organizations and associations are critical to this effort because they provide institutionalized platforms (e.g., annual conferences and events) for the conversations that lead to professional improvements over time.[19] Some of this infrastructure is in place, such as the Intelligence Studies Section at the International Studies Association, which has existed since the mid-1980s to encourage and develop scholarship about intelligence as a function of government. And then in 2004, the International Association for Intelligence Education (IAFIE) was created to foster conversations that bridge the gap in the space of intelligence education.[20] More recently, in 2018 National Intelligence University helped establish the Intelligence Studies Consortium as a platform for information exchange and knowledge transfer for intelligence education programs in the Washington, DC area.[21] More institutionalized collaborative relationships of this kind will help information and knowledge sharing between academic intelligence studies and the intelligence community.

Intelligence education provides a valuable way to integrate intelligence studies knowledge produced in academia with the skills of the working intelligence professional to ensure that the intelligence community can meet and overcome the challenges of the future. As articles in this special issue highlight, this can be done through building that body of knowledge and teaching it to students, integrating aspects of training and skills development into the curriculum, or ensuring the socialization and acculturation of best practices for those who are likely to enter and encounter the sometimes unique challenges of the intelligence community's workforce. Articles like these help identify the best practices and ideas for improving current practice, and for that, the authors of these articles are to be commended for their valuable contributions to these conversations.

NOTES

[1] The meaning of the term "intelligence studies" is used to only refer to academic knowledge, as with other interdisciplinary "studies" fields. In that sense, "studies" is a noun, representing the body of knowledge. Other "studies" fields include terrorism studies, security studies, international security studies, and area studies. In 1986, the Intelligence Studies Section at the International Studies Association was created to foster and encourage the development of scholarship about intelligence as a function of government. However, beginning in the mid-2000s, "intelligence studies" also began to be used as a term to refer to vocationally oriented intelligence education programs. While a better name for these programs would be "intelligence schools"—per other vocationally oriented professional education programs—some have continued to use the term "intelligence studies" to refer to them.

[2] There is a large literature on bridging the gap between academic theory and government practice, with the following as the most significant in the political science/foreign policy space. *See*, for example, Alexander L. George, *Bridging the Gap: Theory and Practice in Foreign Policy* (Washington, DC: United States Institute of Peace Press, 1993).

[3] For an overview of the U.S. intelligence community's role within the U.S. government's machinery, *see* Stephen Marrin, "The United States," in *Routledge Companion to Intelligence Studies*, eds. Michael Goodman, Rob Dover, and Claudia Hillebrand (London: Routledge, 2013).

[4] Stephen Marrin, "Intelligence Studies Centers: Making Scholarship on Intelligence Analysis Useful," *Intelligence and National Security*, vol. 27, no. 3 (2012): 398-422.

[5] *See* Gregory F. Treverton, Seth G. Jones, Steven Borazmand, and Phillip Lipscy, "Conference Proceedings: Toward a Theory of Intelligence Workshop Report" (RAND National Security Research Division, 2006). For more on purposes of intelligence, *see* the literature on theory or theories of intelligence such as Stephen Marrin, Mark Phythian, and Peter Gill (eds), *Intelligence Theory: Key Questions and Debates* (London: Routledge, 2008); Stephen Marrin, Mark Phythian, and Peter Gill (eds), *Developing Intelligence Theory: New Challenges and Competing Perspectives* (London: Routledge, 2018).

[6] Jennifer Sims, "Defending Adaptive Realism: Intelligence Theory Comes of Age," in *Intelligence Theory: Key Questions and Debates*, edited by Peter Gill, Stephen Marrin, and Mark Phythian (London: Routledge, 2008), 151-165.

[7] Office of the Director of National Intelligence, "Vision 2015: A Globally Networked and Integrated Intelligence Enterprise" (2008).

[8] Stephen Marrin, "Intelligence Analysis Theory: Explaining and Predicting Analytic Responsibilities," *Intelligence and National Security* 22:6 (December 2007): 821- 846.

[9] Thomas Fingar, *Reducing Uncertainty: Intelligence Analysis and National Security* (Stanford, CA: Stanford University Press, 2011); David Omand, *Securing the State* (New York: Columbia University Press, 2010).

[10] Richard K. Betts, "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable," in *Intelligence Theory: Key Questions and Debates*, edited by Peter Gill, Stephen Marrin, and Mark Phythian (London: Routledge, 2008), 87-111; Robert Jervis, "Why Intelligence and Policymakers Clash," *Political Science Quarterly,* vol. 125.

[n]o. 2. (Summer 2010): 204.
[11] R.L. Frerichs and S. R. DiRienzio, "Establishing a Framework for Intelligence Education and Training," *Joint Forces Quarterly* 62 (3rd Quarter 2011): 68-73.
[12] For more on intelligence analysis training and education, *see* Stephen Marrin, "Training and Educating US Intelligence Analysts," *International Journal of Intelligence and Counterintelligence*, vol. 22, issue 1 (Winter 2008-2009): 131-146.
[13] Joseph. W. Gartin, "The Future of Analysis," *Studies in Intelligence* 63(2) (2019): 1–5.
[14] Nicholas Hare and Peter Coghill, "The Future of the Intelligence Analysis Task*," Intelligence and National Security*, 31(6) (2016): 858–870.
[15] Stephen Marrin and Sophie Cienski, "Experimenting with Intelligence Education: Challenges in the Design of Multidisciplinary Undergraduate Intelligence Analysis Programs in the United States," in *Routledge International Handbook of Universities, Security and Intelligence Studies* (ed. Liam Gearon). (London: Routledge. 2019).
[16] Rob Johnston, *Analytic Culture in the United States Intelligence Community: An Ethnographic Study*. (Washington, DC: Center for the Study of Intelligence, 2005); Bridget Rose Nolan, "Information Sharing and Collaboration in the United States Intelligence Community: An Ethnographic Study of the National Counterterrorism Center," PhD dissertation, University of Pennsylvania, 2013.
[17] Stephen Marrin. "Improving Intelligence Studies as an Academic Discipline," *Intelligence and National Security*, vol. 31, no. 2 (2016): 266-279.
[18] Stephen Marrin. "Academics and Practitioners: Competitors or Collaborators?" *Competitive Intelligence and Strategy*, vol. 3, issue 5, May 2010.
[19] For more on intelligence professionalization, *see* Stephen Marrin and Jonathan Clemente, "Modeling an Intelligence Analysis Profession on Medicine," *International Journal of Intelligence and Counterintelligence*, vol. 19, no. 4 (Winter 2006-2007): 642-665.
[20] Mark Lowenthal, "Intelligence as a profession: IAFIE Sets its Sights," *American Intelligence Journal* (2006).
[21] For the original vision of what became the Intelligence Studies Consortium, *see* Wes Westbrooks, "A Community Approach to Intelligence Studies and Research," Working paper (2018).

Dr. Stephen Marrin is Professor and Director of the Intelligence Analysis program in the School of Integrated Sciences at James Madison University, and editor of the journal Intelligence and National Security. Previously, he has held positions with Brunel University's Centre for Intelligence and Security Studies and Mercyhurst University's Intelligence Studies Department. Before that, he was an analyst with the Central Intelligence Agency and the U.S. Government Accountability Office (GAO). He holds a PhD from the University of Virginia and was chair of the Intelligence Studies Section at the International Studies Association from 2013-2018. A prolific author on aspects of intelligence analysis, the National Journal in 2004 profiled him as one of the 10 leading experts on the subject of intelligence reform.

American Intelligence Journal - Call for Submissions

The *American Intelligence Journal,* the professional journal of the National Military Intelligence Foundation, is pleased to announce a call for articles and book reviews for its fall 2025 edition. We're accepting submissions on any intelligence/national security topic related to "Professional Stewardship." This topic invites readers to submit a range of articles on issues involving the nature of intelligence as a "profession," the nature of "virtuous" intelligence practitioner, the legal and ethical challenges facing intelligence practitioners, the respective roles and responsibilities of current and retired intelligence officers, and the extent to which "dissent" has a place in professional practice. As always, we accept articles and book reviews that are both on and off theme.

Deadline and Submission. The deadline to submit an article or a book review is October 15, 2025.

Author's Guidelines. Submissions should be a simple Word document, in Times New Roman font, 12-point for text, and 10-point for notes. The citations can be either footnotes or endnotes (author's preference, as our layout software converts to endnotes anyway); double-spaced text to facilitate editing; single-space notes but double-space between entries; do not indent the first line of each paragraph of text, which should be formatted flush to the left margin. Draft articles should be 3,000-8,000 words in length, not counting notes; this can be waived only by permission of the editor and the criteria for waivers include the complexity of the topic, timeliness, and space available. You can also review previous journal editions on the NMIF website (nmif.org, under Publications) for sample articles.

Book Reviews. Book publication dates should normally be no older than 1-2 years; otherwise, the books can be stale, outdated, and/or already reviewed by too many other outlets. Book reviews should be 800-2,000 words in length; footnotes are not required or expected, but a few are acceptable. Longer reviews will be accepted if the reviewer can compare and contrast a new book with one or two other books on the same subject; these are considered "review essays," and will be listed as such in the table of contents. The journal editor is Dr. Chris Bailey; if you have an interest in writing a review, he will forward to you more detailed guidance in an Editor's Note titled "What Makes for a Great Book Review?" published in the "In My View" section of AIJ, Vol. 37, No. 2, 2020.

Questions? For any questions or inquiries, including the full Author Guidelines, please contact Dr. Christopher Bailey at christopherbailey286@yahoo.com.

Grounded Theory or Grounded in Theory: Implications for Practitioners and Academics of the Intelligence Community

by **Dr. David J. Kritz**

OVERVIEW

The U.S. Intelligence Community (IC) consists of 18 agencies and organizations. It is widely agreed upon that numerous theories exist to explain the phenomenon of the threats and opportunities facing practitioners, but there is yet to be a grand theory that encapsulates strategic intelligence. Theory is important because it helps us learn from history, understand the present phenomenon, and predict future events. Theoretical frameworks are important to academics as they help scope and structure research to address central research questions. Analyzing theoretical concepts may also apply to intelligence professionals trained on how priority intelligence requirements that often come with incomplete and ambiguous information are thought of to build more effective collection plans to gather relevant information to analyze for its customers to make more informed decisions. As intelligence programs are gaining popularity across academic institutions, ranging from certificates to terminal degrees, how academics teach research design may lead to formalizing and normalizing a grand theory on intelligence. The central research question guiding this article is *to what extent grounded theory can develop a grand strategic intelligence theory.*

THE AWARENESS AND UNDERSTANDING OF GROUNDED THEORY AS A RESEARCH METHOD AND GROUNDED IN THEORY AS A THEORETICAL FRAMEWORK

There is a difference between grounded theory as a qualitative research method and something grounded in theory as in a theoretical framework. These terms should not be discussed as interchangeable as it creates confusion. Distinguishing the terms matters because without profoundly understanding the meanings of both, it is unlikely that either would be leveraged appropriately and, at best, would not arrive at meaningful findings with results that matter to future researchers and at worst would create flawed research with invalid results. An assumption this researcher has is that the purpose of having a real education, at least the graduate level, is to be able to provide more options when faced with a dilemma and to work through complexity by applying a suitable research design (methodology + research method(s) + data gathering instruments) and/or the scientific method of research. Also, analytic tradecraft always applies to intelligence analysts.

GROUNDED IN THEORY

Grounded in theory is not a research method. Instead, it is primarily found in literature reviews that align with a qualitative methodology to provide a theoretical framework as a lens through which researchers may view phenomena to address research questions. Theoretical frameworks are important to construct meaning and gain a deeper understanding of problems, not by testing hypotheses or using the scientific method but by aligning phenomena to preexisting knowledge.

PRIMARY THEORIES FOR THE INTELLIGENCE COMMUNITY

Practitioners and students of intelligence under the context of military or national security issues may find the below theories of interest to learn from certain aspects of the past, understand current issues of the present, and make improved forecasts through refined analysis for future events. This researcher agrees with Mark Twain's adage that history does not repeat itself, but it often rhymes.[1] Those who have a deeper understanding of previous events and the dependent and independent variables present during the period will be better prepared in making analysis and presenting intelligence products to their customers to make more informed decisions. It should be noted that the below theories are meant to be a starting point for conversation and future research endeavors and are not all-encompassing. Theories that typically fall under international relations include constructivism, liberalism, and realism. However, readers of this journal should be aware that theories focused on national security issues are more expansive. As a starting point, this researcher selected theories depicted in alphabetical order that aligned with national security issues.

Cognitive Constructivist Theory

Students within certain academic institutions, such as the American Military University and the National Intelligence University intelligence programs, are often already within the IC workforce, and this portion of this student population can be labeled as student-practitioners. Cognitive constructivist theory centers on the educators' selected methods to increase learning effectiveness through the concepts that benefit students' cognitive processes to interpret and organize information. In short, it helps students construct meaning to the academic content that helps bridge academia to the work setting.

Cognitive constructivist theory largely stems from Jerome Bruner, an American psychologist, and Jean Piaget, the famous Swiss psychologist. Both are widely known for their work on cognitive development. According to the theory, "when the student's activity is stimulated; he/she uses previously acquired knowledge, anticipates, draws conclusions, and independently formulates solutions".[2] Cognitive constructivist theory posits that students acquire new knowledge when learning develops "through the assimilation of new information into existing cognitive structures (schemas) and the accommodation of these structures".[3] This theory aligns well with the pragmatic approach intelligence analysts conduct. Ortola (2024) states "Intelligence analysis is typically conducted by applying familiar ways of functioning in the world. Analysts accommodate some evidence and then attempt to decipher what the present is telling them".[4] This researcher suggests that in both analytic tradecraft and in academic learning environments, evidence and academic content that is presented can be built upon to create new knowledge at the individual level that can then be applied to add value at the organizational level and depending on the impact could affect the nation by helping to create more effective policy. As students are given the freedom to learn material that best makes sense to the individual student, the cognitive constructivist theory posits that it is an active learning technique to increase knowledge.

Communication Theory

Communication theory is applicable to gain a deeper understanding of communication processes as people communicate intentions, plans, ideas, disinformation, and propaganda. Communication theory includes how communications are delivered, received, and interpreted. Previous research suggests that communication theory can be viewed through multiple lenses. van Ruler (2018) depicts three lenses to observe how the processes occur include: 1) communication as a one-way process of meaning construction; 2) communication as a two-way process of meaning construction, in which two or more people construct new meanings together; and 3) communication as an omnidirectional diachronic process of meaning construction, "in which the focus is on the continuous development of meaning itself."[5] Communication theory touches upon the major intelligence disciplines for collection, especially with open source intelligence.

Intelligence Analysis Theory

Dr. Stephen Marrin, an intelligence practitioner and scholar, commenced a general theory of intelligence. The essence of intelligence analysis theory is that "information or intelligence can enable the application of power with greater efficiency or effectiveness".[6] Marrin (2007) argues that intelligence is used to wield power with increased precision.[7] This is a valid argument as information is one of the instruments of power that is often portrayed in the Diplomacy, Information, Military, and Economics (DIME) paradigm.

Liberalism

Liberalism, as opposed to realism or conservatism, is another grand theory within international relations that can be defined as "a political philosophy based on belief in progress and stressing the essential goodness of the human race, freedom for the individual from arbitrary authority, and protection and promotion of political and civil liberties".[8] Liberalism is a philosophy that starts from the premise that political authority and law must be justified, and seeks freedom for the individual and a move toward a smaller government. If citizens are obliged to exercise self-restraint, especially if they are obliged to defer to someone else's authority, there must be a reason. Restrictions on liberty must be justified.[9] One of the shortcomings of liberalism theory is the belief that humans are perfectible.

National Security Theory

As the U.S. IC is charged with assessing and warning of the threats and opportunities that face the nation, it makes sense that national security theory is one of the most significant theories for exploration and application. Previous researchers adroitly argue that "National interests are realized in conditions of global challenges, risks and uncertainty. In this regard, when developing and implementing planning and policy documents at all levels of State-building, there is a need to know and assess real and potential threats."[10] This aligns with the unclassified version of *The Annual Threat Assessment of the U.S.*

Intelligence Community, which is published by the Office of the Director of National Intelligence each spring. The 2024 version focused on the following themes: state actors, nonstate actor issues such as human trafficking, transnational issues such as weapons of mass destruction and disruptive technology, and health security.[11] Interestingly, the 2025 version was pared down to two primary themes: nonstate transnational criminals and terrorists, and major state actors.[12]

Normative Ethics

Civilian national security leaders select how to respond to threats. The warfighters' morals and ethics within the profession of arms affect how war is waged and have implications that ripple throughout the tactical, operational, and strategic levels of nation-states. "Every member of our team — whether enlisted, officer, or civil servant — is responsible for embodying and upholding the high standards that come with serving the United States in the Profession of Arms".[13] There are three prominent normative theories that act as lenses to explain how to address moral questions: virtue ethics, deontology, and consequentialism. What separates each of these theories is where the emphasis is placed. Virtue ethics focuses on the agent and what the agent needs to be virtuous to accomplish the objective.[14] Deontology is derived from the Greek words *deon* (duty) and *logos* (science).[15] The focus of deontology is centered on the rightness and wrongness of individuals' selected actions.

Organizational Learning Theory

Organizational learning theory's definition follows its label as it "focuses on how organizations acquire, retain, and apply knowledge to improve performance and adapt to changing environments".[16] It is not a leap in logic to see these themes within the definition align with some of the intelligence cycle's elements, including collection and analysis. Organizational learning theory refers to how organizations learn from previous mistakes to increase performance, and unlike the U.S. IC, which appears to primarily focus on intelligence failures as case studies, it primarily focuses on successes.[17]

Realism

Realism, also referred to as classical realism, is one of the significant theories in international relations. Realism's primary theme centers on power. As a foil to liberalism, it portends the notion that nation-states act in their own self-interest and are in direct competition with one another. Students of the Profession of Arms are familiar with the historical thought leaders of realism, including Thomas Hobbes, Niccolò Machiavelli, Friedrich Nietzsche, Thucydides, and Max Weber. Realism posits that "states exist within an anarchic international system in which they are ultimately dependent on their own capabilities, or power, to further their national interests. Within realism theory, as international politics are considered anarchic, sovereign states (principal actors) are considered rational.[18] The most important national interest is the survival of the state, including its people, political system, and territorial integrity".[19]

Emanating from realism, neo-realism, also called structural realism, is more contemporary and is another leading theory in international relations that focuses on state survival and how power is wielded. The significant difference between the two theories posits that "unlike classical realism, which views war, conflict, and struggles for power as a consequence of the nature of states, neorealism views these political phenomena as a function of how the international system is structured. States exist by themselves in a system characterized by anarchy".[20]

Technological Determinism Theory

Over the last two decades, the world has become more interconnected through technology such as social media. What may be taken for granted by younger generations, technology has truly broken down barriers. Social media allows its users to associate regardless of distance, culture, and social status with instant communication. It is not hyperbolic to claim that social media has shaped people's lives and personalities by having an online persona. Theory can help explain what is known about a phenomenon and how different independent variables affect the dependent variable. For the purpose of this paper, technological determinism theory will help explain how characteristics within technology affect human intelligence (HUMINT). Technological determinism explores "media's systems and mediated content's cultures in contemporary societies … and takes into account the influences of media on the respective societies".[21] Technological determinism can be defined as:

> The claim that technology causes or determines the structure of the rest of society and culture. Autonomous technology is the claim that technology is not in human control, that it develops with a logic of its own. The two theses are related. Autonomous technology generally presupposes technological determinism. If technology determines the rest of culture, then culture and society cannot affect the direction of technology. Technological determinism does not, on the face of it, presuppose autonomous technology. It could be that free, creative inventors devise technology, but that this technology determines the rest of society and culture.[22]

GROUNDED THEORY AS A RESEARCH METHOD

Grounded theory as a research method may be highly instrumental in forming a holistic grand intelligence theory as a process through conducting human subject research of the intelligence workforce. Grounded theory as characterized by Creswell, who is largely considered the subject matter expert on research design, defines grounded theory as "a qualitative strategy in which the researcher derives a general, abstract theory of a process, action, or interaction grounded in the views of the participants of a study."[23] The last part is important for those conducting research as it means human subject research, which requires approval from an Institutional Review Board. Although grounded theory falls under a qualitative methodology, a mixed methods approach of quantitative data-gathering instruments such as surveys could be used to create large data sets and, with testing hypotheses and the use of statistical analysis, help determine correlation and/or causation, which would likely add scientific rigor. Conversely, by using qualitative data-gathering instruments such as questionnaires and interviews, a researcher could observe a deeper understanding of the human elements that could add greater context and nuance to aid leaders in forming a more agile, efficient, and effective agency or organization.

Previous research posits there are four major themes labeled as core canons that researchers using grounded theory as a research method must abide by: 1) It is an iterative process of data collection and analysis; 2) theoretical sampling; 3) constant comparative method; and 4) the explanation of coding and the theory building process.[24]

CONCLUSION

In conclusion, this article presents an argument that grounded theory can be used to promote research endeavors as a theoretical framework and may be a catalyst for developing a holistic grand theory of intelligence through the use of grounded theory as a research method. This article was meant as a starting point for theoretical frameworks that align with the responsibilities of the U.S. IC workforce. Numerous other theoretical frameworks may be explored for future research. For those focusing on intelligence as an organization, theories on integration, group dynamics, and information hoarding may be explored. For those focusing on intelligence as an activity, theories on cognition, information, and technology may be explored

NOTES

[1] Mark Twain, https://www.owu.edu/alumni-family-friends/owu-magazine/fall-2018/history-doesnt-repeat-itself-but-it-often-rhymes/, accessed on April 3, 2025.

[2] Grzegorz P. Karwasz and Katarzyna Wyborska, "How Constructivist Environment Changes Perception of Learning: Physics is Fun," Education Sciences 13, no. 2 (2023, 2023): 195. doi:https://doi.org/10.3390/educsci13020195. http://ezproxy.apus.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fscholarly-journals%2Fhow-constructivist-environment-changes-perception%2Fdocview%2F2779540081%2Fse-2%3Faccountid%3D8289.

[3] Teach Thought Staff (Website), "What is Cognitive Constructivism," (2024), https://www.teachthought.com/learning/what-is-cognitive-constructivism/

[4] Carles Ortola, "A Unified Theory for Intelligence Analysis," Intelligence and National Security 39 (4) (2023): 677. doi:10.1080/02684527.2023.2272349.

[5] B. van Ruler, "Communication Theory: An Underrated Pillar on Which Strategic Communication Rests," International Journal of Strategic Communication, 12(4) (2018), 368. https://doi.org/10.1080/1553118X.2018.1452240

[6] Stephen Marrin, "Intelligence Analysis Theory: Explaining and Predicting Analytic Responsibilities," Intelligence and National Security 22 (6) (2007): 827, doi:10.1080/02684520701770634.

[7] Stephen Marrin, "Intelligence Analysis Theory: Explaining and Predicting Analytic Responsibilities," Intelligence and National Security 22 (6) (2007): 821–46. doi:10.1080/02684520701770634.

[8] Merriam-Webster.com, "Liberalism," https://www.merriam-webster.com/dictionary/liberalism

[9] "Liberalism," Stanford Encyclopedia of Philosophy, February 22, 2022, accessed April 7, 2025.

[10] Beibut Yergaziev, Yerdan Bazarov, Zhanybek Amanov, Vassiliy Mamonov, and Urkiya Smailova. "Methodology for Informational Base Preparation for Development of Preventive Measures and Threat to National Security Manageability," Journal of Advanced Research in Law and Economics 10, no. 8 (Winter, 2019): 2575, https://doi.org/10.14505/jarle.v10.8(46).36.

[11] Office of the Director of National Intelligence, The Annual Threat Assessment of the U.S. Intelligence Community (2024), accessed April 2, 2025, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf.

[12] Office of the Director of National Intelligence, The Annual Threat Assessment of the U.S. Intelligence Community (2025), accessed April 2, 2025, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf

[13] Frank Kendall, "A Profession of Arms: Our Core Values," U.S. Air Force (May 16, 2022), https://www.doctrine.af.mil/Portals/61/documents/Airman_Development/BlueBook.pdf

[14] Nico J. Grönum, "A Return to Virtue Ethics: Virtue Ethics, Cognitive Science and Character Education," Verbum Et Ecclesia 36, no. 1 (2015): 1.

[15] Łukasz Kiraga and Andrzej Dzikowski, "Ethical Concerns of the Veterinarian in Relation to Experimental Animals and in Vivo Research," Animals 13, no. 15 (2023): 2476, https://doi.org/10.3390/ani13152476. 3.

[16] Bradley J. Olson, Satyanarayana Parayitam, Matteo Cristofaro, Yongjian Bao, and Wenlong Yuan, "CEO Anger: A Catalyst for Error Recognition and Learning," Management Decision 62, no. 13 (2024): 1-25. doi:https://doi.org/10.1108/MD-12-2022-1750.

[17] Bradley J. Olson, Satyanarayana Parayitam, Matteo Cristofaro, Yongjian Bao, and Wenlong Yuan, "CEO Anger: A Catalyst for Error Recognition and Learning," Management Decision 62, no. 13 (2024): 1-25. doi:https://doi.org/10.1108/MD-12-2022-1750.

[18] Notre Dame International Security Center, "An Introduction to Realism in International Relations," July 21, 2022, accessed April 7, 2025, https://ndisc.nd.edu/news-media/news/an-introduction-to-realism-in-international-relations/.

[19] Duncan Bell, “Realism: International Relations,” Britannica (2025), accessed April 7, 2025, https://www.britannica.com/topic/realism-political-and-social-science.
[20] American Public University System, Theory Review, 6.
[21] Azam Jan, Sadaf Naz Shakirullah, Owais Khan, and Abdul Qayum Khan, "Marshal McLuhan's Technological Determinism Theory in the Arena of Social Media," Theoretical and Practical Research in Economic Fields 11, no. 2 (Winter, 2020): 133-137, https://doi.org/10.14505/tpref.v11.2(22).07.
[22] Jonas Hallström, "Embodying the Past, Designing the Future: Technological Determinism Reconsidered in Technology Education," International Journal of Technology and Design Education 32, no. 1 (March 2022): 17-31. https://doi.org/10.1007/s10798-020-09600-2; Val Dusek, Philosophy of Technology: An Introduction (Malden, MA: Blackwell, 2006).
[23] John W. Creswell, Research Design: Qualitative, Quantitative, Mixed Methods Approaches (Thousand Oaks, CA: Sage, 2009), 229.
[24] Bruce Gurd, "Remaining Consistent with Method? an Analysis of Grounded Theory Research in Accounting," Qualitative Research in Accounting and Management 5, no. 2 (2008): 122-138, doi:https://doi.org/10.1108/11766090810888926.

Dr. David J. Kritz is a full professor and the assistant department chair for the Intelligence Programs at the American Military University, an adjunct professor for the University of Mississippi (Ole Miss, and also at Empire State College (State University of New York). He is the assistant editor for The American Intelligence Journal and an official reviewer for the Journal of Leadership Education. He is a retired U.S. Air Force intelligence officer. He earned his Doctor of Business Administration degree from Walden University.

2024 Night of Heroes Gala Senior Leaders, Awardees and Scholars

Building the Intelligence Workforce of Tomorrow:
Adapting Education for Emerging Threats

by **Dr. Valerie E. Davis**

INTRODUCTION

In today's fast-evolving security landscape, intelligence agencies face increasing pressure to reform—not just in terms of tools and tactics, but also in how they train their personnel. With the escalation of cyber threats, the emergence of artificial intelligence, and global disinformation efforts, the intelligence workforce must be agile, adaptable, and forward-thinking. Encountering these challenges head-on requires more than operational shifts—it calls for a structural rethinking of how we educate and train the next generation of intelligence professionals. Structuring a workforce ready for tomorrow requires reshaping our learning systems today, positioning them to meet the realities of a rapidly changing geopolitical and technological landscape.

THE EMERGENCE OF NEW THREATS

Global security has entered a period of increased instability in recent years. As emphasized in the *Global Trends 2040: A More Contested World report by the National Intelligence Council*, the nature of global conflict is undergoing significant changes and challenges, with both state and non-state actors leveraging novel technologies to achieve their strategic objectives.[1] One of the most pressing challenges facing today's intelligence community is the upsurge in cyber threats. Adversaries now can breach critical infrastructure, compromise classified data, and sway public perception with incredible speed and impact.

Similarly troubling is the increasing use of artificial intelligence and machine learning by state actors to gain a competitive advantage in intelligence collection and warfare. The intersection of AI and cyber threats has generated an urgent need for intelligence agencies to develop new methodologies for threat detection, data analysis, and strategic decision-making. As these challenges intensify, intelligence professionals must become proficient in traditional intelligence practices and innovative technologies that define modern warfare and security.[2]

THE NEED FOR A TECHNOLOGICALLY PROFICIENT WORKFORCE

The workforce of tomorrow must be multidimensional, agile, and deeply familiar with emerging technologies. The U.S. Office of the Director of National Intelligence (ODNI) in the *Intelligence Community Data Strategy 2023-2025* emphasizes that the Intelligence Community's workforce must adapt to rapidly changing technological advancements, particularly in artificial intelligence, machine learning, and cybersecurity. As the strategy makes clear, to counter modern threats effectively, intelligence professionals must have a deep understanding of key technologies such as artificial intelligence, big data analytics, and cybersecurity tools—each playing a key role in identifying, analyzing, and responding to complex security challenges.[3]

While traditional intelligence skills, such as human intelligence (HUMINT), signals intelligence (SIGINT), and imagery analysis, will always be crucial, incorporating innovative technologies is paramount to staying ahead of evolving threats. According to the *Intelligence and National Security Foundation* (INSF) and Srini Pallia*,* the surge of AI in intelligence operations is not merely an improvement of existing tactics, techniques, and procedures (TTPs) but an essential shift in how intelligence is gathered, analyzed, and acted upon.[4] From automating repetitive data processing to predicting adversary activities through machine learning algorithms. Artificial Intelligence (AI) will be at the crux of intelligence operations in the future.

REVOLUTIONIZING INTELLIGENCE EDUCATION

To plan the intelligence workforce for these new challenges, education and training programs must transform. Conventional intelligence training programs, while successful in producing skilled professionals in traditional intelligence fields, must incorporate modern, interdisciplinary methodologies that incorporate modern technologies and methodologies. As posited by Pradhan

and Saxena, intelligence agencies need to "reexamine how we educate and train our workforce to effectively counter threats, Intelligence professionals must have a deep understanding of key technologies such as artificial intelligence, big data analytics, and cybersecurity tools. Equally important is ensuring they possess the judgment and ethical grounding necessary to navigate the complex and often uncertain environments in which these tools are applied."[5]

Integrating cybersecurity, AI, data science, and machine learning into intelligence curricula is crucial to creating a workforce that can address the modern threats presented by adversaries. A report from the *Intelligence Research Institute* emphasizes that educational institutions must develop robust programs that offer intelligence professionals the technical and analytical skills needed for the future of security.[6] This involves creating collaborations between government agencies, military institutions, and academia to develop educational pipelines that merge technical experience with the strategic philosophy needed to navigate global intelligence challenges.

Moreover, it is not enough to teach technical skills. The intelligence workforce of tomorrow will require a more comprehensive understanding of global geopolitics, regional security dynamics, and cultural intelligence to operate effectively in diverse and often complex environments. As K.M. Vogel argues, the future intelligence professional must possess not only technical capabilities but also a deep understanding of political and social lexicons, as well as the ethical considerations that shape intelligence operations.[7]

ETHICAL CONSIDERATIONS AND WORKFORCE INTEGRITY

As the intelligence community increasingly relies on technologies such as AI, big data, and surveillance tools, ethical considerations must be integrated into the educational framework to ensure that future intelligence professionals are not only technically proficient but also capable of making informed, morally sound decisions in ambiguous situations. Wheatley explores these concerns, emphasizing the need for intelligence professionals to understand the moral and legal frameworks that regulate surveillance and data collection.[8] Integrating ethics alongside technical training promotes a workforce that is competent and principled. The ethical implications of these technologies are profound, particularly in terms of privacy, civil liberties, and accountability in intelligence operations.

Educational programs must not simply teach technical skills but also encourage a sense of responsibility and integrity in intelligence professionals. As the ODNI suggests, fostering a workforce that understands the ethical use of innovative technologies is fundamental to maintaining public trust and ensuring that intelligence operations are conducted within legal and ethical boundaries.[9]

LEVERAGING TECHNOLOGY TO ENHANCE LEARNING

Additionally, technology can play a fundamental part in transforming intelligence education. Virtual simulations, augmented reality (AR), and AI-driven adaptive learning platforms pose immersive and customized training experiences that mirror everyday scenarios. These mechanisms can fast-track learning, improve decision-making under pressure, and bridge the gap between theoretical knowledge and practical application. As ODNI delineates, implementing such technologies in training programs is vital to preparing the workforce for the increasingly complex landscape of modern intelligence operations.[10]

By simulating high-stakes decision-making environments and creating realistic operational scenarios, AI-powered training systems empower intelligence professionals to enhance key skills in analysis, interagency collaboration, and crisis management. These simulations not only improve technical proficiency but also promote the cognitive agility needed to respond effectively in volatile and high-pressure situations.

THE FUTURE OF TRAINING: PREPARING THE RENAISSANCE ANALYST

As intelligence operations grow progressively multifaceted, training and education programs must evolve to produce analysts capable of navigating an increasingly shifting landscape. Artificial Intelligence (AI) functions as a vast domain that incorporates a range of subcategories, including computing, large-language models, and machine learning. These technologies are not only modernizing intelligence collection and analysis but are also redefining the skill sets needed of tomorrow's professionals.[11]

Developing and applying AI-driven intelligence methods necessitates a robust understanding of algorithm design, statistical modeling, and computational methodologies. Intelligence professionals must understand not only how these systems function but also how to interpret their outputs properly and apply them successfully in operational environments. Today's intelligence

professionals need to combine technical experience with strategic insight, acting as the critical link between raw data and actionable intelligence. This collective capability safeguards that data is not only processed efficiently but also contextualized within greater security and policy frameworks.

To develop this "renaissance" analyst—one who effortlessly combines traditional intelligence practices with evolving technological competences—intelligence education programs must experience a fundamental change. Academic institutions such as American Military University (AMU) and other advanced training centers are modifying their curricula to include challenging coursework in data analytics, automated decision-support systems, and ethical considerations of AI in intelligence operations.[12] Training must underscore not only technical proficiency but also the 5'Cs (critical thinking, creative thinking, collaboration, communication, and curiosity), operational adaptability, and interdisciplinary collaboration.[13]

The intelligence workforce of the twenty-first century is required to operate in an environment where AI enhances human decision-making rather than replaces it. Training programs must teach analysts to interpret AI outputs, validate conclusions, and apply human judgment in critical situations.[14] Combining AI and traditional data literacy will prepare analysts for the digital intelligence landscape.[15]

CONCLUSION

The Intelligence Community faces a momentous moment as it traverses an increasingly complex security landscape dominated by cyber threats, artificial intelligence, and evolving geopolitical challenges. To sustain a strategic advantage, intelligence organizations must promote a workforce that is not only proficient in advancing technologies but also adaptable, ethically grounded, and capable of interdisciplinary partnership.

Today's intelligence education and training must advance outside traditional tradecraft to include AI-driven analytics, cybersecurity expertise, and data science methodologies. Incorporating these capabilities with foundational intelligence disciplines, institutions can produce a new generation of intelligence professionals armed to analyze and respond to threats with both technical acumen and strategic foresight. Moreover, fostering critical thinking, ethical reasoning, and cross-sector collaboration will be significant in ensuring intelligence operations remain both effective and aligned with democratic principles.

As artificial intelligence continues to redesign intelligence collection and analysis, the function of human judgment remains indispensable. Training programs must underscore AI literacy, analytical rigor, and operational adaptability to train intelligence professionals for an era in which machine-augmented decision-making plays a fundamental role. The intelligence workforce of the future must not only interpret and validate AI-generated insights but also traverse the ethical and strategic implications of these technologies in a global security setting.

Lastly, only by cultivating a technologically proficient, ethically responsible, and strategically agile workforce can the Intelligence Community ensure its continued effectiveness in safeguarding national security. The transformation of intelligence education is not just an option; it is essential for ensuring that the United States maintains its competitive edge in an era defined by rapid technological advancements and emerging global threats.

NOTES

1National Intelligence Council, *Global Trends 2040: A More Contested World* (2021).2 Secretary of Defense Lloyd J. Austin III, *Strategy for Operations in the Information Environment* (Washington, DC: U.S. Department of Defense, 2023).

[3] Office of the Director of National Intelligence, *Intelligence Community Data Strategy 2023-2025* (Washington, DC: Office of the Director of National Intelligence, 2023).

[4] Intelligence and National Security Foundation (INSF). *Future of the IC Workforce*, in collaboration with Avantus Federal (December 2022), https://www.insaonline.org/docs/default-source/uploadedfiles/2022/insf-white-paper-future-of-ic-workforce.pdf; Srini Pallia, *Reshaping work in the Intelligence Age: The Path to Building a Future-Proof Workforce*. (World Economic Forum, 2025).

[5] I.P. Pradhan and P. Saxena, "Reskilling Workforce for the Artificial Intelligence Age: Challenges and the Way Forward," in *The Adoption and Effect of Artificial Intelligence on Human Resources Management, Part B*, edited by P. Tyagi, N. Chilamkurti, Grima, K. Sood, and B. Balusamy (Leeds, UK: Emerald Publishing Limited, 2023), 181-197, https://doi.org/10.1108/978-1-80455-662-720230011.

[6] Intelligence Research Institute. *Adapting Intelligence Studies and Education for a Rapidly Changing Global Landscape* (Intelligence Research Institute, 2024), https://www.intelligence-research.org.il/editor/assets/Adapting%20Intelligence%20Studies%20and%20Education%20for%20a%20Rapidly%20Changing%20Global%20Landscape.pdf.

[7] K.M. Vogel and B. B. Tyler, "Interdisciplinary, Cross-Sector Collaboration in the US Intelligence Community: Lessons Learned from Past and Present Efforts," *Intelligence and National Security* 34, no. 6 (2019): 851–880.

[8] Mary Christine Wheatley, *Ethics of Surveillance Technologies: Balancing Privacy and Security in a Digital Age* (Premier Science, Wheatley Research, 2024).

[9] ODNI, *Intelligence Community Data Strategy 2023-2025.*

[10] Ibid.
[11] W. Chang and P.E. Tetlock, "Rethinking the Training of Intelligence Analysts," *Intelligence and National Security* 31, no. 6 (2016): 903–920.
[12] A. Blanchard and M. Taddeo, "The Ethics of Artificial Intelligence for Intelligence Analysis: A Review of the Key Challenges with Recommendations," *Digital Society* 2, no. 1 (2023): 12.
[13] Justina A. Sava, *Soft Skills Needed by Security Professionals Worldwide 2022*, Statista Accounts, 2022. https://www.statista.com/statistics/1322692/cybersecurity-important-soft-skills-worldwide/.
[14] B. Goldfeder, J. Davis, M. Pillarick, and R. Menon, "Learning and Reasoning with AI: Restructuring Intelligence Organizations Around Innovation," in *Fostering Innovation in the Intelligence Community*, ed. C.W. Gruber and B. Trachik, *Annals of Theoretical Psychology*, vol. 19 (Cham: Springer, 2023).
[15] Alice Toniolo et al., "Human-Machine Collaboration in Intelligence Analysis: An Expert Evaluation," *Intelligent Systems with Applications* 17 (February 2023): 200151.

Valerie E. Davis, PhD, serves as Associate Professor of Intelligence Studies and is an expert in training, human intelligence ideology, strategy, and cyber intelligence at the American Public University System (APUS). Before joining APUS, Dr. Davis served 24 years as an intelligence professional in the United States Air Force. She has over 30 years of experience working and studying information warfare, training, and operational strategies. She earned her Ph.D. from Northcentral University, researching critical skills to harness insights that inform leadership strategies, foster innovation, and strengthen organizational resilience.

2024 Night of Heroes
Senior IC Leaders

Intelligence Studies Redefined: Designing an Attractive, Structured, and Future-Ready Discipline in Service to the Nation

by **Dr. Anthony Ioannidis and Mr. Anastasios-Nikolaos Kanellopoulos, Ph.D. candidate**.

INTRODUCTION: THE URGENT NEED TO REINVENT INTELLIGENCE STUDIES

In an era of fast organizational, technical, and geopolitical change, the field of intelligence studies needs to be radically rethought to serve national security and the public good effectively. Lack of industrial alignment, interdisciplinary integration, and standardization has long plagued intelligence education. While other academic disciplines, like data science, cybersecurity, and business administration, have developed to draw top talent and satisfy labor market demands, intelligence studies are still limited by inflexible academic frameworks and antiquated teaching methodologies that do not adequately prepare professionals for actual security threats.[1]

Further evidence of this stagnation suggests that intelligence education needs to strike a balance between Root Values—the philosophical and ethical tenets that underpin intelligence work—and Root Skills—the practical abilities like cybersecurity, risk management, and analysis. However, intelligence programs frequently overlook these crucial elements, which keep students from gaining a thorough, multidisciplinary grasp of their role in preserving national security.[2] This view is also supported by other research,[3] which emphasizes the need for multidisciplinary learning, technology integration, and professional relationships to address real-world security concerns and transcend theoretical discussions in intelligence education.

Moreover, national security is directly threatened by the inability to update intelligence studies.[4] Intelligence agencies, private sector companies, and associated partners find it difficult to attract professionals with the technical, strategic, and analytical capabilities needed to handle new security threats in the absence of an organized and innovation-driven educational paradigm.

This study suggests a bold transformation of intelligence education to address these shortcomings by establishing a Mega-University, based on the expansive, globally connected establishments outlined by Penprase and Pickus (2024).[5] By combining business administration, political science, international relations, security studies, and emerging technologies into a disciplined, future-ready academic field, this mega-university would act as the hub of a global intelligence studies ecosystem.

Intelligence education can transcend outdated paradigms and concentrate on experiential learning, multidisciplinary cooperation, and strategic business connections by implementing the Mega-University model. This change would result in highly qualified professionals who are dedicated to preserving democratic principles, ethically sound, and analytically strong, in addition to being technically proficient. This kind of redefinition for intelligence studies is necessary to keep the discipline competitive, relevant, and ready to handle security concerns in the 21st century in both domestic and international settings.

PILLAR 1: GENERATING PRESTIGE FOR INTELLIGENCE STUDIES

Establishing intelligence studies as a reputable academic field that can draw elite faculty, students, and international collaborations requires establishing its status. Institutional reputation is frequently used as a stand-in for excellence in the status hierarchy that underpins the U.S. and international higher education systems.[6] This structure is shaped by faculty research output, accreditation standards, and university rankings, which drive new universities to imitate more established ones. However, this conventional approach frequently places more emphasis on research publications than on multidisciplinary education, creativity, and direct assistance to intelligence professionals—all of which are critical components of modernizing intelligence studies.

To redefine intelligence education within a Mega-University framework, prestige generation must be strategically balanced with innovation. Conventional prestige in higher education is typically driven by investments in infrastructure, faculty recruitment, and global reputation.[7] Besides, for intelligence studies to thrive within a globally networked, future-ready

academic model, prestige must be built on academic and professional impact, elite faculty recruitment, strategic global partnerships, and experiential learning—the key pillars of a Mega-University intelligence ecosystem.[8]

Academic and Professional Impact

High-impact research, notable publications, and active industry participation are necessary to establish intelligence studies as an elite field.[9] Intelligence research could grow into an influential and reputable academic and professional discipline by coordinating with operational intelligence requirements and national security policies. Instead of operating in a purely theoretical realm, the Mega-University model must guarantee that intelligence education makes a significant contribution to the development of policies, technological breakthroughs, and strategic intelligence operations.

Elite Faculty Recruitment

Building institutional prestige is mostly dependent on hiring renowned academics and professionals.[10] Top-tier students are attracted to institutions with established leaders in security studies, business administration, intelligence, and emerging technologies. Employing academics with extensive business experience, outstanding research, and the capacity to connect academic theory with practical intelligence practices should be a top priority for universities wishing to develop intelligence studies as a distinguished field.[11] The Mega-University idea, whereby professional intelligence groups and academic organizations work together to create training and scholarships that are operationally relevant, is reflected in this transdisciplinary expertise.[12]

Global Partnerships and Intelligence Networks

A globally connected intelligence education model must leverage strategic partnerships across multiple sectors to enhance institutional standing and ensure intelligence education remains aligned with industry trends.[13] Collaborations with intelligence agencies provide classified research opportunities, specialized training, and direct talent pipelines. Partnerships with private-sector intelligence and risk management firms further reinforce the university's role as a bridge between academic theory and intelligence practice. Additionally, alliances with international organizations and allied intelligence institutions foster cross-border intelligence cooperation, student exchange programs, and joint research initiatives. These partnerships strengthen the university's reputation as a leading provider of intelligence education, ensuring students gain exposure to real-world intelligence challenges, applied research projects, and career opportunities within global security networks.

Experiential and Applied Learning

An important factor in setting up intelligence studies apart from more conventional academic fields is experiential and applied learning, which goes beyond collaboration and recruiting faculty.[14] Case-based learning, simulation-based training, and field experiences must be prioritized in intelligence education in place of traditional political science and history-based courses. The Mega-University model places a strong emphasis on experiential, technologically advanced, and internationally connected learning opportunities, all of which are critical components of contemporary intelligence education.

PILLAR 2: CREATING A SUSTAINABLE BUSINESS MODEL

Even when a start-up university successfully inherits or establishes prestige, it cannot achieve long-term success without a solid and sustainable business model. The financial viability of an institution is critical for maintaining high-quality education, ensuring operational stability, and expanding its global impact.[15] A Mega-University—particularly one designed to serve the evolving intelligence landscape—must secure robust initial funding while simultaneously developing a long-term financial strategy that fosters independence, flexibility, and resilience. Achieving this requires diversifying funding sources across public, private, and philanthropic sectors, building strategic partnerships that align financial sustainability with institutional mission, and leveraging innovative revenue-generating programs without compromising academic excellence.[16]

Addressing the Financial Challenges of a New Intelligence Mega-University

One of the primary challenges new academic institutions face is the high cost of providing top-tier education, especially without the longstanding alumni networks, endowments, and financial backing that established universities enjoy. Traditional universities benefit from legacy funding mechanisms, while new institutions must employ innovative financial strategies to ensure sustainability from inception.[17] To navigate this challenge, a Mega-University for intelligence studies must go beyond standard tuition-based models by integrating multiple revenue streams, public-private collaborations,

and industry-aligned education initiatives. This not only ensures financial stability but also enhances the university's relevance in the intelligence and security sectors.

A Hybrid Funding Model for an Intelligence Mega-University

A hybrid finance strategy functions effectively for an intelligence education paradigm that is internationally networked. The university's position as a strategic national asset will be strengthened by government funding, which will be essential for supporting intelligence training programs, classified research, and national security projects. Diversifying financial sources is crucial since relying just on government support could result in regulatory restrictions.

The university's financial sustainability will be greatly strengthened by private sector investment, especially through collaborations with corporations, defense firms, critical infrastructure and utility providers, cybersecurity firms, and financial institutions that gain access to talent pipelines and intelligence-driven insights. These partnerships guarantee that the curriculum remains in line with industry demands, along with providing funds. Additionally, philanthropic contributions and endowments from foundations, industry leaders, and intelligence community veterans can establish scholarships, research grants, and faculty development funds, further strengthening financial stability while expanding access to students from diverse backgrounds.

Tuition-based revenue must also be strategically structured to ensure affordability while maintaining financial health. A flexible pricing model, including executive education, professional certification programs, and digital learning platforms, can generate continuous income while expanding access to intelligence education on a global scale. By adopting this multifaceted funding approach, the Mega-University can balance financial resilience with academic independence, ensuring that it remains adaptable and mission-driven.

Expanding Revenue Streams Through Intelligence Education Innovation

Beyond traditional funding mechanisms, an intelligence Mega-University must leverage innovative educational models to create sustainable revenue streams while increasing its global reach.[18] Executive education and certification programs tailored for government agencies, corporations, and security professionals provide an opportunity for recurring revenue while enhancing professional training in intelligence disciplines. Additionally, the integration of AI-driven online learning platforms, hybrid intelligence programs, and global intelligence studies networks will allow the university to scale its offerings beyond physical classrooms, increasing both financial sustainability and accessibility.

Significant financial support can also be obtained through strategic partnerships on government and industry research projects. The university could establish itself as a preeminent research center and obtain steady funding sources by collaborating with public and private organizations on classified and open-source intelligence research initiatives. Additionally, the establishment of think tanks and endowed research institutes devoted to cybersecurity, geopolitical intelligence, and future security threats would boost institutional credibility and draw in ongoing research grants and donor funding.

Balancing Financial Prudence with Academic Excellence

Financial sustainability must align with the institution's mission—to deliver world-class intelligence education while serving national and global security needs. Ensuring long-term financial health requires a careful balance between securing diversified funding sources, strategically managing tuition models, and leveraging public-private partnerships to enhance research, training, and professional development.

PILLAR 3: RE-BUILD AND RE-LAUNCH

Once the initial vision, prestige generation, and financial strategy are in place, the build-and-launch phase marks a crucial step in establishing a new intelligence education model. The early years of a new institution are critical in shaping its long-term trajectory, requiring carefully planned strategies to ensure a strong and sustainable foundation. Approaches such as incubation periods, structured codesign processes, and phased launches allow the institution to refine its identity, academic framework, and operational structure before fully opening as a globally recognized university.[19]

Incubation Phase: Refining the Academic and Institutional Model

An incubation phase serves as an internal development period, allowing for iterative refinement of curriculum design, faculty recruitment, and administrative structures. Institutions that invest in incubating their programs before a full-scale launch tend to establish a more coherent academic culture and institutional identity.[20] This approach enables the university to test methodologies, gather feedback from early participants, and ensure alignment with the needs of future students and intelligence professionals. A well-executed

incubation phase can mitigate early operational risks, optimize resource allocation, and refine strategic partnerships before the university opens at scale.

Codesign Process: Building a Collaborative and Adaptive Institution

Another effective strategy is a structured codesign phase, where collaboration with faculty, students, and external stakeholders helps shape the institution's educational and operational models.[21] This process fosters a student-centered learning environment, promoting innovation and adaptability in response to emerging trends in intelligence, education, and practice. However, successful codesign requires a well-defined governance structure, ensuring that decision-making remains clear, consistent, and aligned with institutional goals. Without a structured approach, the institution risks developing an undefined or fragmented academic culture, which could undermine long-term credibility and effectiveness.[22]

Phased Launch: Scaling Up with Strategic Precision

A phased launch offers strategic advantages by delaying full-scale operations until key institutional elements are fully optimized. A gradual rollout allows the university to identify gaps in its business model, refine its approach, and secure additional funding before committing to full-scale academic operations. Additionally, staggered program implementation enables targeted faculty recruitment, ensuring that the institution attracts elite educators, intelligence practitioners, and thought leaders who can bring the expertise needed to guide its academic mission. This approach also provides time for the Mega-University to solidify industry and government partnerships, enhancing its reputation before fully expanding.

Establishing a Strong Institutional Launch

An intelligence-focused Mega-University's founding needs to be managed carefully to establish it as a prestigious establishment that strikes a balance between academic brilliance and real-world, applied learning. This phase will lay the groundwork for long-term success by prioritizing strategic planning, a methodical incubation process, and solid collaborations with the government and industry.[23]

PILLAR 4: RECRUITING THE FACULTY

Recruiting top-tier faculty is a critical component of the build-and-launch phase for any new university, particularly one focused on intelligence studies.[24] At the U.S. National Intelligence University (NIU), faculty members play a crucial role in shaping institutional culture, driving research excellence, and delivering high-quality education that meets the needs of the U.S. Intelligence Community and, to a lesser extent, its allied partners. Attracting world-class educators and practitioners requires a combination of strategic incentives, institutional vision, and competitive employment conditions that align with NIU's mission of national security service and interdisciplinary excellence.[25]

Competitive Career Paths for Intelligence Faculty

One of the key factors in faculty recruitment is the ability to offer attractive and sustainable career paths that balance academic scholarship with operational intelligence expertise.[26] Established universities often recruit faculty through the tenure-track system, which provides long-term job security and academic freedom. However, for NIU, which operates in a classified and specialized environment, tenure may not be the primary incentive for prospective and current faculty members.

Instead, alternative career pathways can be developed, such as long-term contracts, professional development opportunities in national security, government-sponsored research funding, sabbaticals within intelligence agencies, and structured transitions between academia and government service. Faculty members who perceive institutional stability, growth opportunities, and avenues for real-world impact are more likely to commit to NIU's long-term mission.

Security-Centered and Mission-Aligned Recruitment

The faculty recruitment process must be carefully structured to ensure alignment between faculty expertise and NIU's interdisciplinary and applied intelligence focus.[27] Traditional hiring models involve campus visits, research presentations, and structured interviews, but NIU may need to adopt specialized recruitment approaches suited to its unique classified learning environment.

For example, classified recruitment channels, security-vetted selection processes, and targeted faculty onboarding procedures may be necessary to ensure that faculty members can seamlessly integrate into the Intelligence Community's ecosystem. Additionally, NIU's classified setting may limit its ability to attract international faculty, particularly if intelligence studies at NIU diverge significantly from conventional higher education models. As a result, recruitment may need to prioritize professionals with security clearances, government service experience, or prior military and intelligence backgrounds to maintain the university's operational integrity.

Attracting Institutional Pioneers and Managing Faculty Growth

Start-up universities often benefit from the excitement of building a new institution. At NIU, early faculty members may see themselves as institutional pioneers, contributing to the redefinition of intelligence education and the strategic evolution of intelligence studies as an academic discipline. This sense of purpose can serve as a powerful recruiting tool, motivating faculty members to shape the university's long-term impact.

However, this also introduces challenges, particularly in blending faculty cohorts recruited at different stages of institutional growth. To preserve a cohesive academic culture, faculty recruitment tactics need to adapt if NIU broadens its scope, incorporates private-sector intelligence partnerships, or evolves toward a Mega-University model. These risks can be reduced and the faculty skills, research agendas, and national security goals can be aligned by establishing an early faculty governance model with defined academic and operational expectations.

Enhancing Regional and Global Appeal

A globally connected intelligence education institution must leverage regional and international expertise to enhance its institutional standing. NIU's unique position as the U.S. Intelligence Community's university gives it access to a global network of intelligence professionals, strategic partners, and industry specialists.

Institutions seeking to revolutionize intelligence education may attract expatriate faculty, senior intelligence analysts, and industry professionals who bring international perspectives and specialized operational knowledge.[28] These individuals can enhance NIU's credibility and effectiveness by incorporating global intelligence frameworks, comparative intelligence methodologies, and cross-national security perspectives into the curriculum. A globally diverse faculty ensures that NIU remains at the forefront of intelligence education innovation, equipping students with multidimensional analytical skills for an increasingly interconnected security environment.

Positioning the NIU as a Competitive Institution for Faculty Recruitment

Faculty recruitment must be approached as a competitive process in which NIU strategically positions itself as the leading institution for intelligence education. To attract and retain top-tier faculty, the university must provide compelling career prospects, a dynamic institutional culture, and meaningful opportunities for national service. Establishing structured career advancement pathways, offering competitive contracts, and integrating faculty members into the national security ecosystem will be critical in attracting the best talent. Additionally, fostering an institutional culture that prioritizes interdisciplinary research, applied intelligence education, and government-industry collaboration will ensure that NIU remains an attractive destination for leading scholars and intelligence professionals.

PILLAR 5: CURRICULUM AND ACCREDITATION

One of the greatest advantages of establishing a new intelligence education model is the ability to design an innovative curriculum from the ground up. Unlike traditional universities, which are often constrained by historical precedents and rigid disciplinary structures, a reimagined NIU can adopt a forward-thinking approach that integrates intelligence studies with business, technology, and experiential learning.[29] This opportunity would allow the NIU to move beyond conventional models and develop a curriculum that aligns with the demands of modern intelligence operations, equipping graduates with interdisciplinary expertise and practical skills.[30]

Building an Interdisciplinary Intelligence Curriculum

The core curriculum must prioritize interdisciplinary integration, ensuring that students develop competencies in intelligence analysis, strategic risk management, business leadership, and cybersecurity. Intelligence professionals must be able to navigate complex global security challenges, understand financial and corporate risk, and leverage technological advancements such as artificial intelligence (AI) and big data analytics. A well-designed intelligence curriculum should break free from the traditional focus on political science and history and instead emphasize a structured approach to intelligence as a strategic discipline that intersects with national security, international affairs, and business operations.[31]

To achieve this, NIU must incorporate courses that blend intelligence studies with emerging technologies, business strategy, and geopolitical analysis. These courses should address areas such as corporate espionage, cybersecurity risk assessment, intelligence-driven decision-making, and the application of AI in intelligence collection and analysis. By integrating technological fluency, financial literacy, and strategic leadership training, NIU can produce intelligence professionals who are equipped to operate effectively in both governmental and private-sector intelligence roles.[32]

Enhancing Learning Through Experiential Education

Experiential learning is essential to making intelligence education both relevant and impactful. Traditional lecture-based approaches must be supplemented with hands-on training, real-world case studies, simulations, internships, and fieldwork in collaboration with intelligence agencies and private-sector partners. These practical learning opportunities ensure that graduates do not just develop theoretical knowledge, but also gain applied experience in intelligence collection, analysis, and decision-making processes.

To implement this, NIU must establish state-of-the-art intelligence simulation labs, partnerships with classified intelligence agencies, and immersive training environments where students can engage in real-world intelligence exercises.[33] Joint projects with cybersecurity firms, financial intelligence units, and multinational corporations can further enrich the learning experience by exposing students to diverse intelligence challenges beyond traditional governmental roles. By embedding experiential learning elements into the curriculum, NIU can provide a unique and competitive educational experience that prepares students for intelligence careers across both public and private sectors.[34]

Establishing a Strategic Accreditation Framework

An essential part of ensuring NIU's credibility and long-term success is the accreditation process. In higher education, accreditation organizations act as gatekeepers by evaluating the caliber, legitimacy, and academic rigor of degree programs. However, creative institutions looking to modernize intelligence education face difficulties because traditional certification processes frequently favor traditional disciplines and established curricular structures.

NIU has to put forward the initiative of developing programs that not only satisfy accreditation requirements but also highlight the benefits of a contemporary approach to intelligence education to overcome this obstacle. This involves collaborating with industry stakeholders, interacting with accrediting bodies early on, and creating stringent evaluation procedures that confirm the efficacy of NIU's training programs and curriculum. NIU can guarantee that its programs continue to be both academically demanding and professionally relevant by including industry-aligned certifications, competency-based learning outcomes, and interdisciplinary coursework.[35]

Leveraging Accreditation to Enhance Institutional Prestige

Accreditation should not merely be viewed as a compliance exercise, but rather as an opportunity to position NIU as a global leader in intelligence education. By establishing industry-recognized certifications in intelligence analysis, cybersecurity, risk management, and financial intelligence, NIU can enhance its reputation and provide students with tangible credentials that improve their employability. These certifications, combined with a strong academic foundation, will allow graduates to seamlessly transition into roles within government agencies, multinational corporations, and global security firms.

Additionally, NIU must seek global accreditation partnerships to ensure that its degrees and certifications hold international value. Establishing alliances with security studies institutions, think tanks, and private-sector intelligence firms will reinforce NIU's role as a leading provider of intelligence education. This approach ensures that NIU's graduates remain competitive in the global intelligence workforce and that its educational model gains widespread academic and professional recognition.[36]

Balancing Innovation with Academic Credibility

The curriculum and accreditation strategy at NIU must strike a delicate balance between innovation and credibility. While NIU must challenge traditional academic structures to create a future-ready intelligence education model, it must also ensure that its degrees and certifications retain value in the broader educational and professional landscape.

PILLAR 6: CAMPUS AND VIRTUAL ENVIRONMENT

A university's physical campus has long been a key component of its reputation and identity. However, the function of conventional brick-and-mortar campuses is being reexamined as education becomes more digital. Some argue that since online learning has proven so flexible and affordable, physical campuses are no longer required. Others argue that face-to-face learning settings are still crucial for encouraging critical thinking, teamwork, and casual conversations that support a well-rounded education.[37] NIU, a forward-thinking university, must manage conflicting viewpoints to establish an ideal learning environment that strikes a balance between the advantages of both physical and virtual environments.

Designing a Campus for Collaboration and Innovation

Community, multidisciplinary cooperation, and practical intelligence training are all enhanced by a carefully designed physical campus. A university's physical design and layout have a direct impact on how teachers and students interact, facilitating chance meetings that encourage creativity and multidisciplinary problem-solving.

To encourage cross-disciplinary interaction and expose intelligence personnel to a range of viewpoints from business, technology, and security studies, a physical NIU campus needs to be redesigned. For students and professors to effectively collaborate on intelligence problem-solving, common areas, research laboratories, and classified facilities should be organized to support both structured learning and unplanned conversations.

Furthermore, a real campus can function as a safe setting for training in classified intelligence. In-person instruction is required for some components of intelligence education, including simulations, secret research, and experiential training in safe settings. Through highly specialized, experiential learning that cannot be duplicated online, a well-designed physical NIU campus may serve as a center for secure intelligence education.

Expanding Access Through Virtual and Hybrid Learning

A real campus encourages community and collaboration, while virtual learning provides unmatched cost-effectiveness, scalability, and accessibility. Online classrooms, digital platforms, and AI-powered learning tools allow NIU to extend its reach beyond geographical constraints, ensuring that intelligence professionals worldwide can access top-tier education.

Moreover, a hybrid paradigm can optimize flexibility while maintaining the advantages of in-person connection by combining online courses with sporadic in-person residencies or regional learning hubs. This approach allows students to complete coursework remotely, while still experiencing the networking, mentorship, and hands-on training opportunities provided by on-site learning sessions.

Through AI-driven adaptive learning environments, real-time intelligence cooperation activities, and interactive digital simulations, NIU may further improve virtual intelligence education. By leveraging cutting-edge technology, NIU can expand its impact and ensure that intelligence professionals—regardless of location—receive rigorous, engaging, and career-relevant education.

Ensuring Security in Physical and Digital Spaces

Both the physical campus of NIU and the online learning environments are designed with security as a top priority. NIU must set in place extremely secure digital tools that permit open-source and classified learning without jeopardizing national security since intelligence education is a delicate subject.

To achieve this, NIU must invest in cutting-edge cybersecurity measures, including encrypted communication systems, restricted-access digital classrooms, and advanced authentication protocols for classified coursework. A secure virtual learning environment will also be necessary to guarantee that intelligence professionals, instructors, and students may collaborate on research projects, analyze data, and have private conversations without worrying about online threats.

For its physical campus, NIU must incorporate secure research labs, classified intelligence training spaces, and high-security operational centers that allow students to train in realistic intelligence environments. These secure spaces will be critical in preparing students for intelligence operations, where classified information and real-time decision-making are integral to their professional responsibilities.

Integrating Emerging Technologies in Intelligence Education

Institutions like NIU must lead their peers in incorporating cutting-edge technologies into their classrooms as hybrid education becomes more popular. AI-powered intelligence simulations, digital collaboration tools, and virtual reality (VR) can greatly improve both in-person and virtual learning environments.

For instance, AI-driven analytics tools can offer real-time intelligence scenario modeling, and virtual reality (VR)-based intelligence simulations can let students participate in immersive information-gathering activities. Additionally, by allowing students to collaborate in real time on intelligence challenges with experts and peers worldwide, secure digital collaboration platforms can help close the gap between professional intelligence practice and academic learning.

Establishing NIU as a Global Leader in Hybrid Intelligence Education

Looking ahead, the future of intelligence education will likely incorporate elements from both traditional and online models. NIU must take the lead in developing an intelligence education ecosystem that seamlessly integrates physical and virtual learning spaces to ensure accessibility, security, and academic excellence.

PILLAR 7: SHARED GOVERNANCE

Establishing a system of shared governance is essential for balancing institutional autonomy, academic freedom, and responsiveness to the evolving needs of intelligence education. NIU must navigate the complexities of governance by integrating the perspectives of faculty, administrative leaders, government stakeholders, and private-sector partners. A well-structured governance framework will ensure that decision-making processes remain transparent, adaptive, and aligned with NIU's mission to serve national security and global intelligence cooperation.

Rethinking Shared Governance for Intelligence Education

The traditional shared governance model in U.S. higher education has long been both a source of strength and an innovation challenge. Authority is typically distributed among faculty, administrators, and board members, with faculty often holding significant influence over curriculum and pedagogy. While this structure fortifies academic independence, it can also create institutional inertia, making it difficult to implement necessary reforms in response to national security priorities and intelligence challenges.

The NIU must develop a governance model that retains academic integrity while fostering agility in adapting to emerging threats, technological advancements, and intelligence workforce demands. The university must strike a balance between academic self-governance and external oversight, ensuring that faculty expertise shapes intelligence education while government and industry partnerships contribute to real-world relevance.

Navigating Institutional Culture and Decision-Making

Managing the interaction between official decision-making processes and the unofficial institutional culture that develops over time is one of the main issues in shared governance. Universities frequently have to balance the interests of private sector stakeholders looking for innovation and workforce preparedness, academic traditions-promoting academics, and national security imperatives-focused legislators.

If governance structures are too rigid, they risk stifling necessary reforms; if they are too flexible, they may undermine institutional stability and credibility. To ensure ongoing innovation and preserve academic credibility, NIU should adopt a hybrid strategy that permits strategic decision-making without undue bureaucracy.

Integrating Academic and Industry Collaboration

The NIU has to set in place a collaborative governance framework that unites stakeholders from government, business, and academia in order to address these governance issues. Advisory boards made up of business executives, legislators, and intelligence specialists can offer strategic direction, guaranteeing that research projects and curricula are in line with actual intelligence requirements.

Faculty governance organizations should be set up to support multidisciplinary cooperation, curriculum development flexibility, and responsiveness to new security risks. NIU will be able to uphold its dual commitment to academic achievement and national service by forming working groups that connect academic fields with intelligence community needs.

Balancing Research and Teaching Priorities

A critical aspect of governance at NIU is maintaining equilibrium between research and teaching priorities. Many traditional universities emphasize research as the primary metric of academic success, often at the expense of teaching excellence. However, NIU must uphold a dual focus, ensuring that faculty contributions to intelligence education remain both intellectually rigorous and practically relevant.

This requires a faculty evaluation system that recognizes contributions to applied intelligence research, experiential learning initiatives, and national security service. Performance metrics should reward faculty engagement in real-world intelligence problems, rather than relying solely on traditional academic publishing models.

Institutional Growth and Leadership Continuity

As NIU evolves, it must also be prepared to address governance challenges associated with institutional growth and leadership transitions. Many start-up universities have encountered difficulties when early visionary leaders step aside, leading to shifts in institutional priorities and internal conflicts over governance structures.[38]

To mitigate these risks, NIU should establish clear policies for leadership succession, institutional mission continuity, and the long-term role of founding members in shaping its trajectory. Strategic leadership planning must ensure that NIU remains mission-driven, resilient to political and organizational shifts, and continuously forward-looking in its governance approach.

Establishing a Governance Model that Balances Stability and Innovation

Innovation and institutional stability must be balanced in NIU's governance approach. NIU could establish a governance framework that supports its mission as the leading intelligence education institution by encouraging cooperation between academia, government, and industry, guaranteeing open decision-making, and upholding a dedication to academic excellence and national security service.

CONCLUSION

The transformation of intelligence studies into a dynamic, interdisciplinary, and globally connected discipline is no longer optional; it is essential. The security challenges of the 21st century demand intelligence professionals who transcend traditional academic silos, integrating expertise from business administration, cybersecurity, emerging technologies, political science, strategic leadership, and international relations. By redefining intelligence education, NIU can position itself at the forefront of intelligence innovation, serving national security and private-sector intelligence functions with unparalleled academic and professional rigor.

By expanding NIU into a Mega-University, intelligence studies can leverage cutting-edge educational models, ensuring that students and faculty engage with real-world intelligence challenges through experiential learning, digital innovation, and global partnerships. The Mega-University model facilitates a structured, future-ready approach, balancing academic excellence with practical intelligence training. Through strategic governance, financial sustainability, and interdisciplinary collaboration, NIU can establish itself as the premier institution for intelligence education, fostering a new generation of intelligence professionals capable of navigating complex geopolitical landscapes, emerging security threats, and intelligence-driven decision-making.

Eventually, intelligence education must evolve to embrace both traditional and open intelligence methodologies, ensuring accessibility while maintaining national security imperatives. A hybrid campus and digital learning model will enhance accessibility, security, and collaboration, ensuring that intelligence professionals worldwide benefit from world-class education, research, and training.

The success of this transformation hinges on a governance model that balances institutional stability with innovation, securing long-term academic prestige, financial sustainability, and global influence. NIU's transition into a Mega-University will elevate intelligence studies as a prestigious and indispensable field and serve national security, public service, and international intelligence cooperation in a period of unprecedented challenges and opportunities.

NOTES

[1] Stephen Marrin, "Improving Intelligence Studies as an Academic Discipline," Intelligence and National Security, vol. 31, no. 2, 22 (October 2014): 266–279.
[2] Jules Gaspard and Giangiuseppe Pili, "Root Values and Root Skills: A New Model for Intelligence Education," Intelligence & National Security (September 2024): 1–19.
[3] Peter de Werd, et al. "Special Forum on Intelligence and Theory," Intelligence and National Security (March 2024): 1–24, https://doi.org/10.1080/02684527.2024.2324534.
[4] Nicholas Eberstadt and Evan Abramsky, "America's Education Crisis Is a National Security Threat," Foreign Affairs (September 20, 2022).
[5] Bryan Penprase and Noah Pickus, The New Global Universities (Princeton, NJ: Princeton University Press, 2024).
[6] Corbin M. Campbell, et al. "Prestige or Education: College Teaching and Rigor of Courses in Prestigious and Non-Prestigious Institutions in the U.S." Higher Education, vol. 77, no. 4 (July 2018): 717–38, https://doi.org/10.1007/s10734-018-0297-3.
[7] Orhan Dursun and Cigdem Altin Gumussoy, "The Effects of Quality of Services and Emotional Appeal on University Reputation: Stakeholders' View," Quality Assurance in Education, vol. 29, no. 2/3 (June 2021): 166–82, https://doi.org/10.1108/qae-08-2020-0104.
[8] John Sexton, "Building the First Global Network University." In Armand Heijnen and Rob van der Vaart, Places of Engagement: Reflections on Higher Education in 2040- A Global Approach (Amsterdam: Amsterdam University Press, 2018), https://doi.org/10.2307/j.ctvfjd0xs (JSTOR).
[9] Caroin Nast, et al. "Sourcing Insights Elsewhere: The Positive Influence of Academic Engagement on Scientific Impact," Technovation, vol. 139, Elsevier, (November 2024): 103112, https://doi.org/10.1016/j.technovation.2024.103112.
[10] Adam Williams, et al. "Scholars' Influence on Their Institutions: Reputation, Prestige, and Rankingsm" Teaching Public Administration, vol. 38, no. 3 (February 2020): 233–56, https://doi.org/10.1177/0144739420901741.

[11] Audrey Williams, "How One College Reinvented Its Hiring Process to Better Test for 'Fit,'" The Chronicle of Higher Education (July 6, 2018), www.chronicle.com/article/how-one-college-reinvented-its-hiring-process-to-better-test-for-fit/, accessed April 11, 2024.
[12] Samatha Newbery and Christian Kaunert, "Critical Intelligence Studies: A New Framework for Analysis," Intelligence and National Security, 38(5) (2023): 780–798, https://doi.org/10.1080/02684527.2023.2178163.
[13] Stephan Von Delft, et al. "Leveraging Global Sources of Knowledge for Business Model Innovation," Long Range Planning, vol. 52, no. 5 (October 2019): 101848, https://doi.org/10.1016/j.lrp.2018.08.003.
[14] Stephen Marrin, "Understanding and Improving Intelligence Analysis by Learning from Other Disciplines," Intelligence and National Security, 32(5) (2017): 539–547. https://doi.org/10.1080/02684527.2017.1310913.
[15] Abdulrahman Obaid Al-Youbi, et al., ed.. International Experience in Developing the Financial Resources of Universities (Springer International Publishing, 2021), https://doi.org/10.1007/978-3-030-78893-3.
[16] Vicki Chandler, et al. A New Look at Majors and Concentrations (Boston, MA: The MIT Press, 2017), 121–34, https://doi.org/10.7551/mitpress/11142.003.0012, accessed April 11, 2024.
[17] Team, Editorial, "Financial Models for Universities Must Go beyond Student Numbers - Higher Education Digest," Higher Education Digest, February 4, 2025, www.highereducationdigest.com/financial-models-for-universities-must-go-beyond-student-numbers/, accessed April 11, 2024.
[18] Jan Lynn-Matern, "How to Build a Unicorn by Partnering with Universities to Diversify Their Revenue Streams (Part 2)," Medium, Emerge Insights, January 26, 2021, https://medium.com/emerge-edtech-insights/how-to-build-a-unicorn-by-partnering-with-universities-to-diversify-their-revenue-streams-part-2-6b3215f26d55, accessed April 11, 2024.
[19] Maribel Guerrero and Marina Dabić, Re-Building University Capabilities, Applied Innovation and Technology Management Series (Springer International Publishing, 2023), https://doi.org/10.1007/978-3-031-31667-8.
[20] Dacin, M. Tina, et al. "Institutional Theory and Institutional Change: Introduction to the Special Research Forum," The Academy of Management Journal, vol. 45, no. 1 (February 2002): 43, https://doi.org/10.2307/3069284.
[21] Lawrence Susskind, et al. "A Critical Assessment of Collaborative Adaptive Management in Practice," Journal of Applied Ecology, vol. 49, no. 1, (October 2011): 47–51, https://doi.org/10.1111/j.1365-2664.2011.02070.x.
[22] Thomas Weimer, Bryon Williams, Robert Szaro, and Carl Shapiro, Adaptive Management: The U.S. Department of the Interior Technical Guide (Boston, MA: Massachusetts Institute of Technology, 2025), https://scienceimpact.mit.edu/adaptive-management-us-department-interior-technical-guide, accessed April 11, 2024.
[23] Harvey Luskin Molotch and Davide Ponzini, The New Arab Urban: Gulf Cities of Wealth, Ambition, and Distress (New York: New York University Press, 2019), 159.
[24] Liam Gearon, Education, Security and Intelligence Studies (London: Routledge, 2018).
[25] William C. Spracher, "National Intelligence University: A Half Century Educating the next Generation of U.S. Intelligence Community Leaders," Intelligence and National Security, vol. 32, no. 2, (November 2016): 231–43, https://doi.org/10.1080/02684527.2016.1248316.
[26] Samantha Newberry and Christian Kaunert, "Critical Intelligence Studies: A New Framework for Analysis," Intelligence and National Security, vol. 38, no. 5 (February 2023): 780–98, https://doi.org/10.1080/02684527.2023.2178163.
[27] Malin Henningsson and Lars Geschwind, "Recruitment of Academic Staff: An Institutional Logics Perspective," Higher Education Quarterly (November 2021), https://doi.org/10.1111/hequ.12367, accessed April 11, 2024.
[28] Larry E. Greiner, "Evolution and Revolution as Organizations Grow," Harvard Business Review (1998), hbr.org/1998/05/evolution-and-revolution-as-organizations-grow, accessed April 11, 2024.
[29] Boston Consulting Group, "Learning Is Reimagined at Fulbright University in Vietnam." BCG, 2022, https://www.bcg.com/en-us/industries/education/reimagining-learning-experience-fulbright-university-vietnam, accessed April 11, 2024.
[30] Liam Gearon, Education, Security and Intelligence Studies (London: Routledge, 2018).
[31] Christopher Sheehy, "Reforming the U.S. Intelligence Community: Successes, Failures and the Best Path Forward," JMU Scholarly Commons, Senior Honors Projects (2014), https://commons.lib.jmu.edu/cgi/viewcontent.cgi?article=1009&context=honors201019, accessed 11 April 2024.
[32] Edgar H. Schein, Organizational Culture and Leadership, 5th ed. (Hoboken, NJ: Wiley, 2016), 56.
[33] William J. Lahneman and Rubén Arcos, "Experiencing the Art of Intelligence: Using Simulations/Gaming for Teaching Intelligence and Developing Analysis and Production Skills," Intelligence and National Security (June 2017): 1–14, https://doi.org/10.1080/02684527.2017.1328851.
[34] Rebecca L. Frerichs and Stephen Di Rienzo, "Establishing a Framework for Intelligence Education and Training," ResearchGate (July 2011).
[35] William C. Spracher, "National Intelligence University: A Half Century Educating the next Generation of U.S. Intelligence Community Leaders," Intelligence and National Security, vol. 32, no. 2 (November 2016): 231–43, https://doi.org/10.1080/02684527.2016.1248316.
[36] Ibid.
[37] Bunmi Isaiah Omodan, "Redefining University Infrastructure for the 21st Century: An Interplay between Physical Assets and Digital Evolution," Journal of Infrastructure, Policy and Development, vol. 8, no. 4, (February 2024), https://doi.org/10.24294/jipd.v8i4.3468.
[38] KinHo Chan and Pamela Stacey, "Desirable Difficulties and Student-Faculty Partnership," Innovations in Education and Teaching International, (December 2020): 1–11, https://doi.org/10.1080/14703297.2020.1861964, accessed April 11, 2024.

Dr. Anthony Ioannidis is an Assistant Professor of Management at the Athens University of Economics and Business, Greece. He holds a B.S. from the University of Athens, Greece, and an M.B.A., an M.Phil., and a Ph.D. from Baruch College, The City University of New York. He also possesses working experience as a management consultant with leading consultancy firms in the US and Greece, in the areas Telecommunications, Media and Technology. His current research interests include intelligence education and practice, strategy formation, organizational design, public-private partnerships, and technology entrepreneurship.

Mr. Anastasios-NikolaosKanellopoulos is currently a PhD candidate at the Athens University of Economics and Business, and holds a master's in international relations, Strategy and Security from the University of Neapolis Pafos in Cyprus, a bachelor's in business administration from the Athens University of Economics and Business, and a bachelor's in public security from Hellenic Police Academy.

Assessing Future Trajectories in the Pacific Islands through Scenario Development: The Influence of Chinese Aid and Western Economic Engagement

by **Dr. M. John Bustria**

INTRODUCTION

Political leaders frequently engage in retrospective inquiry when confronted with unforeseen crises, complex strategic dilemmas, or emergent systemic/collective phenomena. These reflective inquiries often revolve around fundamental fact-finding questions: *How did this go undetected? Why was it not foreseen? What caused it to be overlooked? Where did the earliest warning signs appear? Who did it take by surprise?* Most critically, *who failed to recognize the impending threat?* These concerns indicate a broader challenge within policy analysis—the inherent constraints of predictive models and forecasting methodologies in capturing the complexities of dynamic, interconnected systems and multifaceted issues.

Future planning is inherently uncertain because predictive frameworks often struggle to fully encapsulate the evolving nature of political, economic, and social events. Every so often, they fail to reflect the objective and subjective dimensions of the object of reality or research accurately. This results in a gap between the limitations of what can be known about the future and the necessity of preparing for it.[1] Addressing this gap requires a more nuanced approach that integrates adaptive planning, scenario analysis, and rigorous methodology, which will enable policymakers to navigate uncertainty with greater flexibility.

As global power dynamics continue to evolve within an increasingly complex security environment, geopolitical rivalry—particularly the strategic and adversarial competition between the West and China—has become increasingly prominent across various regions, including the Pacific Islands. This geopolitical space, often described by the West as "patch," "backyard," or "near abroad,"[2] has emerged as a contested space where diplomatic, information, military, and economic interests shape regional governance and strategic alignments.

Within this context, Alternative Futures Analysis (AFA)—also referred to as futures research, futures studies, scenario analysis, or scenario development[3]—provides a structured methodological framework through which scholars and policymakers can examine potential trajectories and anticipate emergent dynamics within the evolving geopolitical landscape. Furthermore, while traditional geopolitical forecasting often relies on linear extrapolation of existing political, economic, or social trends, patterns, and developments, alternative futures research acknowledges the inherent complexity and uncertainty of global power shifts. This approach recognizes that multiple plausible trajectories may emerge rather than a single, predetermined outcome.[4]

Despite the growing recognition of scenario planning as a critical tool in creating insights, gaps remain in understanding how different methodologies influence policymaking processes.[5] By utilizing AFA as a structured analytic framework, this study aims to assess plausible trajectories of Western-Chinese geopolitical competition in the Pacific region, with a focus on their aid strategies. Through this lens, the research explores the broader implications of such strategic engagements for the governance, economic development, and stability of Pacific Island countries (PICs). This study applies AFA to the ongoing West-China aid competition in the Pacific region, examining how various scenarios—such as strategic accommodation, continued competition, regional fragmentation, or unforeseen disruption[6]—might influence the Pacific region's political, economic, and security landscape.

The article first establishes the theoretical foundations of AFA as a structured analytic technique, followed by a detailed discussion of its methodology. It then presents a structured scenario analysis of the Pacific Islands region, examining potential futures based on prevailing dynamics and emerging trends, such as China's aid expansion. After further discussion on the scenarios' generation, the conclusion assesses strategic implications for policymakers and regional actors.

AFA AS A STRUCTURED ANALYTIC TECHNIQUE

Structured Analytic Techniques (SATs) are systematic methodologies used in intelligence analysis to deconstruct and simplify complex problems by dividing them into manageable components. Their main goal is to improve the analytical process by increasing transparency, ensuring a systematic approach, and minimizing the influence of cognitive biases.[7] By methodically breaking down intricate issues, SATs facilitate more structured assessments. This streamlining of analysis fosters clarity, consistency, and objectivity throughout the decision-making process.

The techniques are grouped by their purpose. Diagnostic techniques focus on increasing transparency in analytic arguments, underlying assumptions, and intelligence gaps. Contrarian techniques explicitly challenge prevailing thinking. Imaginative thinking techniques foster new insights, explore diverse perspectives, and generate alternative outcomes by expanding the scope of possibilities.[8] While many of these techniques serve multiple purposes, analysts should prioritize selecting the methodology that most effectively achieves their specific objectives. Choosing the right tool ensures a more focused and efficient analytic process tailored to their needs.[9] It also promotes methodological rigor and ensures a systematic approach to complex decision-making.

This study employs AFA as an imaginative thinking technique, leveraging its systematic approach to construct and assess multiple potential future scenarios. By evaluating possible trajectories and their implications, AFA enables analysts to anticipate diverse possibilities or array of outcomes, such as a range of possible futures, promoting a mindset of adaptability and readiness to navigate uncertainties and unexpected changes.[10] Furthermore, AFA serves as an analytical framework for scrutinizing assumptions and considering alternative hypotheses, enhancing the robustness of analytical reports to help shape policymakers' thinking.[11]

While AFA serves as the analytic frame for this study in discussing the selected topic, within the structure of that frame includes a diagnostic technique called Indicators or Signposts of Change. This technique, which AFA explicates as one of its elements, shows that focusing on critical indicators within indications and warnings analysis improves analysts' ability to foresee and address emerging threats or developments. This method involves identifying key indicators that, when observed, can act as warnings or early signals of significant events or shifts within a given scenario.[12] Analysts can proactively interpret trends by analyzing these indicators, strengthening their ability to minimize risks and respond to shifting situations.

AFA AS A RESEARCH METHODOLOGY

One SAT that can reshape a state's engagement with a dominant material force is scenario analysis, which provides a framework for envisioning potential future trajectories. Scenario analysis facilitates reflection on multiple plausible futures by systematically constructing scenarios, ranging from the most likely to the least probable and most disruptive.[13] This approach enhances awareness of the fundamental forces and critical variables that influence, for instance, geopolitical shifts.

In complex, ambiguous, and rapidly evolving decision-making environments, the future is inherently unpredictable. Some events may carry low probability but have high-impact implications, necessitating structured insight. Leading researchers employ scenario analysis to "identify the driving forces that may determine future outcomes and monitor those forces as they interact to become the future."[14] Scenarios function as essential analytical instruments for doing this identification and monitoring of driving forces, offering credible, compelling narratives about how the future might be revealed. Moreover, scenarios can serve as interventions that alter or transform geopolitical relations, exemplified by the participation of recipient states in the donor's strategic economic and foreign policy initiatives.

AFA encompasses a body of techniques designed to generate scenarios that explore alternative or possible futures in response to a specific research question. These scenarios serve as projected hypothetical constructs, derived from a systematic analysis of current and historical information and knowledge.[15] Unlike traditional forecasting models that focus on a singular projected future, AFA emphasizes the construction of multiple future scenarios to offer the fullest conceivable range of plausible possibilities.[16] More than two dozen techniques exist for conducting AFA, employing both qualitative and quantitative research methodologies. Regardless of the approach, these techniques provide decision-makers with insights into a spectrum of potential futures,[17] equipping them to navigate uncertainty with greater adaptability. Because AFA

assesses the time horizon for all possible futures, it can challenge current assumptions, identify consequential new or emerging trends, or provide a systematic, novel way to approach a specific problem.[18]

Scenarios generated through AFA offer detailed, plausible narratives about how a future might unfold—even if that future is improbable.[19] In futures research, it is essential to distinguish between a "future" as a projected endpoint in time and a "scenario" as the pathway through which that future could materialize.[20] Within the AFA framework, scenarios hold greater significance than singular future predictions, as they provide decision-makers with alternative analysis and actionable insights rather than deterministic forecasts.

Scenarios serve as indicators or "signposts" that show emerging trends, enabling policymakers to recognize the development of a particular future. This approach creates opportunities to redirect a projected trajectory or guide efforts toward a more favorable outcome. Additionally, scenarios function as early warning mechanisms, particularly in identifying low-probability, high-impact "wild card" events. By incorporating a spectrum of possible futures—including unforeseen contingencies—AFA equips analysts with a systematic framework for evaluating uncertainty and informing strategic decision-making in complex environments.[21]

Although the AFA technique is grounded in current and historical information, it requires an imaginative component to generate informed predictions of both probable and improbable futures.[22] The imaginative capacity of AFA enables researchers to conceptualize even the most unlikely scenarios, considering how they might unfold based on existing knowledge, without necessitating factual confirmation for future projections. As an illustration, to conduct futures research effectively, analysts must think beyond conventional paradigms, exploring innovative possibilities through structured scenario development. For instance, imagining a low-probability, high-impact "wild card" scenario does not rely on empirical verification, as few concrete indicators may suggest its occurrence. Instead, futures research leverages subject matter expertise and analytical judgment to construct plausible narratives, providing a structured framework for considering emergent possibilities within the realm of uncertainty.[23]

Turning to the intellectual landscape of AFA, this methodology is often described under various terms, including futures studies, futures research, scenarios, scenario planning, or future scenarios—all of which fall within the broader domain of foresight.[24] The concept of "futures studies" gained prominence in the 1990s, notably through Richard A. Slaughter's seminal work, *The Foresight Principle: Cultural Recovery in the 21st Century*. Slaughter redefined foresight beyond its conventional meaning of "seeing before," positioning it as a strategic planning tool applicable to individuals, communities, and societies.[25]

Expanding on the concept of strategic foresight, Richard Slaughter posited that this field constitutes an academic discipline aimed at cultivating anticipatory thinking to enhance decision-making processes.[26] He added that a core component of strategic foresight involves the formulation of alternative futures—or scenarios—which serve as structured projections to assist organizations and states in planning for and advancing toward their preferred future. Slaughter further argued that while organizations may converge on a particular vision of the future, they remain incapable of precisely predicting probabilities. He concluded that futures studies do not seek to forecast a singular definitive future but instead construct multiple plausible and probable scenarios to account for uncertainty.[27]

Joseph Bezold agreed with Slaughter's claim, stating that this methodological approach enables decision-makers to navigate complexity by conceptualizing a range of potential futures. He noted that organizations and states can develop adaptive strategies that enhance resilience and preparedness for unanticipated developments.[28] Based on Slaughter's redefinition of foresight, Eva Hideg suggested that strategic thought and foresight lend themselves to most types of analysis, seeking to help users consider relevant data around a topic while driving toward a useful outcome.[29] These studies and more indicate the rigor and impact AFA brings to policies.

As AFA has evolved into an established analytical framework, it calls upon researchers to assess a subject by identifying two independent variables or characteristics that influence the plurality of potential futures. This aligns with Schwartz's assertion that "the future is plural,"[30] emphasizing the multidimensional nature of scenario planning. Building upon these principles, researchers have developed a 2×2 matrix, derived from the Global Business Network's framework, which systematically organizes variables along maximum and minimum values. This construct generates four distinct future scenarios: A-Max vs. B-Max, A-Max vs. B-Min, A-Min vs. B-Max, and

A-Min vs. B-Min,[31] thereby offering a structured approach to exploring alternative trajectories.

The added value of AFA lies in its capacity to equip policymakers with a structured framework for anticipating and navigating diverse future trajectories. Rather than striving to predict a single most likely outcome, an approach that often proves inaccurate, scenario-based analysis establishes a contextual foundation for exploring multiple plausible futures. Constructing scenarios helps analysts identify the key forces and factors most likely to shape how a situation evolves.[32] Effective methodologies for overcoming analytical stagnation include defining a period for the estimate (such as five or ten years) that one cannot easily extrapolate from current events.[33] In contrast to Multiple Scenarios Generation, AFA differs primarily in the number of scenarios analyzed. AFA operates within a structured constraint of two driving forces, each conceptualized as a spectrum with two extremes, resulting in four probable scenarios. Conversely, Multiple Scenarios Generation imposes no predefined limitations aside from those dictated by time constraints and analytical complexity,[34] allowing for a broader exploration of potential futures.

The next section's findings and analysis on West-China rivalry through the expansion of Chinese aid in PICs employs the 2×2 matrix framework, a structured analytical tool utilized when two primary driving forces can be identified as determinants shaping the outcome of a given issue.[35] This method systematically categorizes four distinct potential scenarios, each representing the extreme conditions associated with the two major drivers. By spanning the logical possibilities inherent in the interaction between these driving forces, the 2×2 matrix facilitates the generation of scenarios that analysts might otherwise overlook.[36] This structured approach enables a more nuanced examination of possible trajectories within the evolving geopolitical landscape. The four scenarios are mapped within a 2×2 matrix, where both variables are positioned along the X and Y axes.[37]

GROWING PRC AID, INFLUENCE IN THE PACIFIC AMID REFOCUSED WESTERN AID

The geopolitical landscape of the Pacific Islands region has undergone significant transformation, marked by a notable increase in Chinese aid alongside a relative decline in Western assistance. Beijing's expanding aid initiatives serve as a key instrument in its broader strategy to consolidate regional influence, positioning China as an increasingly dominant actor in Pacific affairs. This evolving dynamic raises critical questions regarding the future of Western engagement and its capacity to maintain strategic footholds in the region. Given China's growing presence and the broader implications for regional stability, Western policymakers face the pressing challenge of counterbalancing Beijing's influence. Addressing this geopolitical shift necessitates the development of targeted policy initiatives and strategic interventions,[38] enabling proactive measures that can shape future regional outcomes and ensure sustained engagement with the island states.

On November 19, 2024, the Lowy Institute's Pacific Aid Map revealed a significant post-pandemic surge in Chinese aid to the Pacific Islands, coinciding with a decline in Western assistance, as global priorities shifted toward Ukraine.[39] This development resulted in China surpassing the United States to become the region's second-largest bilateral donor,[40] marking a strategic recalibration of Beijing's aid approach to target key PICs and consolidate regional influence.[41] Given these geopolitical shifts, the AFA framework serves as a valuable methodological tool for examining potential future trajectories and informing strategic decision-making. By applying AFA, analysts can assess the long-term implications of China's expanding aid initiatives and explore policy responses that may shape regional stability and Western and international engagement in the Pacific Islands.

AFA employs scenario-based methodologies to examine multiple possible futures, generating plausible trajectories that inform strategic decision-making. Its primary analytical value lies in the construction of scenarios, which serve as actionable signposts for policymakers, enabling them to anticipate trends and shape future developments toward preferred outcomes.[42]

As mentioned, AFA requires researchers to identify two independent variables or key driving forces that determine the plurality of future possibilities.[43] Given the current geopolitical and regional power dynamics, two critical factors—each with a distinct range—can be utilized to construct scenarios: Availability of Chinese aid, measured by an increase or decrease in Chinese infrastructure investments; and Level of Western economic engagement, defined by either a higher or lower degree of involvement. By mapping these driving forces across a 2×2 matrix, analysts generate four distinct scenarios, each representing the intersection

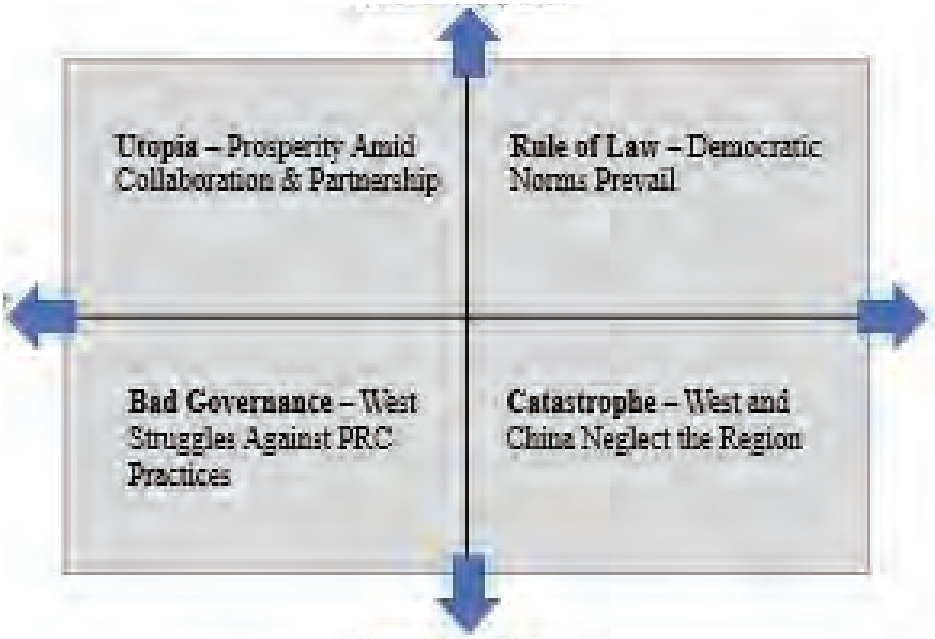


FIGURE 1. PACIFIC ISLAND COUNTRIES' MATRIX SCENARIO

of these variables. This structured approach assists in a deeper understanding of potential geopolitical trajectories, informing policy adaptation and strategic anticipation within the Pacific Islands region.

The following discussion will examine each quadrant in detail, incorporating narrative analyses, key indicators, and policy implications for each designated scenario.

FUTURE SCENARIO 1: UTOPIA (PROSPERITY AMID COLLABORATION AND PARTNERSHIPS)

The Story. In this scenario, China and the West engage in sustained collaboration and strategic partnerships, prioritizing coordinated resource allocation to advance regional development in the Pacific. Through mutual consultation, both actors work to harmonize aid strategies, ensuring that investments are aligned with the specific economic and infrastructural needs of the region. As a result, PICs experience economic prosperity, overcoming long-standing challenges related to limited human and natural resources, restricted access to raw materials, and constraints in broader material resource development.[44] This cooperative dynamic fosters regional stability, inclusive growth, and strengthened governance structures, positioning PICs as a key beneficiary of balanced global engagement rather than as a contested geopolitical arena.

Foreign aid has often been characterized as an instrument of ideological subjugation, reinforcing asymmetrical power structures that produce social relations of domination. This perspective underscores the complex interplay between economic instruments of national power and broader foreign relations practices,[45] illustrating how aid can serve as a mechanism for influence rather than genuine development support. However, within this scenario, the collaborative engagement between China and the West mitigates these concerns. In this idealized model, both actors recognize PICs as equal partners, ensuring that aid initiatives do not perpetuate dominance, inequality, or control. Through joint development projects, leaders from both ideological spheres uphold sovereignty and agency, affording Pacific leaders an opportunity for meaningful participation and equal footing in strategic engagements. This equitable dynamic fosters regional empowerment, reinforcing governance autonomy and sustainable development across PICs.

Indicators. Several observable indicators suggest the emergence of this scenario, including: signed collaborative project agreements between China and the West; trilateral cooperation among China, the West, and PICs; non-restriction on both sides giving assistance to PICs; buildup of staff in both group's companies in the Pacific region (e.g., rising visa approvals and expanded institutional presence); growth in institutional capacity-building initiatives; initiation of co-funding on infrastructure developments, among other indicators.

These indicators collectively signal a heightened level of Western regional engagement, alongside China's growing aid initiatives, reinforcing Western and Chinese bilateral commitments to fostering economic development and stability in the PICs. Their visibility stresses the tangible efforts by both actors to move beyond geopolitical competition and toward collaborative partnerships that prioritize regional growth.

Policy Implications. The ideal setup in this scenario would allow China and the West to redirect their programs and policy efforts elsewhere and toward broader global concerns. However, this cooperative framework remains inherently fragile because realist theory asserts that states prioritize power accumulation as a means of self-preservation within an anarchic international system.[46] Should regressive conditions emerge in the Pacific Islands region, the West's primary concern would likely shift toward violence prevention and stability restoration, necessitating cooperation with China to maintain regional order and national unity.

Given the potential for escalating crises, regional governments might require external assistance out of utilitarian necessity, prompting both Western and Chinese policy initiatives to focus on preventing governmental collapse. For Pacific governments, survival would remain paramount. Military forces from Fiji, Papua New Guinea, and Tonga, alongside paramilitary units in the Solomon Islands and Vanuatu, would likely play a pivotal role in responding to domestic instability. However, these forces could resort to violent suppression to counter perceived threats to state authority, raising legitimacy concerns within the international community.

In the event of widespread degradation of civil liberties and economic activity, China and the West may adopt increasingly coercive measures to maintain political stability and counter opportunistic actors seeking to exploit the crisis. Regime survival would take precedence as a guiding policy objective, reinforcing the imperative for strategic coordination between global powers in the Pacific Islands region.

FUTURE SCENARIO 2: ORDER (DEMOCRATIC NORMS AND WEST'S INTERESTS PREVAIL)

The Story. In this scenario, the West pursues strategic economic objectives in the Pacific Islands region through democratic principles of openness and transparency. Western engagement is characterized by accountability and oversight, ensuring that aid allocations and investments are traceable, regulated, and effectively used for sustainable development. This liberal, democratic practice fosters an environment where Western influence shapes the socioeconomic policies of PICs. As aid recipients, these states experience a shift in governance behavior, adopting institutional reforms that align with Western standards of economic management and fiscal responsibility.

Although Western nations exert significant direction over regional economic structures, aid and resources remain accessible, flowing freely to PICs under a system that prioritizes transparency, proper accounting, and effective allocation. This structured engagement strengthens regional stability, reinforcing governance mechanisms that support democratic norms and economic development in the Pacific Islands.

In this scenario, PICs experience sustained economic growth, which is independently reported by the media, reinforcing transparency and accountability. The presence of legal guarantees for free expression enables citizens to openly voice their perspectives on the impacts of Western and Chinese aid, fostering public discourse and civic engagement. Additionally, this scenario is characterized by robust government regulations, ensuring effective fiscal management and enhanced revenue generation. These financial windfalls contribute directly to addressing persistent socioeconomic challenges, including unemployment and economic inequality.

Indicators. Indicators of this scenario emerging include the following: increase in transparency and accountability requirements for new projects; lack of protest on regulatory oversights for infrastructure and development projects; sustained presence of civil society organizations; increase in legal frameworks and enforcement mechanisms; a rise in transparent reporting and critical analyses of government policies and foreign aid projects; and equitable distribution of economic opportunities, among other things. This scenario fosters an increase in economic output, largely attributed to reduced corruption, which often impedes development. The adoption of good governance norms—practiced in liberal, democratic societies—becomes a defining characteristic of Western-led economic engagement in PICs, ensuring sustainable growth and financial stability.

Policy Implications. While this scenario may appear uneventful, it presents strategic advantages for policymakers by offering valuable time for deeper engagement and long-term positioning in the Pacific Islands region. The West can leverage this stability to gain a nuanced understanding of in-country dynamics, strengthening relationships across the political spectrum—from government figures to opposition leaders. Western messaging and diplomatic outreach

would be tailored to different audiences, ensuring targeted engagement that fosters continued support among Pacific Island elites for democratic governance norms. Sustained political and economic involvement is crucial in reinforcing Western values and institutional frameworks, preventing disengagement and diminishing geopolitical influence.

Beyond economic development, this scenario provides an opportunity for the West to focus on strategic objectives, including countering China's expanding regional influence. The extended period of stability allows for calibrated decision-making, giving Western policymakers space to develop forward-looking strategies that shape the future trajectory of geopolitical competition in the Pacific Islands region.

Regarding climate change as an existential threat to PICs, the West could create more climate-resilient support infrastructure projects to gain influence with PICs to counter China's climate leadership. The West needs to provide aid and investment in climate change to help Pacific governments mitigate its effects and improve PICs' quality of governance. Exposure to rules-based practices and transparency requirements for aid could provide reform incentives for status-conscious island leaders. This exposure would lead some island leaders to consider aid from the West, a preference that might give them a chance to show PICs that Western governments remain committed to the region. Elsewhere, PICs have established anti-corruption laws and institutions to make leaders and officials more responsible.[47] These initiatives could increase accountability, prevent corruption, and extend the proper use of donor funds for climate change.

FUTURE SCENARIO 3: BAD GOVERNANCE (WEST STRUGGLES AGAINST PRC ECONOMIC DOMINANCE).

The Story. In this scenario, Western development partners withdraw or reduce engagement with PICs, leading to a diminished Western influence over local policymakers and officials. As Western aid declines, its ability to compete with China's expanding economic and sociopolitical presence weakens, allowing Beijing to consolidate its dominance across the region.

With fewer external constraints, some Pacific elites exploit this shift, engaging in corrupt practices to secure financial resources that maintain political loyalty and electoral support. The resulting governance environment reflects a continuation of entrenched corruption, as accountability mechanisms weaken in the absence of Western oversight and engagement.

China, having established itself as the principal economic actor in the region, asserts authoritarian practices in pursuit of its strategic interests. Despite Beijing's official stance of non-interference, its expanding economic footprint enables it to propagate an alternative governance model that dismisses democratic norms. As a result, Western values of transparency and accountability erode, replaced by a system prioritizing state-led economic control and political consolidation under China's influence.

Indicators. The emergence of this scenario is signaled by several observable trends, including: local acceptance of authoritarian models for economic growth; rise in corruption linked to infrastructure projects; protests from marginalized groups whose resources are exploited; lack of oversight in aid agreements; failed socioeconomic policy reforms; electoral losses for pro-West candidates; and continued dominance of "big-man" political leadership, among other things. This scenario underlines the erosion of democratic norms and the ascendancy of authoritarian governance, exacerbated by elite-driven corruption and organized criminal violence, factors that threaten political stability and societal cohesion in PICs.

Policy Implications. In this scenario, regional governments exhibit minimal behavioral change, continuing to operate inefficiently despite shifting geopolitical dynamics. Governance remains static, marked by low electoral participation as skepticism grows among the local populace regarding the fairness and legitimacy of political processes. Elite-dominated parties sustain their grip on power through unfree and unfair elections, leveraging Chinese assistance projects to maintain influence.

Meanwhile, natural resource flows remain unchecked, benefiting foreign buyers, particularly China, while PICs struggle to exercise economic autonomy. In response, the West faces mounting pressure to offer additional economic incentives tailored to the changing Pacific landscape. While the specifics of such incentives remain uncertain, any major economic policy restructuring would necessitate proactive Western engagement to prevent unsustainable dependencies on Chinese financial support.

Without strategic intervention, PICs risk following the trajectory of several African nations that have endured crushing debt burdens, escalating Chinese influence, and significant loss of sovereignty to Chinese business interests.[48] To mitigate this outcome, the West must invest in strengthening PICs' civil society, fostering democratic norms, civil liberties, and free enterprise as counterweights to Beijing's economic and political

entrenchment. Ensuring a vibrant, independent civil society could serve as a crucial mechanism for preserving governance

FUTURE SCENARIO 4: CATASTROPHE (BOTH CHINA AND THE WEST NEGLECT THE REGION)

The Story. In this scenario, China and the West disengage from the Pacific Islands region, shifting their geopolitical focus elsewhere. As a result, foreign development aid is suspended, leading to the collapse of essential services within PICs. The absence of external support exacerbates state fragility, leaving governments unable to maintain territorial control or regulate critical resources, rendering the region vulnerable to criminal activity and illicit networks.

With weak governance and unsecured borders, illicit actors exploit high-value resources such as timber, oil, and minerals, engaging in corrupt dealings where bribes equal lifetime salaries for complicit officials. This breakdown in accountability erodes governance structures, fueling security breaches and regional instability, creating a spiral of failure that extends beyond the Pacific Islands.

Rebel groups—reminiscent of past unrest in the Solomon Islands—operate with indifference to state sovereignty, challenging national borders. Their motivations remain uncertain, ranging from grievance-driven resistance to profit-seeking exploitation and subsistence survival strategies. Furthermore, these groups may pursue political objectives, intensifying fragmentation and deteriorating national cohesion. The absence of international intervention allows these dynamics to escalate unchecked, accelerating the decline of governance and societal stability across the region.

While widespread starvation is unlikely due to the region's vast maritime resources, the absence of law enforcement and military oversight in fragile PICs could lead to a surge in piracy. Criminal networks may exploit ungoverned maritime zones, engaging in illicit activities such as smuggling, human trafficking, and resource theft, further destabilizing regional security.

Beyond security concerns, food and medical crises emerge as critical issues. With scarce food supplies, violent clashes erupt during sporadic rationing events, exacerbating tensions between communities. Simultaneously, hospital services collapse due to a shortage of medical staff and essential supplies, revealing the systemic failure of healthcare infrastructure. The destabilizing effects of food scarcity, health crises, and unchecked criminal activity extend beyond PICs, creating a ripple effect across neighboring states. Cross-border displacement leads to refugee movements, worsening existing humanitarian challenges. The spread of disease, compounded by malnutrition and inadequate medical care, amplifies the region's vulnerability, further reinforcing the downward spiral of governance failure.

Under this scenario, climate change emerges as an existential threat to PICs, exacerbated by the neglect of both China and the West. The absence of humanitarian and development assistance forces PIC governments to grapple with intensifying climate emergencies without external support, leading to severe socioeconomic and environmental consequences.

As donor nations reallocate aid elsewhere or prioritize domestic concerns, PICs—particularly low-lying island nations—face frequent flooding, resulting in abandoned islands, destroyed infrastructure, forced land acquisitions in safer regions abroad for crop cultivation, and the displacement of communities. Beyond displacement, natural disasters, including flooding and extreme weather events, jeopardize food supply chains and accelerate the spread of disease. In the absence of aid, hospitals lack medical supplies and personnel, amplifying health crises and leading to regional spillover effects, including refugee movements and cross-border disease outbreaks. Thus, this scenario underscores the urgent need for proactive climate resilience measures, as unchecked environmental degradation threatens regional stability, food security, and public health.

Furthermore, under this catastrophic scenario, the lack of foreign assistance leads to state fragility in PICs, rendering governments unable to sustain essential public services. Critical sectors such as education, healthcare, infrastructure development, and law enforcement suffer severe disruptions, pushing communities further into socioeconomic distress. As institutional capacity deteriorates, the inability to maintain governance functions accelerates state collapse, triggering widespread chaos. This political and administrative breakdown fosters prolonged instability, creating an environment where PICs struggle—or fail—to recover from institutional incapacity.

Each occurrence of governance failure, whether in service delivery, security, or infrastructure, reinforces unstable political conditions, deepening regional uncertainty. Without effective intervention, this downward spiral jeopardizes long-term recovery efforts, leading to chronic instability and weakened state sovereignty.

Indicators. Several observable signals point to this scenario's emergence: collapse of basic infrastructure and public services; frequent floods and natural disasters; absence of foreign experts and consultants; failure of renewable energy and climate projects; rising fuel consumption and expensive imports; escalating public protests and political instability; and weakening electoral integrity and the rise of political upheaval, among other things.

This pessimistic scenario underscores the severe consequences of geopolitical neglect, with failed governance structures, economic degradation, and climate vulnerability collectively accelerating regional instability.

Policy Implications. Despite the potential for political, economic, and security efforts, weak Pacific Island governments remain incapable of sustaining basic services or addressing climate resilience without substantial foreign support. The absence of collaboration between China and the West further exacerbates vulnerabilities, reinforcing institutional instability and crisis conditions across the region.

To preclude regional collapse, external stakeholders must reallocate time and resources toward targeted interventions that enhance governance capacity and climate adaptation measures. If left unaddressed, governance failures in PICs will deepen economic stagnation, escalate humanitarian crises, and invite security threats that could destabilize neighboring states. Additionally, Pacific elites must acknowledge that one-party dominance sustained by rigged elections undermines political legitimacy and long-term stability. Without a shift toward transparent governance and democratic processes, opposition movements will continue to gain momentum, fueling widespread protests and eroding public trust. Convincing ruling elites of the disadvantages of autocracy—particularly its unsustainable reliance on external financial flows—remains essential to preventing governance collapse and fostering institutional resilience in the Pacific Islands.

This scenario reflects the urgent need for proactive engagement, where both China and the West recognize the imperative of strategic reallocation of resources to prevent regional failure.

POST-SCENARIO ANALYTIC DISCUSSIONS

The four scenarios serve as analytical tools for forecasting geopolitical influence across plausible trajectories, reflecting potential regional shifts and evolving power dynamics. Moreover, each scenario integrates the present geopolitical reality, historical context, and projected trends to explore how existing conditions may persist or transform over time. As Hannah Arendt articulates, "Predictions of the future are never anything but projections of *present* automatic processes and procedures, that is, of *occurrences* that are likely to come to pass if men do not act and if nothing unexpected happens."[49] This perspective suggests the importance of human agency in shaping geopolitical outcomes, emphasizing that the scenarios generated are not deterministic predictions but rather explorations of possibilities.

The core objective of scenario generation is to broaden the range of conceivable futures, offering a framework for examining the interplay of key factors—such as China's economic engagement and Western strategic influence—in shaping regional stability. By considering multiple combinations of these dynamics, policymakers can refine strategic decision-making, a policy step that fosters proactive responses to emerging geopolitical challenges in the Pacific Islands region.

In using AFA as an analytical framework to generate the scenarios, the stories strive to be coherent and explanatory, bridging present realities and future prospects. Important common threads emerge when reviewing the alternative futures. In three of the four scenarios, some government change occurs. Likewise, Western interests are served in some scenarios by increasing engagement rather than maintaining the status quo. All four scenarios display indicators that, if monitored, would prepare analysts to anticipate challenging strategic issues and preclude leaders from asking them, "*What blinded people to the signs?*"

Wildcards represent some low-probability, high-impact factors that may affect future decisions. In the region, they are unexpected. Climate emergencies like big tidal waves or rising sea levels can be a future source of instability and a stumbling block for Western

engagement and China's presence. These factors could substantially change the domestic and foreign environment where the region's governments make decisions.

These scenarios highlight the critical importance of strategic engagement by the West to counter China's influence. Increasing Western aid, such as in non-infrastructure projects focusing on PICs' socioeconomic needs like health and education, and fostering collaboration, can lead to prosperous and stable outcomes. Stressing democratic values and transparency can strengthen governance in PICs, while Western neglect or reduced engagement can have severe negative consequences. Western policymakers should consider these potential futures, which bridge present realities and future prospects, to make informed decisions that promote stability and development in the Pacific region. By understanding and acting on these scenarios, the West can navigate the complexities of the geopolitical landscape and maintain or rebalance its influence in the region.

Based on the preceding discussion, AFA, or scenario thinking, serves as a powerful tool for challenging the status quo and enhancing individuals' ability to do so by posing the question "*What if*?" This approach allows practitioners and decision-makers to rehearse the possibilities of tomorrow and then to take action today, empowered by those provocations and insights.[50] The four scenarios offer compelling and credible narratives about how the future might unfold in the Pacific region. They explore how the ongoing geopolitical rivalry between China and the West—along with Beijing's increasing focus on the region, as underscored in the Lowy Institute's Pacific Aid Mapreport—might evolve. The four scenarios recognized but did not predict how the socioeconomic life of the Islanders would change.

CONCLUSION AND IMPLICATIONS

This study derives its conclusions on futures research from the alternative future worlds developed within the 2x2 matrix framework, which explores various trajectories for the region. These scenarios provide valuable insights and implications that policymakers can leverage for decision-making. While these conclusions do not represent the only possible short-term outcomes for PICs, they outline broadly plausible scenarios that capture a range of possibilities. By integrating these disparate elements—the alternative future worlds and the 2x2 matrix—this study enriches existing knowledge, offering context for assessing complex circumstances that practitioners and policymakers may find "too complex or the outcomes as too uncertain to trust a single outcome assessment."[51]

The alternative futures of PICs, as explored across the four scenarios, provide insights into potential regional trajectories, including the possibility of their emancipation from the opaque structures of exploitation that sustains Chinese influence. While scenarios two and three lack strategic contemplation at the state level, civil society actively engages in such discourse in the scenario where the West predominates. In this particular scenario, should civil society secure sufficient funding, it could emerge as the dominant force in the Pacific Islands region, shaping governance, policy direction, and sociopolitical influence.

Beyond the bleak scenario, the transformative scenario produces possibilities for the West to reshape PICs' relations with China. Through technical partnerships with the West, PICs can begin a gradual emancipation from Chinese influence while exposing policy distortions through critical assessments. Genuine bilateral dialogue would then be possible. Additionally, if China's asymmetrical economic and social relations—driven by its aid policies—continue to marginalize PICs, strengthened partnerships with traditional allies could empower island leaders to resist political and economic sidelining. The four scenarios suggest a broader hegemonic struggle between China, an authoritarian state with a state-led economic model, and the West, capitalist democracies advocating liberal international order and governance norms. While future-oriented, the West's potential actions in these scenarios are framed or theorized as those of a legacy power seeking to safeguard its traditional leverage, whereas China, as a rising geopolitical force, aims to reshape regional dynamics by expanding its influence and challenging established dominance.

Further reinforcing this point, China's characterization of its relationship with PICs suggests that its strategic engagement has successfully advanced the objectives outlined in its assistance efforts. Beijing, through its state-controlled media outlet Xinhua, asserts that its ties with PICs are founded on mutual benefit and a balance between principles and interests, describing the current phase as "the best time in history"[52] for these relations. The sustainment of this achievement portends an increase in Chinese activities and influence, an outcome that will challenge, if not diminish, the Western traditional powers' sphere of influence.

Nevertheless, some PICs have assuaged traditional partners on the soundness of their infrastructure and investment policies, as reflected in their pronouncements and elites' remarks on China's infrastructure aid projects. Hence, the West needs to guard against complacency on the supposed benign intent of China's increasing aid to the region. They must use a whole-of-partnership approach to ensure that nothing slips through the cracks of secrecy—a PIC loan from China is sustainable, an infrastructure has no dual purpose, Chinese aid is not tied to favorable policy responses, and the like. As the U.S. *National Security Strategy* states: "China is using economic inducements and penalties, influence operations, and implied military threats to persuade other states to heed its political and security agenda. China's infrastructure investments … reinforce its geopolitical aspirations."[53] Accordingly, this study's findings reinforce Beijing's geopolitical aspirations to maintain the Chinese Communist Party's existence.

APPENDIX: GENERATING OTHER POTENTIAL PACIFIC ISLANDS SCENARIOS USING AFA[54]

Aside from the four scenarios discussed in this study, understanding internal and external risk factors could form the basis for creating four new distinct scenarios using AFA. This analysis could then assign the internal factors to the horizontal axis of the matrix. A positive end could represent a permissive internal operating environment for access to the region. The negative end could represent a restrictive internal environment. Similarly, external factors could be assigned to the vertical axis of the matrix, with maximum and minimum levels of foreign influence by China.

After that, a list of indicators, implications, and opportunities could be created for each of the four scenarios (quadrants of the matrix). Next, the current operating environment and its trend would be mapped based on the analysis of recent past indicators of the internal and external factors. Then, a desired end state on the quadrant of the matrix with the least amount of China influence (external risk) and the most permissive environment in terms of internal risks would be plotted. The differences between individual indicators or whether those indicators existed on the current and desired end-state quadrants would form the basis for generating opportunities and challenges the West might need to exploit or overcome to reach the preferred objectives.

Another set of drivers for creating different scenarios is to analyze the future of the region through the effectiveness of the PIC governments and the strength of civil society. The effectiveness of PIC government could be fully operational, and its opposite would be marginalized effectiveness. The strength of civil society could be robust at one end, but its opposite would be nonexistent. Still, another set of drivers could be PICs' security capability, which could be effective at one end and ineffective at the other end of the spectrum. The other driver would be the helplessness of neighboring countries, with neighboring states as stable and supportive at one end and neighboring states as unstable and disruptive at the other endpoint.

Besides these factors, many categories can derive drivers: social, economic, political, technological, cultural, religious, military, diplomatic, information, and demographic. Note that "demographic" is not a driver but rather a category. A demographic driver may be a growing youth bulge. Various studies cited in this study's explanation of the AFA as an analytic framework emphasize that the characteristics of scenarios are that they are not predictions, plans, or designed to reinforce certainty. In fact, there are multiple possible futures, hypotheses, and stories designed to stretch mental maps and customize them to contexts.

Full reflection, positive and negative partial reflections, and hopeless reflection could also take place in each scenario as a form of praxis to alter the existing order. That is to say, framing the future comes in many stories and with different elements and indicators depending on a country's or region's history, politics, society, and culture.

The author recommends using a diverse multidisciplinary team to generate potential drivers and scenarios. The researcher conducted the process of generating the drivers and scenarios alone. Who knows what could have been more robustly produced if a diverse team were used for a brainstorming exercise, although there could be a groupthink trap. By adopting this method, imaginatively plausible scenarios could be generated, and each scenario's characteristics, indicators, and strategic implications would be richer, including risks and opportunities.

NOTES

[1] Mann Virdee and Megan Hughes, "Why Did Nobody See It Coming? How Scenarios Can Help Us Prepare for the Future in an Uncertain World," Commentary – RAND (January 28, 2022), https://www.rand.org/pubs/commentary/ 2022/01/why-did-nobody-see-it-coming-how-scenarios-can-help.html.

[2] Philippa Brant, "China's involvement in Fiji and Australia and New Zealand's position," *East Asia Forum,* December 8, 2009, https://www.eastasiaforum.org/2009/12/08/chinas-involvement-in-fiji-and-australia-and-new-zealands-position/; Richard Herr and Anthony Bergin, "Our Near Abroad: Australia and Pacific Islands Regionalism," Australian Strategic Policy Institute (Canberra, November 2011), 2, https://www.aspi.org.au/report/our near-abroad-australia-and-pacific-islands-regionalism.

[3] Andrew Curry and Wendy Schultz, "Roads Less Travelled: Different Methods, Different Futures," *Journal of Futures Studies* 13, no. 4 (May 2009): 35-60; Sergion Uruena," Understanding "Plausibility": A Relational Approach to the Anticipatory Heuristics of Future Scenarios," *Futures* 111 (August 2019): 15-25.

[4] The approach called Generic Alternative Scenario Analysis is a heterodox approach proposed by the Hawaii Research Center for Futures Studies. Four basic scenarios – continued growth, collapse/ decline and stagnations, toward discipline/sustainable society, and transformation – are established and then fleshed out to explore and illustrate the entering arguments and impacts. This study did not necessarily model most of these scenarios, but it subscribed to the steps of this approach by describing a scenario and then finding paths toward it from the present. See: Dator, "Alternative Futures at the Manoa School," 8-10. The Institute for Alternative Futures came up with variants of Dator's four alternative futures, as follows: Best Estimate or the "Official Future"; Challenge/Hard Times Scenario (Some groups will choose variants of Disciplined or Sustainable Society as their vision); and Visionary Scenarios (defined by the community). In Clement Bezold, "Jim Dator's Alternative Futures and the Path to IAF's Aspirational Futures," *Journal of Futures Studies* 14, issue 2 (November 2009): 133, https://jfsdigital.org/ wp-content/uploads/2014/01/142-E01.pdf.

[5] The most common methodologies policymaking employs for implementing policies involve qualitative (narratives and case studies) and quantitative (statistical data) analysis, as well as mixed method research, which combines qualitative and quantitative approaches to comprehensively understand the impact of policies. Other approaches include the following: survey methods to gather public opinions and data to inform decisions; cost-benefit analysis to evaluate the financial and social costs versus the benefits of a policy to determine its overall value; input-output analysis to understand the relationships between different sectors of an economy and how policy changes affect them; optimization techniques to find the most efficient policy solutions by analyzing multiple variables; computer simulations to predict policy outcomes by simulating different scenarios; and policy evaluation to assess the effectiveness of existing policies and suggest improvements. See: Rachel A. Epstein and Oliver Kaplan, "Responsible Policy Engagement," in: Rachel A. Epstein and Oliver Kaplan, eds., *Speaking Science to Power* (Oxford University Press, 2024); Stephane Moyson , Peter Scholten , Christopher M Weible, "Policy Learning and Policy Change: Theorizing their Relations from Different Perspectives," *Policy and Society* 36, Issue 2 (June 2017): 161–177; Sheila Sia, "The Challenges and Approaches of Measuring Research Impact and Influence on Public Policy Making," *Public Administration and Policy: An Asia-Pacific Journal* 26, Issue 2 (September 5, 2023):169-183; "Research Methods for Public Policy," E. Remi Aiyede and Beatrice Muganda, eds., Public Policy and Research in Africa, Palgrave MacMillan (2022); and Deborah Stone, *Policy Paradox: The Art of Political Decision Making*, revised ed. (W. W. Norton and Company, 2002).

[6] Jim Dator, "Alternative Futures at the Manoa School," *Journal of Futures Studies,* November 2009, 14(2): 8-10, https://jfsdigital.org/ wp-content/uploads/2014/01/142-A01.pdf. See also Peter Bishop, Andy Hines, and Terry Collins, "The Current State of Scenario Development: An Overview of Techniques," *Foresight* 9, no. 1 (2007): 5-25.

[7] A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis (Washington, DC, 2009), 1-3, 38-39, https:// www.hsdl.org/?view&did=20945.

[8] A Tradecraft Primer, 7-36.

[9] A Tradecraft Primer, 5.

[10] A Tradecraft Primer, 34-36.

[11] RAND Europe, through its Center for Futures and Foresight Studies, publishes useful articles on futures research to inform decision-making.

[12] A Tradecraft Primer, *12.*

[13] Dator, "Alternative Futures at the Manoa School," 8-10.

[14] Randolph H. Pherson and Richards H. Heuer, Jr., Structured Analytic Techniques for Intelligence Analysis, 3rd ed. (Thousand Oaks, CA: Sage Publications, 2021), 133.

[15] Hannah Kosow and Robert Gabner, Methods of Future and Scenario Analysis: Overview, Assessment, and Selection Criteria. German Development Institute, Bonn (2008), https://www.idos-research.de/uploads/media/ Studies_39.2008.pdf.

[16] Kosow and Gabner, Methods of Future and Scenario Analysis.

[17] Peter Bishop, Andy Hines, and Terry Collins, "The Current State of Scenario Development: An Overview of Techniques," *Foresight* 9, no 1 (2007): 5-25, https://dx.doi.org/10.1108/14636680710727516.

[18] Preparing for the Unexpected, *2015, 1.*

[19] The Futures Group, "Scenarios," 1.

[20] Bishop, Hines, and Collins, "The Current State of Scenario Development," 6.

[21] Preparing for the Unexpected, 2015, 2-3.

[22] Preparing for the Unexpected, 2015, 2.

[23] Preparing for the Unexpected, 2015.

[24] The Foresight Process, 2010.

[25] Richard A. Slaughter, The Foresight Principle: Cultural Recovery in the 21st Century (Praeger Studies on the 21st Century), 1995.

[26] Ibid.

[27] Ibid.

[28] Bezold, "Jim Dator's Alternative Futures and the Path to IAF's Aspirational Futures," 123-134.

[29] Eva Hideg, "Theory and Practice in the Field of Foresight," *Foresight* (October 2007), 38.

[30] Peter Schwartz, The Art of the Long View: Planning for the Future in an Uncertain World (New Day: Doubleday, 1996), quoted in A Tradecraft Primer, 34.

[31] Global Business Network, "Why Scenarios?" 2010.

[32] Heuer and Pherson, Structure Analytic Techniques, 137.

[33] Heuer and Pherson, Structure Analytic Techniques, 138.

[34] Heuer and Pherson, Structure Analytic Techniques.

[35] Heuer and Pherson, *Structure Analytic Techniques,* 175.

[36] Heuer and Pherson, *Structure Analytic Techniques,*143-144.

[37] Jay Ogilvy, "Scenario Planning and Strategic Forecasting," *Forbes* (January 8, 2015), n.p., https://www.forbes.com/ sites/stratfor/2015/01/08/scenario-planning-and-strategic-forecasting/?sh=677f5809411a.

[38] Australian Department of Foreign Affairs and Trade, "Overview of Australia's Assistance for Governance," Aid -- Effective Governance: Policies, Institutions and Functioning Economies > Governance, https://www.dfat.gov.au/aid/topics/investment-priorities/effective-governance/governance/Pages/governance; New Zealand Ministry of Foreign Affairs and Trade, "A larger, re-oriented New Zealand Aid Programme," https://www.mfat.govt.nz/en/aid-and-development/our-approach-to-aid/; Japan Ministry of Foreign Affairs, Official Development Assistance, ODA By Region, https://www.mofa.go.jp/ files/000406648.pdf.

[39] Alexandre Dayant, Riley Duke, Nasirra Ahsan, Roland Rajah, and Herve Lemahieu, Pacific Aid Map: 2024 Key Findings, Lowy Institute, November 19, 2024, https://pacificaidmap.lowyinstitute.org/ analysis/2024/key-findings/.

[40] China increased development spending slightly in the Pacific in 2022, which meant it overtook the United States to become the second largest bilateral donor in the region, although its $256 million contribution was still dwarfed by the $1.457 billion provided by Australia. In Stephen Dziedzic, "Latest Lowy Pacific Aid Map shows aid decrease amid focus shift to Ukraine," *Australian Broadcasting Company,* November 20, 2024, n.p., https://www.abc.net.au /

news/2024-11-21/lowy-pacific-aid-map-2024/104626366.

[41] Dziedzic, "Latest Lowy Pacific Aid Map shows aid decrease amid focus shift to Ukraine," n.p.

[42] "Preparing for the Unexpected," 2-3.

[43] Pherson and Heuer, Structured Analytic Techniques, 175.

[44] Box 5.2: Infrastructure Investment Needs in the Pacific, in "Asian Development Bank," *Meeting Asia's Infrastructure Needs (*Mandaluyong City, Philippines: 2017), https://www.adb.org/sites/default/files/publication/ 227496/special-report-infrastructure.pdf; Asian Development Bank, "Asia Infrastructure Needs Exceed $1.7 Trillion Per Year, Double Previous Estimates," February 29, 2017, https://www.adb.org/news/asia-infrastructure-needs-exceed-17-trillion-year-double-previous-estimates.

[45] See also "The Critical Tradition: Communication as Discursive Reflection" in Robert T. Craig, "Communication Theory as a Field," International Communication Theory 9, no. 2 (May 1999):146-149.

[46] John Mearsheimer, "The False Promise of International Institutions," *International Security* 19, no. 3 (Winter 1994), *10.*

[47] Australian Department of Foreign Affairs and Trade, "Overview of Australia's Assistance for Governance," Aid -- Effective Governance: Policies, Institutions and Functioning Economies > Governance, https://www.dfat.gov.au/aid/topics/investment-priorities/effective-governance/governance/Pages/governance.

[48] This is based on media reports about narratives of China's aid in the African continent.

[49] Hannah Arendt, *On Violence. Harvest Book:* Houghton Mifflin Harcourt, Inc. (1970), 13 (emphasis added).

[50] Diana Scearce and Katherine Fultin, and the Global Business Network community, What if? The Art of Scenario Thinking for Nonprofits. Global Business Network: Monitor Group (2004), 3, https://www2.deloitte.com/content/dam/ Deloitte/us/Documents/monitor-institute/us-monitor-institute-what_if.pdf.

[51] "Alternative Futures Analysis," *A Tradecraft Primer, 34.*

[52] "The future is bright for China, Pacific Island countries," Xinhua, October 21, 2019, http://www.xinhuanet.com/ english/2019-10/21/c_138491033.htm.

[53] U.S. President, *N*ational Security Strategy of the United States, Washington, DC (October 12, 2022). 1-48,https://nssarchive.us/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

[54] See generally Richard Slaughter and Andy Hines, eds., Knowledge Base of Futures Studies 2020 (Washington, DC: Association of Professional Futurists); Richard A. K. Lum, 4 Steps to the Future: A Quick and Clean Guide to Creating Foresight (FutureScribe: Honolulu, HI, 2016); and Wendell Bell, Foundations of Futures Studies: Human Science for a New Era (Vol. 1. Transaction Publishers, 1997). The study China-US Competition: Measuring Global Influence, published by the Frederick S. Pardee Center for International Futures at the University of Denver in collaboration with the Scowcroft Center for Strategy and Security, focuses on assessing the global influence dynamics between the United States and China. The study's Formal Bilateral Influence Capacity Index, a quantitative framework designed to measure multidimensional influence between states, allows for longitudinal analysis, tracking changing influence dynamics across more than 200 countries and 20,000 country pairs from 1960 to 2020. This enables futures researchers to forecast geopolitical trends based on historical influence patterns, identify emerging power shifts and potential regional realignments, and evaluate the long-term sustainability of U.S. and Chinese influence strategies. See Jonathan D. Moyer, Collin J. Meisel, Austin S. Matthews, David K. Bohl, and Mathew J. Burrows, "China-US Competition: Measuring Global Influence," Pardee Institute, Josef Korbel School of International Studies, May 2021, https://korbel.du.edu/pardee -resources/china-us-competition-measuring-global-influence/

M. John Bustria has worked for nearly 15 years in various capacities as a staff and manager covering geographic and functional accounts, as well as project management, for the U.S. government. He has 18 years of work experience in policy, diplomatic, and academic positions. A graduate of National Intelligence University's master's and graduate certificate programs, Dr. Bustria did a one-year research fellowship at this institution, where he is an adjunct faculty.

NMIF Scholarships

Supporting the Next Generation

The NMIF is dedicated to inspiring new generations of intelligence professionals, recognizing the success of current intelligence professionals, and sustaining the intelligence workforce needed to ensure the overall capability of the military intelligence function to support the national security of the United States of America.

The Impact of Donating

The NMIF scholarships mean the world to the students. It is an acknowledgement of their hard work and dedication in pursuit of courses of study, internships, and degrees building towards a career in intelligence, national security, and related disciplines. These brilliant students look to their predecessors for guidance, validation, and support. This support contributes to the furtherance of their career, providing them the recognition and encouragement needed to go forth and do great things for our nation. Supporting students in pursuit of undergraduate and graduate programs that lead to careers in the Intelligence Community remains a major priority for NMIF. Your donations help NMIF make this happen. Help us give a scholarship to a well-deserved recipient. www.nmif.org

New Employees Deserve Better

by **Ms. Cheyenne O. Patnode**

If the Intelligence Community (IC) wants to get the best work from its new employees and entice them to make the IC a career, not just a job, the IC needs to cultivate psychological safety and trust among its new employees. Research conducted for a National Intelligence University 2023 master's thesis demonstrates new hires are not having these needs met.[1] The research consisted of in-depth, open-ended, semi-structured interviews with newly hired Defense Intelligence Agency (DIA) civilian employees who were still serving their two-year probationary term. Fourteen volunteers from six distinct organizations and combatant commands within the DIA representing a variety of occupational disciplines and specialties, varied government, non-government, and Defense Department backgrounds participated in the study. The ages of participants ranged from early twenties to late forties. The population of participants included a balance of men and women from multiple ethnicities. A group of fourteen participants is considered a large number for this type of qualitative research. In fact, many more newly hired DIA civilian employees volunteered to participate in the study, but there was not the capacity to add their views. To protect employees' privacy, their direct quotations provided for this article have been attributed to a randomly generated number so that individuals cannot be personally identified.

HIRING, ONBOARDING, AND PCS EXPERIENCES

The topic that was most often raised in the interviews was that unresponsive government officials involved in the hiring and permanent change of station processes and the confusing, inaccurate information they provide new employees make the hiring and permanent change of station (PCS) process traumatic for new employees. Every single one of the 14 interviewees cited having trouble with the PCS and hiring processes. Most of the interviewees expressed a great deal of frustration in the tone of their voice and body language while describing their hiring and/or PCS process. Some became incredibly emotional and were moved to tears describing what some of them deemed an incredibly difficult and frustrating time in their lives. Some of the experiences they recounted included the following:

> Employee 95: "PCSing was terrible. A lot of the materials that were given to me to help me PCS had incorrect information on them. Also, none of them were meant for someone brand new to the government. There was a ton of information in the paperwork I did not understand, because this is my first time working for the federal government. So many acronyms and jargon I was completely unfamiliar with. The Office of Human Resources (OHR) and PCS Coordinators were also really hard to get ahold of. They seemed very unresponsive. I would send multiple emails and call them but would not hear back for weeks. When I did get ahold of them and asked questions a lot of time my PCS Coordinator would say, "I don't know. You'll have to ask someone else" …. It was such a stressful and confusing time. I was not making any money, sitting by the phone and computer every day, and no one was talking to me. …. No one responded to me. I had to borrow thousands of dollars from my parents to move myself. My first several months after I PCSed were not good. I was alone, I was broke, and I was frantic. DIA did not help me."

> Employee 80: "The minute I said, Okay, I'll do this [accept the job offer]. Like nothing. I basically just didn't hear back. It felt like radio silence. As far as the PCS process is concerned, it was extremely expensive and there was no help whatsoever…. Once I received my final job offer it had the wrong salary on it. So, it wasn't just radio silence, it was also sloppy. Other new employees told me they experienced very similar issues."

> Employee 39: "When I received the job offer for this job, I was very hesitant to accept it. I asked OHR a bunch of questions regarding finances and moving. Can you please tell me what you financially cover? So, I can do some calculations and just do the math. Like, what can I afford? Am I putting myself at risk? My PCS coordinator told me, "Oh we just PCS

you." I have no idea what PCS means. I asked her to explain, and she indicated it is part of the paperwork. So then, I google "PCS" and of course there are a million descriptions of that that means. I am not part of the military and most of the descriptions I can find online apply to military personnel. So then, I am questioning what part of the PCS process applies to me. Therefore, I reach back out to OHR and get met with the following response, "If you don't accept this job, we will put your resume at the bottom of the pile." And I was so hurt. I shared that hurt and embarrassment with all my friends, family, and colleagues so they could understand how the government was treating people trying to get hired. I am not asking for additional money. I am asking for someone to help me understand. Someone to treat me with human decency. These people are in HR roles, and they treat you worse than trash."

Employee 46: "My PCS coordinator really did not communicate with me. None of the timelines were ever accurate. I lived out of boxes for months waiting to PCS. My wife and I took our kids out of school. She [wife] quit her job. We always knew what the next step was, but the timelines were outrageous, and no one was communicating with me…. It was a nightmare."

The employees' perception that the information provided to them was misleading or incomplete had profound consequences as it undermined their trust in DIA as an institution. This lack of trust may significantly affect employee morale, engagement, and productivity. Some of the interviewees conveyed the following:

Employee 141: "[Starting to work at DIA] has truly been one of the worst experiences of my professional life. I sacrificed so much for this job. I changed everything about my human behavior to get accepted, and I feel like it is a privilege, or I thought it would be a privilege to work here and I'm just embarrassed. But you know, it was a difficult onboarding. It was humiliating. There are so many people that don't treat people with human decency. You know, it's so funny because they have so many recruitment and retention issues. And I'm like, I've devoted seven years of my life to higher education for this specific job for you guys [DIA]…. My mentors told me not to join and I didn't listen because I felt it was important that I have my own data because they're all Cold War veterans – so I thought things have changed. And I would give it a shot and I regret my decision wholeheartedly."

Employee 133: "I have zero trust in this agency. I live in fear of what this organization will do to hurt me and not help me. My immediate supervisor is great, but the larger Agency does not engender any loyalty. It honestly felt like the people working in OHR were intentionally negligible. They [OHR] were avoiding me. Not helping me. Not investing in me. I felt so isolated. I had no support. No community."

Employee 200: "If I didn't already have a job I would have been really struggling, because the process took so long. At a certain point, it felt like DIA was doing everything they could to forget that I was even hired, whereas my current company I was working with while waiting to start at DIA was doing everything, they could to keep me. I really started to worry toward the end, like am I making the right decision – joining DIA that doesn't even know I exist?"

Employee 103: "I was offered a bonus to take this job, and I heard from others that they did not get a bonus. I do not know how DIA decides who gets a bonus, but that is pretty messed up if they are just picking and choosing people. What if the OHR person is super biased and unfair? Has anyone looked into whether we are providing bonuses equitably across genders, ethnicities, or even education levels? I tell every new person that I meet to ask for it now. I do not trust DIA is being fair."

PROBATIONARY PERIOD EXPERIENCES

Newly hired DIA civilian employees are hired into a two-year probationary period. During that period, supervisors are supposed to gauge their performance to determine whether they should be offered long-term employment. This practice is widespread throughout the federal government. While the Government Accountability Office and the U.S. Merit Systems Promotion Board have issued reports questioning whether federal agencies are effectively supervising and evaluating probationary employees, there has been no research asking the new employees about their experiences in the probationary period. Determining how probationary employees experience the probationary period was the original intent of this research. The results were dumbfounding.

Many employees had never been informed that they were in a probationary period. Others said they had received very little information about the probationary

period, which hindered their capacity to engage in more informative dialogues about expectations, OHR regulations, and employee rights. In addition, new employees felt their immediate supervisor and OHR staff were not adequately prepared to assist new employees. This trend was considerably more prominent among respondents who lacked military or government experience prior to assuming a federal government position. Many of these professionals were particularly dissatisfied that the information provided to them was difficult for someone new to government service to comprehend. Some of the comments they offered included:

> Employee 388: "The main thing I would change is we need more information. New people are left in the dark a lot, especially when going through the hiring process. Maybe OHR does not have enough people or maybe they do not have enough trained people, but that process is miserable. I also feel like supervisors need more training, especially if they are given a brand-new employee, because we do not know a lot about the Agency and our supervisor is our only outlet for information. They need to know how to assist different types of new people better."

> Employee 319: "The probationary period is sketchy, because if you have a bad supervisor and you do not get along. What does that mean? You just lose this job that took you over a year to start. What a waste that would be. And maybe that is not how it works, but I don't know that because no one has told me differently, so that is how I feel. I still feel like there were certain topics in Touchstone[2] that they spent a lot of time on, that might not have been as beneficial as spending more time on you know, maybe the probationary period or just even explaining what it was or HR people talking more about the different benefits."

> Employee 350: "I think supervisors need a lot more education on how to handle probationary employees. Employees need more access to the information too in case they have a supervisor that is unwilling to help them. I would say the lack of information causes a lot of confusion…."

> Employee 392: "I think that an HR department needs to be really, really strong no matter what, but especially if that is like the first point of contact for new employees. Right? So, it's, you know, one thing maybe if you've been in and you're dealing with other personnel matters, but if you're new to the agency, and essentially if you're new to the IC, like you really want to make sure that there's like a flawless transition or entry point into that community. And I didn't feel that way at all. I've always had questions. I never had answers. I tried calling. I tried emailing. And there was nothing until I guess somebody else decided to pick up my case a few months later, and they still got my information off. So yeah, I wasn't happy with it. I think they need to overhaul everything. And like I was sending, like my social security number and other like sensitive information through Gmail. Whereas with some of the other IC agencies they wanted me to send it through a password encrypted format. And here I was just, you know, sending stuff and I was thinking like, come on. I had federal training about this, sensitive information is not supposed to be handled through Gmail, so I find that kind of ironic."

> Employee 328: "New employees need more information and formal training. I appreciated the efforts of Touchstone, but for someone brand new to government work it was not enough information. Also, currently I have a great supervisor, but he does not know everything, and I only know what he has shared with me. I wish I knew where to go to get more information like a Newcomers SharePoint page that has a ton of information on it or something. Also, as you now know, I know nothing about the probationary period, if I get fired overseas what happens? Do they just leave me here? If someone has a bad supervisor, are they just screwed? This is why new employees need access to more information. I should know these things or at least know how to look them up."

> Employee 380: "…. I wish expectations were clearer. Just tell me what I should and shouldn't do while on the probationary period. Touchstone should go into greater detail about being probationary, so more employees are informed early on. Ideally, supervisors should be trained too, because communication with your direct supervisor is so critical when you are a brand-new employee. A recommendation would be to create a SOP Library for new people. A place that has a lot of this information so we can inform ourselves too instead of just relying on what our supervisors know."

If they knew about the probationary period, new employees were often ill-informed as to the implications. Some of the interviewees related:

Employee 300: "Umm. I am assuming it means I did something wrong. Probation – sounds like I am in trouble. I honestly have no idea. No one has ever said anything about it."

Employee 237: "No one really talks about it [probationary period]. Basically, supervisors can fire you up to the last day of the period though. I am a bit of cynical person and feel like they can fire you for any reason. I really do want to a good job."

Employee 290: "I think the probationary period only matters if you are planning on moving. I do not plan on looking for another position anytime soon – so I don't think it really applies to me. Also, I took the recruitment bonus and I think you have to pay it back if you don't finish your probationary period, so I definitely don't plan to move."

Employee 295: "I don't really know what it [probationary period] means. I saw it on one of my documents and I was like, 'Ohh I didn't know I was a probationary employee.' So, I asked about it a bit and was told it means I cannot apply for other jobs for at least two years, but other than that it hasn't been explained to me. So, I have just assumed it means I stay in the position I was hired into for at least two years, and I can be fired at any moment without cause, because no one talks about it."

Employee 225: "No one has talked to me about it – but I think it means I can be instantly canned anytime. Like right now I must prove myself."

Employee 251: "I don't understand what it means [probationary period]. No one talked to me about it. I know I am supposed to go to PACE and CDASA within in two years of starting my job."

Employee 279: "The probationary period basically means I can be terminated at any time for any particular reason."

The interviews demonstrated that DIA employees did not feel welcomed during the hiring and PCS periods. Their experiences were instead traumatic, characterized by confusing, inaccurate information and unresponsive government officials. As a result, new employees began their DIA careers with significant misconceptions about the probationary period and a fundamental distrust of the organization's operation and transparency which eroded employees' confidence in the DIA generally.

EMPLOYEE VOICE EXPERIENCES

Fortunately, new employees' experiences improved upon arrival at their duty station; however, the employees still indicated a reluctance to offer fresh ideas or views inconsistent with those of their leadership.

Employee 413: "Oh, I feel very comfortable expressing my opinion. Which is good because I don't necessarily think I'd feel as comfortable if I were in another office, like, you know, another set of cubicles. I have a really nice supervisor and then my other four colleagues are all very nice. I don't feel like I need to be careful with what I say."

Employee 491: "Certainly in my little team, I don't have any qualms asking for help and basically, every day, like you know, whether it was timecards or computer things. There's nothing that I haven't asked. I'm constantly asking for help, and everyone's been really awesome on my team. They're going the extra mile to help try to clarify things for me, even before I can ask so I have no problems asking for help in my immediate little branch."

Employee 416: "Hmm I don't think I have a problem asking for help. I think I have a problem with gauging when it is appropriate to ask for help. I tend to be a bit timid at first. I will say as I get more comfortable, I am more willing to ask. I think my teammates and supervisors will be very receptive. I did not ask for enough help when I was struggling dealing with HR things. I regret that, but then again, I didn't even really know who to ask."

Employee 568: "I do not have any experience disagreeing with anyone at work. I am still at that stage where I just do the tasks assigned to me and don't ask questions. I just feel like I have too much to learn."

Employee 600: "I am still too new for that. If I have an idea, I might share it with someone peer level, which I have done before, but above that – yeah, I probably wouldn't do that yet."

Employee 585: "I am unsure what I would have to disagree about being so new. I am overwhelmed by what is on my plate now. I don't have anything to disagree about."

Employee 511: "So I am a much more mature employee, in my position I will be expected to be the guy coming up with new ideas eventually. But for now, I am trying to learn my team and gather all the information I can so I can be more educated about trying new things. The other important thing to remember is a lot of people have been here a long time. Some of them don't want a leader to come in and make a bunch of changes. I have to be sensitive to that.

Employee 566: "I had an older colleague call me adorable. I did not like that, but I did not make an issue out of it. I guess that would be a disagreement. This is my first real job. I guess I don't really know what to expect in some cases."

Employee 556: "I have one terrible disagreement story where I totally disagreed with someone's behavior, but I did not respond. Thinking back on it – I definitely wish I would have handled it differently like maybe said something, but I just walked away. This guy was literally screaming at me, and someone had to calm him down. I did not know how to respond. I just left."

STUDY IMPLICATIONS

This reluctance to offer fresh ideas or views inconsistent with those of their leadership was not unexpected. Harvard University professor Amy Edmondson has found that achieving high performance requires employees having the confidence to take risks, especially in a knowledge-intensive world. Edmondson wrote, "When an organization minimizes the fear people feel on the job, performance—at both the organizational and the team level—is maximized. People [need to be able to] feel able to speak up when needed—with relevant ideas, questions, or concerns—without being shut down in a gratuitous way."[3] Probationary employees may perceive reduced psychological safety as a result of their view of their own vulnerability. Therefore, these employees may approach their positions with greater trepidation and exhibit more caution than those who have successfully completed the probationary term or who are not subject to one. There is significant scholarly research supporting positive correlation between psychological safety and employee engagement, employee voice behavior, employee motivation, and creativity, knowledge sharing, organizational trust and organizational learning.[4]

Employees evidenced a higher degree of psychological safety upon arrival at their duty station, as many participants spoke fondly of their direct supervisors and work teams. The researcher felt this positive experience indicates the importance of managers in creating a culture that values feedback, honesty, and advancement opportunities for every employee. In addition, the contrast between the positive current team experience and the perceived deficiencies of the hiring or PCS processes suggests that organizations should endeavor to create a consistent and positive employee experience throughout the entire employee lifecycle. This conclusion also highlights the value of leadership and management education in forming productive relationships with direct superiors. Based on the employee responses successful teams often include supervisors that put an emphasis on open lines of communication, attentive listening, and offering direction and encouragement. Investing in leadership training may help managers form supportive relationships with their staff and create a productive office climate.

As noted above, however, psychological safety would be enhanced by employees and supervisors both being better informed about the probationary process, its rationale, and implications. Because new employees interviewed indicated a reluctance to offer fresh ideas or opposing views, supervisors should analyze their organization's culture or long-standing procedures to ensure they are not serving as a barrier to honest communication. New hires often require encouragement to provide their own creative solutions or to question established norms.

RECOMMENDATIONS

Addressing the major shortfalls in the hiring, onboarding, and PCS processes is crucial for the organization to maintain its reputation and attract top talent. The negative experiences shared by current employees during interviews not only impacts their morale and engagement but also has the potential to deter potential candidates from considering employment with the organization. This can result in a diminished ability to attract highly qualified individuals, which can ultimately hinder the organization's success.

One key aspect that needs attention is the provision of accurate and sufficient information for newly hired employees. It was observed that in many cases, employees were provided with little or incorrect information about the processes involved in their

employment. This lack of clarity and guidance can lead to frustration, confusion, and a negative perception of the organization. To rectify this, there is a need to overhaul the hiring, onboarding, and PCS processes. Clear and comprehensive communication should be prioritized, ensuring that new employees are well-informed about the processes, expectations, and available resources. There needs to be a way for new employees to track where they are in the hiring, onboarding, and PCS process. Additionally, providing customer service training to the OHR staff can improve their communication styles and approachability, enhancing the overall experience for new hires.

Furthermore, establishing a feedback process and mechanisms for new employees to share their concerns is essential. Many public and private sector companies utilize customer service feedback surveys to allow individuals to express their concerns and provide suggestions for improvement. The Agency could consider implementing a similar feedback mechanism to provide new employees with a platform to voice their grievances, address incorrect information promptly, and offer suggestions for enhancing the processes. This feedback loop would not only allow the organization to identify areas for improvement but also demonstrate a commitment to actively listening to and addressing the concerns of its employees.

In addition to addressing the information gaps and implementing feedback mechanisms, it is crucial to address instances where new employees feel ignored or experience rudeness from their PCS coordinators or hiring managers. Such behaviors are detrimental to the employee experience and can lead to disengagement and dissatisfaction. Implementing a feedback mechanism that allows new employees to report such incidents would serve as a deterrent for staff to engage in unprofessional behavior. It would create accountability and foster a more respectful and supportive work environment.

PROBATIONARY PERIOD

Organizations should prioritize effective communication strategies and educational initiatives surrounding the probationary period in order to address the lack of information and dispel misconceptions. This can include conducting orientation sessions, distributing written materials, and conducting regular mandatory check-ins and performance reviews with probationary employees. During the probationary period, transparent and open communication channels, such as town hall meetings or dedicated Q&A sessions, can help resolve any concerns or questions that may arise. These educational/training initiatives should not solely be focused on new employees. It is important for supervisors and managers to be thoroughly informed on the probationary period as they are the ones guiding the new employees through this time. By proactively addressing and clarifying misconceptions, organizations can ensure that new employees have a better understanding of the purpose, expectations, and implications of the probationary period. This can, in turn, foster a more positive and supportive work environment, reduce unnecessary stress and anxiety, and set employees on a path toward success and long-term employment.

NOTES

[1] Cheyenne O. Murray, "New Employees Deserve Better" (master's thesis, National Intelligence University, 2023)

[2] Defense Intelligence Agency (DIA) orientation program for newly hired employees.

[3] Amy Edmondson, *The Fearless Organization: Creating Psychological Safety in the Workplace for Learning, Innovation, and Growth,* (Hoboken, New Jersey: John Wiley & Sons, 2019).

[4] Amy C. Edmondson and Zhike Lei, "Psychological Safety: The History, Renaissance, and Future of an Interpersonal Construct," *Annual Review of Organizational Psychology and Organizational Behavior 1, no. 1* (2014): pp. 23-43, doi:10.1146/annurev-orgpsych-031413-091305; Yuanqin Ge, "Psychological Safety, Employee Voice, and Work Engagement," *Social Behavior and Personality: An International Journal 48, no. 3 (March 1, 2020): pp. 1-7, doi:10.2224/sbp.8907*; Alexander Newman, Ross Donohue, and Nathan Eva. "Psychological safety: A Systematic Review of The Literature." *Human Resource Management Review 27, no. 3 (September 2017): 521-535. https://doi.org/10.1016/j.hrmr.2017.01.001.*

Ms. Cheyenne O. Patnode is an employee of the Defense Intelligence Agency and a recent graduate of the National Intelligence University in Bethesda, Maryland.

Job Rotational Programs:
Promoting New Employee Engagement

by **Jack A.**

High turnover rates have recently challenged the federal government, with many employees leaving for the private sector, draining the Intelligence Community (IC)'s experience and lowering productivity.[1] In 2021, the then Director of National Intelligence, Avril Haines, reported that attrition is most commonly caused by few advancement opportunities, insufficient mentoring, a lack of fairness in the workplace, and low attachment to the organization and employees' roles.[2] New data from research firm Gartner on the post-pandemic workforce shows that maintaining high retention rates will be increasingly difficult. The data shows that "employee turnover is forecast to be 50–75 % higher than companies have experienced previously."[3] This trend is especially prevalent among younger generations, the majority of whom don't see themselves working at a specific company for more than four years and are likely to be more motivated than previous generations to hop from job to job[4]; improvements to mentorship programs and equitable paths to promotions, while important, do little to address younger generations' desire to explore different careers.

One strategy to boost retention used by the private sector is to offer job rotation options to entry-level and recent graduate employees.[5] A job rotation program can give officers a greater understanding and attachment to the IC mission, develop their professional networks earlier in their careers, and satisfy their desire to explore alternative career options without losing talented workers and their expensive clearances to the private sector. While broadening assignments and the freedom to change career disciplines exist, they often take place in the middle stages of an employee's career, minimizing the potential benefit this process has to help employees determine the appropriate job fit and then choose a career in the IC.[6]

The IC would benefit from implementing a job rotational program to give agency employees a broad understanding of how different departments function across their organization, with an opportunity at the end of three years to select a career path that they are best suited for. This paper examines how job rotation programs mesh with literature descriptions of organizational culture, how they expand the diversity of thought and promote employee engagement, and how this process can be implemented in the IC to improve the problem of employee retention. Job rotation programs are a popular tool in some parts of the private sector intended to develop entry-level employees and give them a diverse skill set and network to benefit the rest of their careers.

Private sector firms like Northrop Grumman have programs such as Pathways, which target recent college graduates, providing them with three-year job rotations "that provide guided, intentional experiences to acquire a breadth of technical skills to establish a foundation in their career and develop business acumen."[7] Programs like these allow employees to explore different opportunities and interests throughout the company. For example, suppose someone joins an agency as an HR officer. In that case, they may spend a year supporting an analytical component and subsequent years supporting an operational or technical component, giving them a greater understanding of how different parts of the agency contribute to the mission and opening up at least three potential departments they can explore more permanently.

Junior employees entering the IC may experience issues with "job fit" or ensuring their role is aligned with their expertise and personality[8] Job fit in the IC can be challenging for new hires because of the limited information publicly available on the work culture and job expectations of these organizations. Poor job fit is a major indicator of an employee's likelihood to seek new positions elsewhere and represents a serious concern to the federal workforce.[9] By allowing new employees to explore multiple departments, they are more likely to find a position they feel comfortable in, thereby reducing their desire to seek opportunities outside of their home agency. The U.S. Merit Systems and Protection Board found that the right job fit is important to positive workplace outcomes such as employee engagement, job satisfaction, and lowering attrition rates.[10] Unfortunately, not everyone's first job is the best fit for the employee or

the company, which is why easy pathways to alternative positions can be a benefit to all.

Employees in rotational programs also gain opportunities to develop new skills and expand their professional networks in ways otherwise limited, helping the organization create a diverse interconnected array of workers to help tackle multi-disciplinary problems. According to Mclean and Company, establishing a job rotational program can boost employee engagement with the organization and develop a wide range of diverse skills in the workforce; but such programs require consistent support from management and HR to ensure that employees get the development and career guidance they need to grow and feel like they are integrated with their office.[11] Another potential roadblock is ensuring there are enough entry-level jobs that can consistently support the stand-up of rotational employees to make such a program successful. If there are too many officers competing for a select number of slots, it can reduce the benefits of networking and learning intended by these programs and lead to infighting between employees.

Job rotation programs apply lessons from several leadership and management strategies, including developing organizational culture and promoting diversity of thought. Leaders striving to shape a specific organization's culture and values may find rotations are an incubator for what is going right and what is going wrong in cultivating a learning environment. If enough new hires with similar experience are asked via end-of-rotation surveys if this program fosters curiosity, learning, and other values a company wants to promote, they may gain access to a new source of early career data that can be used for more enlightened decision-making. Whitney Johnson's article on organizational learning provides evidence that job rotations are a tool for teaching new hires about a company's values and mission, helping employees connect with the bigger picture early on.[12]

Ensuring employees have a range of experiences across multiple departments helps broaden an organization's diversity of thought. It also encourages innovation, rather than being pigeon-holed into specific departments that have limited engagements with one another, which is reflected in Ely and Thomas' *Harvard Business Review* article: "The case for establishing a truly diverse workforce, at all organizational levels, grows more compelling each year …. The financial impact—as proven by multiple studies—makes this a no-brainer."[13] These rotations will also encourage the development of broad professional networks among new employees, which is critical for building future career success and may prove helpful with current employee concerns surrounding promotion and career growth. The "First 90 Days in Government" reading shows how mapping influence networks, building your credibility within an organization, and applying this 90-day approach over several years will prove fortuitous for employee job engagement and personal attachment to the workplace.[14]

A job rotation program can be integrated into the IC post-onboarding process to provide new hires with a clear path for two or three rotational opportunities in a directorate before settling on a permanent position, similar to the private sector. For new hires who come to the IC without a strong specialized background, a rotational program allows them to tour different directorates like analysis, operations, or support, with an ultimate career service decision made at the end of their rotational period. This program could be heavily resisted by members of the IC who do not already practice similar rotation-based assignments, and cultural understanding of the program's value would have to be instilled at a leadership level. If a program like this is seen as a waste of time or unnecessary by management, it will likely not have the desired effect of encouraging people to stay within the IC, as employees may feel they are being dragged through a process viewed with disdain and little enthusiasm. The IC would also have to change how it approaches training its officers by encouraging a greater emphasis on the development of IC-wide culture and skills that can be cross-applied to different disciplines, specifically in the form of rotational programs.

A job rotational program for new employees can help reduce the future attrition rate of officers and cultivate valuable IC-integrated professional networks, culture, and diversity of thought. Potential challenges to this effort, such as workplace stigma surrounding "job hoppers" and the "this is how we have always done things" mentality, can be shifted with training and the celebration of programs that create diverse work experiences. Shifting the organization's values towards interdepartmental development can help reduce employee fears of prioritizing their development over mission needs.

NOTES

[1] Tamara Harutyunyan, "Employee Retention in the Public Sector," California State University, Northridge (2019), https://scholarworks.calstate.edu/downloads/v979v580q

[2] Nicole Ogrysko, "Intelligence Community Workforce Is More Diverse, but Still Struggles with Retention and Promotion," *Federal News Network*, October 27, 2021. https://federalnewsnetwork.com/workforce/2021/10/intelligence-community-workforce-is-more-diverse-

but-still-struggles-with-retention-and-promotion/.
[3] Helen Tupper and Sarah Ellis, "It's Time to Reimagine Employee Retention," *Harvard Business Review*, July 4, 2022, https://hbr.org/2022/07/its-time-to-reimagine-employee-retention.
[4] Emma Waldman, "How to Explain Job Hopping in an Interview," *Harvard Business Review*, September 2, 2024, https://hbr.org/2024/09/how-to-explain-job-hopping-in-an-interview?ab=HP-topics-text-5.
[5] Imamah MNasir, "Dayforce - Why Job Rotation Programs Are Key to Engagement and Retention," www.dayforce.com, https://www.dayforce.com/blog/why-job-rotation-programs-are-key.
[6] "Joint Duty," n.d. www.dni.gov, Director of National of National Intelligence, https://www.dni.gov/index.php/careers/joint-duty.
[7] "A Pathway into an Engineering Career | Northrop Grumman," Northrop Grumman (2022), https://www.northropgrumman.com/life-at-northrop-grumman/a-pathway-into-an-engineering-career.
[8] Scott Dust, "What Is Job Fit and Why Does It Matter?," *Psychology Today*, October 20, 2020. https://www.psychologytoday.com/us/blog/what-we-really-want-in-a-leader/202010/what-is-job-fit-and-why-does-it-matter.
[9] "The Importance of Job Fit for Federal Agencies and Employees in Brief," (2020), https://www.mspb.gov/studies/researchbriefs/The_Importance_of_Job_Fit_for_Federal_Agencies_and_Employees_1774214.pdf.
[10] "The Importance of Job Fit for Federal Agencies and Employees in Brief," (2020), https://www.mspb.gov/studies/researchbriefs/The_Importance_of_Job_Fit_for_Federal_Agencies_and_Employees_1774214.pdf.
[11] "Implement a Job Rotation Program | McLean & Company." n.d. Hr.mcleanco.com. https://hr.mcleanco.com/research/ss/implement-a-job-rotation-program.
[12] Whitney Johnson, "Your Organization Needs a Learning Ecosystem," *Harvard Business Review* (July 2019).
[13] Robin J. Ely and David A. Thomas, "Getting Serious about Diversity: Enough Already with the Business Case," *Harvard Business Review* (November 2020), https://hbr.org/2020/11/getting-serious-about-diversity-enough-already-with-the-business-case.
[14] Peter H. Daly, Michael Watkins, and Cate Reavis, *The First 90 Days in Government: Critical Success Strategies for New Public Managers at All Levels* (Boston, MA: Harvard Business School Press, 2006).

Jack has served as a U.S. intelligence officer since 2018 and is pursuing a Master's in Strategic Intelligence from the National Intelligence University. Jack aspires to serve in leadership and managerial roles in the future, contributing to the future of the intelligence community and developing the next generation of intelligence community officers. Jack resides in Northern Virginia with his wife and two dogs.

2025 NMIF Night of Heroes
SAVE THE DATE

Planning and fundraising is currently underway for the 2025 Night of Heroes Intelligence Annual Awards Banquet.

Event Details:
When: 20 November 2025
Where: Crystal City Gateway Marriott, Arlington VA

The NMIF is excited to have you with us to celebrate individuals from all the Services, the Guard and Reserves, and the Military Intelligence Agencies.

Please visit www.nmif.org for more information

Mission and Meaning:
Strengthening the Intelligence Community Workforce

by **Troy O.**

The Intelligence Community (IC) stands at the forefront of national security, requiring a workforce of exceptional individuals equipped with specialized skills and unwavering commitment. However, a pressing issue that undermines the IC's operational effectiveness is the challenge of talent recruitment and retention.

Amidst an increasingly complex global landscape, the IC's need for adept analysts, linguists, field operators, and cyber specialists has never been more critical. Yet, it faces significant hurdles in attracting and retaining such professionals. The allure of the private sector—with its competitive salaries, vibrant work environments, and rapid career progression—often eclipses the IC's value proposition of patriotism and job security.[1] The lengthy and rigorous security clearance process and associated stringent security-centric work environment likely deters potential candidates. This talent shortfall leaves the IC at a strategic disadvantage, demanding immediate attention and rectification to ensure an able-bodied and healthy IC enterprise to combat the challenges it faces in the 21st century. To mitigate the talent acquisition and retention crisis within the IC, it is imperative to adopt and tailor private sector best practices that emphasize competitive compensation, career mobility, and enriched work culture, thereby enhancing the IC's appeal to top-tier candidates and current employees, resulting in more robust, capable, and dynamic intelligence apparatus that is able to better execute in support of the national security strategy.

The strategy is simple, according to the Harvard Business Review, "Ask people what they want and try to give it to them."[2] Private industry leaders, recognizing the competitive environment employers currently find in the recruitment market and talent retention arenas, have reimagined their strategies to obtain the best possible workforce in order to give their businesses a competitive edge in their respective industries.

This approach, centered around a robust Employee Value Proposition (EVP), has redefined employee engagement and loyalty. A key component of the strategy is a 'Total Rewards' system that extends beyond salary to include performance bonuses, stock options, and comprehensive benefits tailored to employee needs. This so-called "talent war" reinforces sound recruitment and retention strategy based upon an encompassing EVP's tenets of 1) material offerings, 2) growth and development, 3) community and connection, and 4) meaning and purpose.

> Material offerings focus on employee compensation and other financial incentives, office infrastructure, updated technology packages to increase productivity, and flexibility in the workplace and employee schedules. Material offers are undoubtedly important, but alone, they are not enough if other value proposition areas are neglected.
>
> Opportunities to develop and grow center around how an organization supports employees' personal and professional development by acquiring new skills, education, and other developmental opportunities. This can include room for growth in the organization into leadership or technical oversight roles.
>
> Connection and Community aims to foster an inclusive environment that makes team members feel part of a larger team. This principle values the individual employee and creates an environment that nurtures a sense of belonging and an open platform for expressing and sharing ideas.
>
> Meaning and purposes answer the 'why' of the organization and aligns the workforce behind the mission. This tenant aims to establish a calling or purpose of a higher nature that seeks to improve an agency's local or global footprint on a small or large scale. This is the core of establishing the workforce's purpose at an organization and what drives them to continue as part of an organization in the long term.

A well-rounded value proposition is an active process between an organization and its workforce to understand its team's needs and adapt its practices around that feedback. A firm such as Tesla, while having all the elements to offer a strong value proposition to its employees centered around its altruistic mission, falls short in extending a work/life balance, which greatly reduces its EVP.[3] Conversely, Amazon, in many ways, does not have as selfless a mission to stand behind as a

firm such as Tesla, but it has better embraced other tenets of the EVP that balance employee growth and mission, which allows Amazon to retain talent long-term.

The 2023 *National Intelligence Strategy's* (NIS) primary goal of positioning the IC for intensifying strategic competition cannot be accomplished without also fulfilling the NIS's stated objective of recruiting, developing, and retaining a talented and diverse workforce.[4] In order to succeed, senior leaders of the IC must embrace some basic but also transformative approaches to develop the IC around a value proposition that supports the ambitions laid out in the NIS.

Gary Yukl, in *Leadership in Organizations*, makes it clear that strategic leadership requires top executives to monitor an organization's external environment and formulate a competitive strategy around those findings.[5] Using external monitoring or environmental scanning, senior leaders within the IC are able to survey the current talent recruitment and retention challenges their organizations face and then use private industries' best practices, in the form of effective EVP practices, as a source of relevant information to develop their own strategies to competitively compete for those finite resources—people.

The type of change required to affect this level of change within the IC certainly cannot be described in any other way than transformational. It requires fresh and innovative approaches to how organizations manage, direct, and employ their resources. As John Kotter points out in *Leading Change*, prior attempts to implement these changes have failed because managers often have taken an event-based approach to their implementation, which is nearsighted, rather than embracing these changes as a continuing process over time.[6] The IC must spearhead a whole government approach to tackle this tough problem by recognizing that the time to act is now, given the increasing pace of global competition.

In the IC, implementing a comprehensive EVP akin to that of a successful technology firm necessitates a strategic and deliberate adaptation to the IC's distinctive operating environment and mission. It must leverage a blended EVP that addresses a broad spectrum of areas that appeal to the multifaceted workforce that makes up the IC and which uniquely demands different values from their employer.

At its core, the IC already offers a powerful calling to fulfill its members' meaning and purpose through its vital mission to the nation. This focus must be renewed and refashioned to align with the IC's mission-centric ethos, offering employees a job and a calling to serve national security interests. The IC must trim the fat out of its bureaucratic processes, additional duties, and requirements that distract and degrade from its primary mission of protecting the American people. Often, IC employees are distracted from the core mission – protecting the American people – by the burden of work outside the scope of their core functions that fall under administrative requirements. The essence of this practice is to balance competitive compensation with intrinsic rewards such as recognition for service, thereby creating a compelling narrative of duty and honor that resonates with intelligence personnel.

The EVP tailored for the IC would emphasize a suite of benefits that address its workforce's professional and personal needs. Government employment and, by extension, the IC, have developed a reputation for their substandard working environment when compared to private sector alternatives. This includes endless windowless hallways within dated infrastructure, well-worn office furnishings, and outdated technology that has more profound implications on the workforce than just a suboptimal atmosphere. A comfortable and inviting work environment that employees look forward to visiting to engage in their work is critical to overall job satisfaction and meeting employees' psychological needs.[7] IC employees may not expect to find the most exquisite of amenities, such as those provided by top private firms such as Google and Meta, but they should be able to expect a modern, updated, and conducive environment in which to spend their workday. The IC must offer its workforce an environment that is not only conducive to its work but also excites it to come to work and contribute to its mission.

Flexibility within the IC's EVP must be reinterpreted to balance the need to fit the security constraints inherent to intelligence work with employees' needs. While remote work may not be broadly feasible, alternative forms of work arrangement, such as flexible hours or compressed workweeks, should be explored to provide an enhanced degree of work-life balance.[8] The U.S. Bureau of Labor Statistics has reported that with the rise of remote work since the pandemic, overall job turnover has been lowered, and overall job satisfaction has risen. At the same time, overall productivity also increased across almost all industries by embracing remote work.[9] A recent analysis by Deloitte reveals that more federal agencies are adopting hybrid models, recognizing both the logistical and mental benefits to employees' benefit and their performance in the workplace[10]. Deloitte's findings indicate that hybrid work enhances productivity, promotes healthier work-life balance, and offers a more attractive prospect for prospective employees who are considering multiple career options. The IC cannot ignore these trends if it intends to attract, retain, and maintain a workforce that is both resilient and committed to its mission.

The IC's capacity to fulfill its mission is inextricably linked to its ability to recruit and retain a skilled workforce. The IC can enhance its talent management strategies by adopting a tailored EVP framework

inspired by successful private sector practices. This adaptation not only promises a more engaged and committed workforce but also ensures the IC's agility and preparedness in the face of evolving global threats. It is through such strategic human capital initiatives that the IC can maintain its edge and continue to safeguard national interests.

NOTES

[1] "DoD Decades behind Private Sector in Recruiting Talent for Civilian Jobs, Study Finds," *Federal News Network*, March 20, 2023, https://federalnewsnetwork.com/defense-news/2023/03/dod-decades-behind-private-sector-in-recruiting-talent-for-civilian-jobs-study-finds/.

[2] Mark Mortensen and Amy C. Edmondson, "Rethink Your Employee Value Proposition," *Harvard Business Review*, January 1, 2023, https://hbr.org/2023/01/rethink-your-employee-value-proposition.

[3] Bryan Adams, "Make Your Employer Brand Stand Out in the Talent Marketplace," *Harvard Business Review*, February 8, 2022, https://hbr.org/2022/02/make-your-employer-brand-stand-out-in-the-talent-marketplace.

[4] Director of National Intelligence, *National Intelligence Strategy* (Washington DC: Office of the Director of National Intelligence, 2023).

[5] Gary Yukl, *Leadership in Organizations - Strategic Leadership by Executives*, Seventh Ed, 1981.

[6] John P. Kotter, "Leading Change: Why Transformation Efforts Fail," *Harvard Business Review*, January 2007.

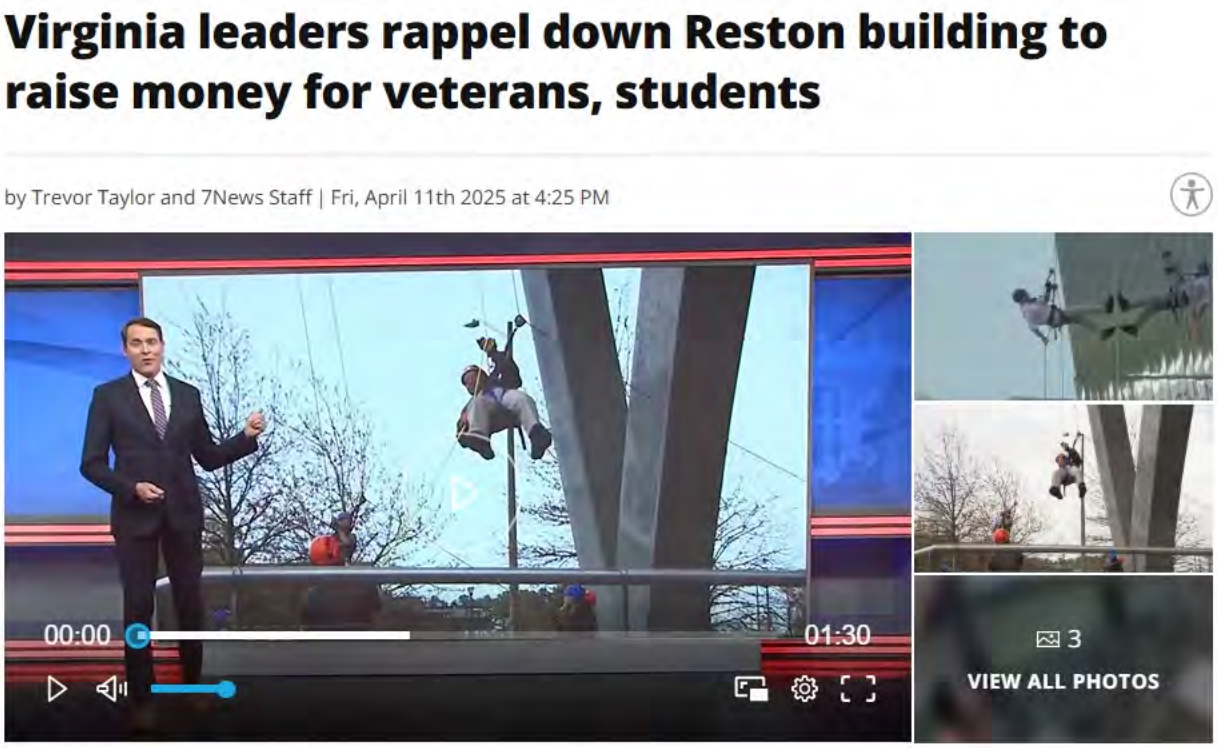
[7] Francisco Reyne-Pugh et al., "Assessing the Impact of the Physical Environment on Comfort and Job Satisfaction in Offices" (arXiv, January 13, 2020), https://doi.org/10.48550/arXiv.2001.04562.January 13, 2020

[8] "Intelligence After Next: The Future of the IC Workplace," 2020.

[9] Sabrina Wuff Pabilonia and Jill Janocha, "The Rise in Remote Work since the Pandemic and Its Impact on Productivity," *Bureau of Labor Statistics* 13, no. 8 (October 2024), https://www.bls.gov/opub/btn/volume-13/remote-work-productivity.htm.

[10] "Activating the Future of Workplace," *Deloitte Insights*, accessed October 31, 2024, https://www2.deloitte.com/us/en/insights/focus/human-capital-trends/2023/future-workplace-trends.html.

NMIF in the News



Virginia leaders rappel down Reston building to raise money for veterans, students

CLICK PHOTO TO VISIT SITE

Using Industry Analysis for Strategic Intelligence Insights: A PEST Analysis of Long Duration Energy Storage in Europe

by **Eitan Jay Sayag and Anne B.**

Just as industries must respond to changing competitive environments, so does the profession of intelligence. Intelligence theorists could turn to business literature for innovative techniques and perspectives. We examine the value of industry analysis for strategic intelligence. Applying an industry analysis to the case of long-duration energy storage delivers three findings. First, this industry analysis could not comprehensively answer typical strategic intelligence questions. Second, this analysis was effective for generating indicators towards intelligence topics. Finally, this study shows how analysis of critical private sector industries could benefit strategic intelligence when paired with context from traditional intelligence analysis.

INDUSTRY ANALYSIS AND INTELLIGENCE ANALYSIS

Although emerging technologies impact national security, much of technological development occurs outside government control. To better understand the private sector, the Intelligence Community (IC) might incorporate lessons from industry into professional development. This article examines the value of industry analysis for strategic intelligence insights. It conducts a case study using the external environment analysis model, known as PEST (political, economic, social, and technological), on the nascent long duration energy storage (LDES) industry in Europe. Based on open-source government and private sector publications, the PEST analysis showed that the overall environment for long-duration energy storage in Europe is currently unfavorable, but government interventions and further technological development could make it more favorable in the medium term.

This PEST analysis is then evaluated against three strategic intelligence questions generated from a review of IC and national strategy publications to assess its utility for strategic intelligence insights. The study found that a single, high-level PEST analysis was not sufficient to answer typical strategic intelligence questions and was better for generating indicators of broader trends. Analysis of critical private sector industries would be more beneficial for strategic intelligence when paired with additional context from traditional intelligence analysis on governments and societal trends.

The next section considers existing perspectives on intelligence analysis, showing an opening for industry analysis. That section is followed by a description of the case study. We then present a high-level PEST analysis and subsequently apply it to a hypothetical intelligence analysis. The final section concludes.

STRATEGIC INTELLIGENCE AND INDUSTRY ANALYSIS

Over the past quarter century, the practice of strategic intelligence has not evolved as quickly as has the global environment. While transnational crime and terrorism have compelled profound organizational change in the intelligence community, much of strategic intelligence continues to focus on countries and governments. This leaves potential blind spots where governments do not control developments in the threat landscape. In particular, various disruptive scientific and technical (S&T) developments have moved away from the government domain. Existing literature in the field of intelligence studies reveals a gap in methods to adapt to emerging S&T. For instance, Michael Warner, in his review of the various attempts to define intelligence, offers "Intelligence is secret, state activity to understand or influence foreign entities."[1] Yet, an exclusive focus on "secret" and "foreign" would distract the IC from staying abreast of technological developments that emerge domestically or in open scientific dialogue. Richard Heuer, Thomas Fingar, and Katherine and Randolph Pherson offer a practitioner's perspective, but tend to focus on the art of analysis or on customer focus.[2]

While such advice fully applies to S&T intelligence, it offers little practical advice on how to frame technological developments, prioritize collections, or understand interactions among non-government entities. R.V.

Jones, considered the father of Science and Technology Intelligence (S&TI), provided the framework for much of the IC's approach. Jones believed science and technology were key to understanding the development of new and existing weapons, as well as misleading enemies about their weapons. S&TI could also assist technically in espionage and counter-espionage.[3] However, Jones' framework does not consider key sub-topics of S&TI: non-military technologies and non-adversary partner countries.

As a result, in order to advise on strategy involving critical technologies, the IC frequently turns to industry experts. But how can the IC improve its relationship with industry, and what can inform the IC's questions? In the business literature, industry analysis reviews market conditions that influence an industry's development. Chuck Howe argues intelligence analysts can use these business tools to "develop strategic intelligence insights."[4] In 2015, he argued the then-*National Intelligence Strategy* did not push the IC enough out of the traditional political-military sphere, and that the IC needs to understand the development of industrial capability in other nations. Industry analysis helps a business understand the competitive environment within its industry.

One of the most common types of industry analysis is Porter's Five Forces, named after Michael Porter, who pioneered the field. It focuses on a handful of factors within an industry: threat of new entrants, bargaining power of buyers, bargaining power of suppliers, threat of substitutes, and rivalry among existing competitors.[5] This model allows an analyst in an existing industry to better understand how a single company is situated within that industry. Another common model is the External Environment Model, which focuses on outside factors that shape an overall industry. This model can consider various factors, typically political, economic, social, and technological (PEST), but may also consider others, such as environmental (STEEP) and legal (PESTLE).[6] Although Howe succeeds in arguing that industry analysis can benefit strategic analysis, he limits its utility to an industry that is "mature, global, and has a large presence in the region or country" of interest.[7] Hence, Howe does not explore how this industry analysis would work for strategic intelligence in a nascent industry, such as emerging technology.

CASE STUDY METHODOLOGY

To expand on the literature, this article applied the PEST model to the case of a nascent industry: long-duration energy storage (LDES) in Europe. The PEST model offers a basic and high-level structure, sufficient for considering industry analysis for an emerging technology. For firms within the industry, more intense detail would apply, but this article surveys the elements of PEST at a higher level.

The choice of LDES for a case study stems from its innovation, its importance, and its ability to illustrate the elements of PEST. LDES depends on technological innovation and has become increasingly important for energy networks in diversifying sources of energy. Energy production supports nations' military and industrial capabilities but lies at an earlier part of the value chain, less examined by intelligence, presenting an opportunity for an initial study of a case. While industries and governments seek to decarbonize, LDES demonstrates the practical complications in pursuing green initiatives. As such, political and social elements provide motivating forces for advancing LDES, but economic and technical elements impede.

For the United States, strategic intelligence has an outward focus, making domestic innovation a poor case study for exploring industry analysis. LDES is also evolving in China, but information there is limited on the various factors of PEST. Europe presents a region with social support for decarbonization, as well as a strategic need to diversify energy sources. Sophisticated S&T also make this region attractive for study.

To assess how well PEST analysis is suited for strategic intelligence in a government context, this article will first conduct a high-level PEST analysis of LDES. We then apply that analysis to three hypothetical strategic intelligence questions. These questions are intended to mimic typical questions presented to intelligence analysts from policy makers who may have less technical knowledge of a subject.

1. How capable is Europe of achieving energy security and independence following Russia's invasion of Ukraine and resulting gas and oil shortages?
2. How will the transition away from reliable fuels impact Europe economically?
3. Is Europe on track to meet its net-zero pledges?

This research is bounded by open-source industry, government, media, and academic documents. The European Commission is one of the most valuable sources of information on this topic. Specific sources from the European Commission included industry and climate legislation, studies reviewing the impact of European

Union (EU) industrial policies, surveys of EU citizens, and publications on EU research programs. Information from the U.S. Department of Energy and the International Energy Association also prove valuable in providing general context for the state of the industry in Europe.

PEST ANALYSIS

Defining LDES

The U.S. Department of Energy defines long duration energy storage as grid-scale energy storage that can deliver 10+ hours of duration.[8] LDES is necessary because utilities have the difficult task of balancing supply and demand on the electrical grid at all times. Because demand is relatively inelastic, utilities keep that equilibrium by controlling the supply side, supplying more electricity during times of peak demand, such as in a hot summer evening, and less during times of low demand, such as in the middle of the night when people are sleeping. Ahead of peaks, plants fire up generators to dispatch additional electricity. But the grid is complex, and some electricity sources are not easily dispatchable. Solar and wind power are dependent on the weather, and utilities cannot ramp up additional solar power to meet short term demand surges or cover short-term supply shortages. Currently, the grid remains dependent on firm, dispatchable energy generated from coal and natural gas combustion.[9]

Political

Although the political environment for LDES across Europe is generally favorable, the LDES industry's reliance on political intervention to overcome other economic and technological barriers compels the industry to maintain close coordination with the EU and national governments. While different countries have different initiatives, this study highlights efforts of the EU.

In 2020, the European Commission approved the European Green Deal with 600 trillion euros to help the EU achieve net-zero emissions by 2050.[10] One piece of the legislation, the Net-Zero Industry Act calls out energy storage as one of the critical technologies.[11] Given the nascent stage of the technology, EU investment is currently focused on research and development (R&D) rather than deployment. The importance of the green transition remains evident even as governments begin to recognize the associated challenges to industrial productivity. In *A Competitiveness Compass for the EU* (2025), the European Commission acknowledges regulatory constraints on manufacturers, environmental regulations among them, but still places value on decarbonization.[12]

While there are several institutions involved in funding European R&D for energy technologies, Horizon Europe is the central research and development fund in Europe.[13] Horizon, describing itself as the EU's "key funding programme for research and innovation" is renewed every seven years in alignment with the EU's research priorities. This allows it to plan research and designate priorities years in advance. "Climate, Energy, & Mobility" is one of the top priorities of the 2021 to 2027 plan.

Horizon is designed to work in tandem with other EU funding programs. Breakthrough Energy Catalyst funds the deployment of emerging renewable energy technologies, including LDES.[14] The Catalyst's goal is explicitly designed to help nascent industries overcome market failures, recognizing that "without additional support, they will not get investments they need to scale."[15] For example, a challenge for LDES is LDES' uncompetitive price gap with traditional fuels due to high cost inputs and sub-scale technology, the nascency of the technology, which increases upfront capital costs, and the lack of commercial performance data, which affords limited visibility for traditional financiers.[16] Breakthrough Energy Catalyst complements Horizon with a specific reduced-emissions energy focus, highlighting the significant EU investment in developing this field.

Despite these investments, some argue that further government interventions are necessary to shift the market to incentivize LDES. Carston Helm and Mattias Mier determined the optimal policy intervention was to subsidize renewables rather than grid storage. Increasing renewables improves the value-proposition and the potential profitability of storage as a substitute for firm fossil fuel generation.[17] Subsidizing renewables attempts to build into the grid the need for energy storage, making it more profitable. In fact, the EU is already incentivizing renewable energy production.[18]

The scale of the problem likely means that both approaches are needed. While the EU political regime is favorable to LDES, its interventions will need to be significant to overcome the technological and economic challenges to enable its emissions goals.

Economic

The economic segment of LDES is currently unfavorable for the industry, although technological advancement and political intervention may make LDES economically viable in the medium term. From a strategic intelligence perspective, the economic segment of PEST analysis in particular reveals the current realities of the industry.

Electricity generators are diverse, such as natural gas power plants, coal-fired power plants, solar power plants, wind power plants, and hydropower dams. Each of these electricity generators has advantages and limitations, which is why no two sources can be a 1:1 substitute. Hydropower, for instance, has more price stability than coal power but is dependent on large natural water features like rivers. Utilities patch these different types of energy together to keep electricity demand and supply in constant balance, typically using natural gas. LDES could enter the market as a substitute for firm, dispatchable natural gas.[19] But a successful substitute for natural gas needs to be at least as cheap as natural gas. Unfortunately, current technology makes LDES more expensive per kilowatt hour (kWh) than natural gas power generation. Under free market conditions, LDES would not enter the market absent shifts that bring natural gas price significantly higher, or technological changes that lower the cost of LDES.

In 2021, Nester Sepulveda, et al, looked at the price comparison of different forms of LDES and found that no current LDES technology is capable of replacing natural gas. LDES can begin to replace some natural gas generation at a cost of $20 or less per kWh and needs to be $1 or less to displace all firm low carbon generation. To give a sense of the scale of the problem, vanadium redox flow batteries, one of the more promising LDES battery chemistries, had an energy capacity cost ranging from $40 to $200 per kWh. The study found that replacing all firm dispatchable energy "requires performance combinations unlikely to be feasible with known LDES technologies."[20]

Even if private investment in the free market could develop LDES, expansion to the level that is socially optimal could take longer than a decade—the goal of many governments and climate modelers. Market forces alone cannot overcome the high costs of R&D and fixed investment because LDES competes in an industry that already has a low-cost technology in natural gas. Additionally, LDES requires an industry with much higher levels of renewables. Just as LDES enables ramping up intermittent renewables, high levels of renewables increase the potential profitability of LDES. These complementary technologies depend on one another to succeed.[21] Without each other, these technologies will be limited and outpriced, a chicken-and-egg problem.

Social

The social environment varies across Europe but can be generally characterized as favorable as long as LDES deployment does not lead to steep energy price increases for the consumer. For intelligence analysts, reviewing the social segment of the external environment for LDES can inform them that although social inclinations favors the energy transition, European societies will not overlook basic economics. Protests over fuel costs, for example, will constrain government regulatory requirements. If the economic and technological challenges were to make LDES price competitive with market alternatives, social dynamics would be favorable for LDES deployment and uptake.

The social impact on LDES can be viewed from three different perspectives: views on climate change, social consumption of energy, and views on nuclear power. Most obviously, the favorable social segment is tied to LDES' role in addressing the climate. According to a 2023 poll, 93 percent of EU citizens believe the climate is a serious problem and 88 percent agree that greenhouse gas emissions should be reduced to make the EU climate neutral by 2050. In responding to national security needs, 58 percent of EU citizens believe the EU should accelerate the transition to a green economy in view of the energy crisis triggered by Russia's invasion of Ukraine.[22] However, despite this large majority supporting climate action, another poll showed respondents were much less willing to make lifestyle changes to address climate change. Only a minority in the European countries surveyed were willing to personally cover the cost of making homes more energy efficient or pay fees to offset emissions from airline flights.[23]

Energy consumption patterns also create an opportunity for LDES. Social behaviors over the course of a day mean that electricity demand is not static. Energy consumption is traditionally highest in the evening hours when people typically return home from work, turn on lights, cook dinner, and watch television. This daily consumption peak has been anticipated and easily met by increasing electricity generation. However, as solar panels have proliferated, daily fluctuations in production have greatly increased.[24] During the middle of the day, electricity from solar panels is at its peak, meaning utilities need little dispatchable energy, sometimes even leading to grid oversaturation. High amounts of solar generation during the day mean low levels of other electricity sources during that time, which creates a steep ramp-up of other electricity sources in the evening, a technological challenge for fossil fuel generation.[25] The increase of renewables on the grid thus creates a natural opening for LDES to meet the challenge of societal electricity demands.

As a third social influence, disdain for nuclear power presents a positive element for LDES. Nuclear energy is seen by many people as risky and societal dynamics disfavor it as an energy source. For example, Germany received 25 percent of its power from nuclear in 2011 but shuttered its last nuclear power plant in 2023.[26] Other potential emerging technologies, such as fusion power, could offer safe, carbon-free, dispatchable energy. However, those technologies are even further away from viability than pairing renewables with LDES.

Despite these positive social forces, the social environment challenges LDES in two key areas: price and demand. While consumers may want green energy, they do not want to pay more for it. The 2018 yellow vest protest in France, a response to rising fuel costs and a green tax, demonstrated how the social segment can limit the energy transition.[27] Additionally, consumer demand for energy is not easily adjustable. A "smart grid" might envision changes such as running the dishwasher during periods of low demand, but consumers are not going to turn off lights or TVs at night absent extreme price pressures. Hence, utilities needing to control the supply side, will not transition to more expensive technologies without regulatory requirements. LDES is currently significantly more expensive than natural gas power. For utilities to truly scale up LDES as a substitute to dispatchable fossil fuels, the technology needs to be capable of meeting demand during extended periods of still wind or cloudy skies.

Technological

Of the four PEST segments, the technological segment of LDES is arguably the industry's largest challenge. Current battery technology is inadequate for efficient grid storage. Short-term grid-scale energy storage allows utilities to store excess solar and wind generation to cover short-term, minute-to-minute fluctuations as well as ease the steep ramp-ups of fossil fuels for the high net load in evenings. Lithium-ion batteries are currently deployed for short-term term grid-fluctuations and work well up to about 4-6 hours of need. This short-term storage suffices to support wind, solar, and hydro-power contributions to the grid for the majority of the time. However, utilities need to provide electricity even at times of peak demand and potentially narrow supply. To meet potential several-day shortages, the electricity grid must have a long-term dispatchable power source. LDES that could provide 10 to more than 100 hours of energy storage does not yet exist in the market. LDES is not a single technology but rather a need that dozens of different technologies could meet (see Table 1).

Potential Grid-Scale Energy Storage Technologies		
Lithium-ion batteries	Reciprocating heat pump energy storage	Zinc-air batteries
Iron-Air batteries	Firebrick resistance-heated storage	Potassium-ion batteries
Pumped hydro storage	Power-H2-power storage	Dual-ion batteries
Compressed air energy storage	Power-syngas-power storage	Lithium iron phosphate batteries
Aqueous batteries	Sodium-ion batteries	Gravity energy storage
Redox-Flow batteries	Aluminum-ion batteries	Liquid air battery
Multijunction photovoltaic thermal storage	Aluminum-air batteries	
Molten Salt batteries	Flywheels	

Table 1: Selected Energy Storage Technologies

In 2021 Ma et al. reviewed different battery technologies and assessed that the most common battery technology of the past two decades—lithium-ion batteries—has been pushed to their limits and has "been found wanting in terms of delivering competitive large-scale devices."[28] They identified three battery types as better fits for grid-scale energy storage: Sodium-ion batteries, aluminium-ion batteries, and flow batteries. Sodium-ion batteries are "competitive in the future grid-scale energy-storage market" and have a "unique market superiority to" lithium-ion batteries because of the abundance of sodium. Sodium-ion batteries also have similar chemical characteristics with lithium.[29] Although proven in lab settings, sodium-ion batteries will take time before they are ready for practical, large-scale commercial applications. Rechargeable aluminium-ion batteries, are low-cost and have high energy density, making them good fits for grid-scale energy storage; however, current cathode designs for these are expensive and not practical at scale.

The furthest along of these three battery types is flow battery energy-storage, such as vanadium flow state batteries and zinc flow-state batteries. These technologies show some potential in industrial applications but are still primarily in the demonstration stage.[30] China, which has been investing heavily in grid-scale battery storage, brought the world's largest vanadium flow state battery storage system online in 2022 with plans to expand.[31] Unfortunately for the United States, most vanadium is mined in China and Russia.[32]

One technology that may have the potential to compete at cost is an air-iron battery, in development by a Massachusetts-based company. Form Energy's Iron-Air battery works through a process involving rust. When discharging, the battery allows oxygen to rust the iron, releasing electrons. The battery charges through the reverse process, where electrical currents convert the rust back to iron and the battery releases oxygen. Iron-air batteries have the potential to be built at one tenth the cost of a Lithium-ion battery.[33] If the company's demonstration projects continue to prove successful, it will allow for 100+ hours of storage, potentially providing the missing piece for full decarbonization of the electrical grid.

However, all of these potential technologies require further development. Incentives are needed to bring down the costs and make these technologies scalable, all while finding a market for them. Although not currently cheap enough to compete with dispatchable fossil fuels, promising technological advancements are likely to become viable in the medium term, especially with governmental support.

PEST FOR STRATEGIC INTELLIGENCE ANALYSIS

The PEST model was designed to understand the environment for an industry, not for strategic intelligence analysis. But this article seeks to explore how an industry perspective could support strategic intelligence. With the preceding PEST analysis in mind, we now turn to typical intelligence questions. We find that a PEST analysis cannot fully answer the test questions raised, although it may contribute to a broader understanding. A PEST analysis offers a useful, high-level introduction to LDES for intelligence analysts needing breadth of awareness, if not detailed knowledge. However, PEST analysis may be most useful in developing indicators for strategic analysis.

Strategic Intelligence Question 1*: How capable is Europe of achieving energy security and independence following Russia's invasion of Ukraine and resulting gas and oil shortages?*

PEST helps answer this question by explaining the current status of technologies necessary to European energy independence; however, it is not able to answer the question in its entirety. LDES is just one of the several potential technologies that are necessary to secure European energy security. PEST analysis on oil and gas industries in Europe would also be necessary to answer this question.

Energy security also requires understanding supply chains and geopolitical trends and economic connectivity with other countries. Even if the EU is not importing oil or gas, if the battery supply chain is dependent on China, it will not have true energy security. Europe will still be reliant on imports for raw minerals or even finished products like photovoltaic panels. None of this information would be factored into a PEST analysis of LDES. Additionally, energy independence and security require overall political will. If Europe is theoretically capable of achieving energy independence, politicians need to actively pursue it. Learning European leaders' motivations is better served through traditional strategic analytic methods like leadership profiles than through industry analysis.

Strategic Intelligence Question 2: *How will the transition away from reliable fuels impact Europe economically?*

Although this question is broad, it reflects the type of tasking that analysts receive based on national security priorities like economic security. An individual PEST analysis, like the one above for LDES, does not add much to this particular question because there are too many other contingent factors left unaddressed. If a European company develops a critical technology, such as LDES, that the rest of the world wants, that company would stand to reap significant economic benefits. European countries may choose to make clean energy a key component of industrial policy, and significant investment in LDES technology may help achieve that. At the same time, there are several clean energy technologies, including long-shot technologies, such as fusion energy, that may eventually make LDES obsolete.

PEST may play a useful role if an analyst can use the framework to analyze several different clean energy technologies in several different regions. However, these PEST analyses would have to consider not only government policies in the specific region but also across regions. U.S. and Chinese trade policies may keep Europe from benefitting from its technological developments, in the same way as "dumping" of cheap solar panels led to Chinese economic benefits despite the technology's development in the United States. Finally, answering this question requires not just looking at the myriad technologies in the clean energy space across regions, but also considering whether clean energy will take off at all. PEST can help understand how an industry or industries develop in a region, but whether the economic benefits reach those countries necessitates an examination of the comparative advantage and policies of trading partners. Though PEST analysis may contribute to a broader analysis of this question, PEST is not well-suited to single-handedly answer overly broad questions like this one. This offers a good example for scoping the utility of PEST for strategic analysis.

Strategic Intelligence Question 3: *Is Europe on track to meet its net-zero pledges?*

PEST analysis can help answer this question in the negative. That is, it can help inform whether Europe is not on track to meet its pledges because a critical industry is not yet mature. However, it cannot answer this strategic intelligence question in the affirmative because there are several more industries and political factors that are necessary to determine whether Europe is on track to meet its emissions commitments. For example, the EU is planning to achieve a reduction of its emissions 55 percent by 2030 compared to 1990 levels. As of 2023, the EU has managed to reduce its emissions by 37 percent.[34] PEST analysis shows that LDES is unlikely to be fully scalable by 2030, which requires the EU to reduce emissions by another 20 percent without that technology. Other technologies might make a 55 percent reduction possible in the next five years, but net-zero is not achievable absent a fully mature LDES industry or some other technological innovation, and the region will likely push against the limits of technology in pursuing a 55 percent reduction by 2030.

To affirmatively answer this question, strategic intelligence analysts would need information on all sectors, not just the energy sector, which is just one of the sectors contributing to greenhouse gas emissions. Emissions monitoring through satellite imagery may be more effective than industry analysis for monitoring foreign emissions levels. Additionally, a deeper review of economic policies and regulations across industries would be necessary to predict future progress on meeting emissions goals.

Using PEST for Indicators

PEST may be most useful for generating indicators of broader strategic intelligence trends. Through Structured Analytical Techniques, intelligence analysts generate lists of potential "observable phenomena ... to help track events, spot emerging trends, and warn of unanticipated changes."[35] These can both be used at the analytical level and for customers in trying to explain the current trajectory of an event (e.g., indicators of a possible invasion by an aggressor nation against a neighbor).

By isolating interconnected factors on a specific technology, the IC can use PEST to generate specific indicators for strategic questions. We can test this using Strategic intelligence question 1: *How capable is Europe of achieving energy security and independence following Russia's invasion of Ukraine and resulting gas and oil shortages?*

Assuming Europe does not develop significant indigenous sources of natural gas and oil, the region will depend on renewable energy sources for power generation. Social constraints around nuclear power use in parts of Europe, like Germany, would almost certainly require an increased use of solar, hydro, and wind power. With the subsequent power intermittency, grid battery storage would be a linchpin technology, key to determining energy security and independence.

Political	• High funding levels for LDES R&D • Subsidies for LDES • Subsidies for renewable energy • Reductions in natural gas imports from Russia
Economic	• Reduced price per kWh from LDES • Stabilization of peak energy prices • Reduced marginal cost ratio between LDES and natural gas
Social	• Social willingness to pay higher energy prices as measured by polls • Public support for addressing climate change as measured by polls • Number or intensity of protests against energy price increases
Technological	• Number of new demonstration projects • Number or amount of funding for LDES systems or R&D • Proof of new LDES capabilities (e.g., patents) • Number of research publications on LDES

Table 2: LDES PEST-Inspired Indicators

Table 2 displays indicators that emerge from this PEST analysis. Political indicators include high funding levels for LDES research and development, increased subsidies for both LDES and renewables, and additional pressures from Russia on nat - ural gas imports. Economic factors include reduced price per kWh of LDES, stabilization of peak energy prices, and a change in the marginal cost curve for LDES rela - tive to natural gas. Social indicators include polling on willingness to pay higher energy prices, public support for addressing climate change, and protests for or against European energy policies. Technological indicators are the number of new demonstration projects, the number of funded LDES systems, proof of new technological capabilities, and a number of research publications on grid-scale batteries. The extent to which each of these observable phenomena is present will help analysts and customers understand how far along Europe is in achieving energy independence. These more detailed indicators, coming from an industry perspective, are unlikely to emerge from more traditional intelligence approaches to answering this strategic intelligence question. In this way, PEST can serve as a useful tool for intelligence analysts to conduct a deeper dive into a strategic intelligence question.

CONCLUSION

This article sought to evaluate the utility of PEST analysis for strategic intelligence insights in a nascent industry. Although PEST helps understand the current technological and economic challenges of the Long Duration Energy Storage market in Europe, industry analysis needs to be paired with more traditional intelligence to answer broad strategic intelligence questions. However, this study finds that industry analysis can contribute to answering strategic intelligence questions in more focused ways. PEST's most direct utility is identifying detailed and specific intelligence indicators.

Understanding the developmental milestones for linchpin technologies can help analysts monitor progress over broader strategic trends. Although on its own, an individual PEST analysis will not yield a complete answer to most strategic intelligence questions, it can contribute to answering some strategic intelligence questions and can help analysts think through the necessary factors for further development of key technologies. Although it will not benefit all, or even most, questions the IC confronts, industry analysis has utility for strategic intelligence when leveraged on specific topic sets.

NOTES

[1] Michael Warner, "Wanted: A Definition of Intelligence," *Studies in Intelligence* 46, no. 3 (2007): 15-22, 21.

[2] Richards J. Heuer, *Psychology of Intelligence Analysis* (Washington, DC: Central Intelligence Agency, 1999); Thomas Fingar, *Reducing Uncertainty: Intelligence Analysis and National Security* (Stanford, CA: Stanford University Press, 2011); Katherine Hibbs Pherson and Randolph H. Pherson, *Critical Thinking for Strategic Intelligence*, 2d ed. (Los Ángeles: CQ Press, 2017).

[3] R.V. Jones, *Most Secret War*: *British Scientific Intelligence, 1939-1945* (London: Hamish Hamilton, 1978).

[4] Chuck Howe, *Using Industry Analysis for Strategic Intelligence* (Washington, DC: National Intelligence Press, 2015).

[5] Michael E. Porter, *Competitive Strategy: Techniques for Analyzing Industries and Competitors* (New York: Free Press, 1980).

[6] Craig S. Fleisher and Babette E. Bensoussan, *Business and Competitive Analysis.* (Upper Saddle River, NJ: FT Press, 2007).

[7] Howe, *Using Industry Analysis for Strategic Analysis*, 21.

[8] U.S. Dept of Energy, *Long Duration Storage Shot*, DOE/EE-2384, (July 2021), paragraph 1.

[9] David Roberts, What? The sun isn't always shining?!" *Volts,* November 1, 2023, paragraph 17.

[10] European Commission, *The European Green Deal,* paragraph 2, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal_en, accessed February 23, 2025.

[11] European Commission, *Net-Zero Industry Act,* paragraph 5, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal/green-deal-industrial-plan/net-zero-industry-act_en, accessed February 3, 2024.

[12] European Commission, *A Competitiveness Compass for the EU, Brussels,* (January 29, 2025), 1-2.

[13] European Commission, *Horizon Europe: The EU Research and Innovation Programme 2021-2027.* (March 19, 2021), accessed March 15, 2025, 3, https://research-and-innovation.ec.europa.eu/document/download/9224c3b4-f529-4b48-b21b-879c442002a2_en?-filename=ec_rtd_he-investing-to-shape-our-future.pdf.

[14] Breakthrough Energy Catalyst, "Our Work," accessed February 23, 2025. https://breakthroughenergy.org/our-work/catalyst, paragraph 3.

[15] European Commission, Innovation Fund Expert Group, *Breakthrough Energy Catalyst Foundation* (July 6, 2021), 7.

[16] European Commission, Innovation Fund Expert Group, *Breakthrough Energy Catalyst Foundation,* 7.

[17] Carsten Helm and Matthias Mie, "Steering the Energy Transition in a World of Intermittent Electricity Supply: Optimal Subsidies and Taxes for Renewables and Storage," *Journal of Environmental Economics and Management* 109 (2021): 1-3.

[18] European Commission, *2024 Report on Energy Subsidies in the EU* (January 28, 2025) 1.

[19] David Roberts, "What? The sun isn't always shining?!" *Volts,* November 1, 2023, paragraph 31.

[20] Nestor A. Sepulveda, et al. "The Design Space for Long-Duration Energy Storage in Decarbonized Power Systems," *Nature Energy* 6, no. 5 (2021)*: 506–51*1.

[21] Helm and Mier, "Steering the Energy Transition," 1-3.

[22] European Commission, "Citizen Support for Climate Action," (2023), paragraphs 2-4, https://climate.ec.europa.eu/citizens/citi-zen-support-climate-action_en accessed March 15, 2025

[23] Jon Henley, "Many Europeans want climate action – but less so if it changes their lifestyle, shows poll," The Guardian, May 2, 2023, paragraphs 12-17.

[24] Julien Jomaux, "The Emergence of Duck Curves in Europe," *GEM Energy Analytics,* February 26, 2024, paragraph 5.

[25] Institute for Energy Research, *Solar Energy's Duck Curve,* paragraph 1, https://www.instituteforenergyresearch.org/solar-energys-duck-curve/, accessed March 15, 2025.

[26] World Nuclear Association. "Nuclear Power in Germany," July 8, 2024, paragraph 8, accessed March 15, 2025.

[27] Jake, Cigainero, "Who are France's Yellow Vest Protesters, and What Do They Want?" National Public Radio, December 3, 2018, paragraph 3.

[28] Jianmin Ma, et al., "The 2021 Battery Technology Roadmap," *Journal of Physics D: Applied Physics* 54, no. 18 (2021)*:* 7.

[29] Ma, et al, "The 2021 Battery Technology Roadmap," 18.

[30] Ma, et al, "The 2021 Battery Technology Roadmap," 31.

[31] Andy Colthorpe, "Energy Storage Industry Hails 'Transformational' Inflation Reduction Act," *Energy Storage News,* August 17, 2022, paragraphs 1-2.

[32] Report Linker, "Top Vanadium Producing Countries," *paragraph 1,* https://www.reportlinker.com/dataset/0a4393104ed6555d1df255a-7b822ae9de50a8a97, accessed March 15, 2025.

[33] Scott J. Mulligan, "2024 Climate Tech Companies to Watch: Form Energy and its Iron Air Batteries," *MIT Technology Review,* October 1, 2024, paragraphs 2-4.

[34] European Commission, "Progress made in cutting emissions," paragraph 1, https://climate.ec.europa.eu/eu-action/climate-strategies-targets/progress-made-cutting-emissions_en.

[35] Stephen Artner, S. Girven, and James B. Bruce, *Assessing the Value of Structured Analytic Techniques in the U.S. Intelligence Community* (Santa Monica, CA: RAND Corporation, 2017)*,* 2.

Eitan Jay Sayag is an Intelligence Analyst at the Federal Bureau of Investigation and graduated with a Master of Science and Technology Intelligence from National Intelligence University in 2024. The co-author is active in the field of intelligence studies. *The authors wish to thank Dr. Michael MacLachlan for technical advice, Robin Lobb, John Robinson, Giangiuseppe Pili, other members of the IAFIE "*Bearpit*," and Stephen Marrin for helpful review of this research.*

Space Power and Party: China's Ambitions to Conquer the Next Domain

by **Abiel Alvarenga and Carlos Alatorre**

As China becomes more technologically advanced, its focus on space will undoubtedly increase. China has, however, a long way to go to catch up with the United States. Internal turmoil throughout its bureaucracy sets back any ambitions in its grand strategy and may stop Chinese leaders from advancing as fast as they would like. Nonetheless, China possesses sufficient potent capabilities to disrupt U.S. space operations. China will continue to use gray-zone tactics throughout all domains as long as Xi Jinping is its leader. The United States must be resilient in response to attempts to thwart space operations and innovation. The United States can mitigate against Chinese efforts by incentivizing private industry to expand efforts to focus on space and reframe the U.S. position in international institutions.

XI'S AMBITION TO DOMINATE SPACE

Decades ago, few could have predicted China's rise to its current level. Cooperation with the West has allowed China to flourish, but as it grows as a global hegemon, the Chinese Communist Party (CCP) seems to favor hostility in its approach to the West. The most significant changes occurred at the 18th Party Congress when Xi Jinping became the party leader, and the 20th Party Congress when he stayed in position past the traditional 10 years and cemented his factions in the Politburo.[1]

This change in tradition raises long-term questions about the future of U.S.-China relations. This raises two questions: how is the CCP evolving and what is the primary plane for its competition against the United States? Broadly, we can say that leaders do not seek technology solely for consumer satisfaction, so there must be a greater aim. In reaching any of China's global objectives, Chinese leaders will require the most sophisticated technology for intelligence gathering. Space is growing its importance to contribute to the common domains of land, sea, and air domains.

Xi has placed an increased emphasis on space in recent years in comparison to previous years. Five of the thirteen new members from the 20th Party Congress come from the aerospace industry.[2] If the United States seeks to understand China's future with Xi Jinping as its lifetime leader, then there must be an understanding of where a 'space strategy' may lead to. To begin assessing a strategy, an analysis of personnel changes will be followed by the current state of China's space technology to understand its ideals and capabilities. Projections of strategy and tactics are then possible in this context.

PERSONNEL IS POLICY

Every personnel move shows the CCP's desire to promote technocrats and Xi Jinping's ambition to grow his legacy. Xi's "Tigers and Flies" anti-corruption campaign is widely covered and was expected to slow because he ousted old factions from previous leaders and established multiple factions of his own.[3] Despite the appearance of a lack of consensus within the CCP, their grand strategy has not deviated from 10 or 20 years ago. What has shifted are the methods or tactics (like gray zone) of reaching these goals as seen with each Party Congress.

We can see an ideological consensus clearly when observing Zhang Youxia's (Shaanxi faction) August 2024 article and Li Qiang's (Zhejiang faction) March 2025 work report. While they oversee very different tasks, both are consistent in emphasizing the goal of Chinese-style modernization "中国式现代化" by focusing on science and technology.[4] If there were a shift in power or vision, then there would be more inconsistent messaging about the country's direction, similar to Li Keqiang's last year as Premier.

Nonetheless, it is important to note that factional infighting is part of the system established by Xi Jinping. This is evidenced by the Politburo Standing Committee, each being of a different faction named after their origins with Xi: Li Qiang of Zhejiang, Cai Qi of Fujian, Zhao Leji of Shaanxi, Wang Huning and Ding Xuexiang of Shanghai, and Li Xi of Guandong. The only faction that is repeated is that of Shanghai, but Wang is the anomaly in this case because he is the only leftover from the time of Jiang Zemin, while Ding is the youngest of the six and a potential successor.[5] Competition among factions can be assumed

because each will naturally take advantage of opportunities to place themselves as successors to Xi with or without his will. Xi likely gains protection from a larger quantity of factions because it is less likely that they will coalesce to target him, which would create a vacuum.

Additionally, no conclusion can be drawn about who Xi trusts from one year to the next. The current turmoil in the People's Liberation Army (PLA) shows that individuals who were thought to be loyalists can be ousted as well. The supposed loyalists began to fall less than a year after the 20th Party Congress in October 2022, most prominently with Li Shangfu. These leadership changes throughout the PLA and military industry are in-line with the rise of technocrats (who are not definitively part of a certain faction like those in the Standing Committee) in the Politburo. **Figure 1**[6]

Given the CCP's focus is on growing its hegemony, the Politburo needed people other than career political administrators; therefore, it has been filled by technocrats. This includes Zhang Guoqing, one of the more prominent members of the Politburo because of his background in China's leading military contractor, Norinco, and currently supervises the State-owned Assets Supervision and Administration Commission of the State Council (SASAC).[7] In his role overseeing SASAC, he can advise the appointment of top executives for all state-owned enterprises (SOEs). This reaches down to essential industries for grand strategy, more specifically, the aerospace industry. To draw closely on the effect of leadership change in China, we can see the Aviation Industry Corporation of China (AVIC) and its recent change in the Chairman position.[8] Tan Ruisong was removed as Chairman of AVIC in March 2023 (a few months after the 20th Party Congress); after a year, they replaced him with Zhou Xinmin. In August 2024, the Central Commission for Discipline Inspection (CCDI) announced that Tan was being investigated for "severe violations of party discipline and the law".[9] Just as Xi picks his members of the Politburo, Zhang must oversee leadership in the defense industry. The preferred method of making changes is to do it in the name of anti-corruption.

Zhang Guoqing is only one of the many from the aerospace industry to gain prominent positions in the CCP. Others include Yuan Jiajun and Zhang Qingwei, both of whom held prominent roles in the China Aerospace Science and

Current and Ousted CCP/PLA Personnel			
Current		*Recently Ousted*	
Name	***Position***	***Name***	***Last Position***
Dong Jun	*Minister of National Defense*	**Li Shangfu**	*Minister of National Defense*
Wang Houbin	*Commander of PLA Rocket Force*	**Li Yuchao**	*Commander of PLA Rocket Force*
Yuan Jiajun	*Politburo member of CCP and Party Secretary of Chongqing*	**Liu Shiquan**	*Chairman and Party Secretary of Norinco*
Zhang Guoqing	*Politburo member of CCP and Vice Premier of China*	**Tan Ruisong**	*Chairman of Aviation Industry Corp of China (AVIC)*
Zhang Qingwei	*Vice Chairman of Standing Committee of National People's Congress*	**Wang Changqing**	*Senior Executive for China Aerospace Science and Industry Corporation (CASIC)*
Zhang Youxia	*Vice Chairman of Central Military Commission*	**Wei Fenghe**	*Minister of National Defense and State Councilor of China*
Zhou Xinmin	*Chairman and Party Secretary of Aviation Industry Corp of China (AVIC)*	**Wu Yangshen**	*Chairman and Party Secretary of China Aerospace Science and Technology Corporation (CASC)*

Figure 1: Current Key Officials. This list is "current" as of March 2025.

Technology Corporation (CASC). Of particular importance is Yuan, who led the Shenzhou missions (including the Shenzhou 5 which was China's first manned spacecraft mission) and was Vice President of the International Astronautical Federation (IAF). He likely had a connection to the ousted Li Shangfu because of their longtime involvement with Shenzhou missions, and Li's leadership of the China Manned Space Agency (CMSA) from 2017 to 2022 before becoming the defense minister.[10]

At minimum, medium confidence can be attributed to relationships between individuals in the PLA and military industry due to the nature of the work, though this doesn't imply the closeness of their connections, only that a working relationship or knowledge of one another's work exists. Alternatively, the assumption of closeness in relationships between individuals can fuel rumors and speculation.[11] Since the anti-corruption campaign implicates leadership in state-owned enterprises (SOEs), then it gives a higher confidence to conclude that the person in charge of SOEs, Zhang Guoqing, would be involved. Examples of potential connections are continually seen like with the arrests of Liu Shiquan of Norinco, Wu Yangshen of CASC, and Wang Changqing of China Aerospace Science and Industry Corporation (CASIC). All were arrested shortly after Li Shangfu's ousting, which by unlikely coincidence, Wu and Wang were also part of the CMSA.

Li Shangfu's influence is the key to understanding the restructuring of the PLA since his disappearance. He served as the first-ever Deputy Commander of the PLA Strategic Support Force.[12] Shortly after, he succeeded Zhang Youxia as the Head of the Equipment Development Department and became Commander of the Manned Space Program.[13] Consequently, Zhang became the Vice Chairman of the Central Military Commission (CMC) which oversees that department.

Although Li's rise is important, the potential contributors to his fall, like Wang Houbin and Wei Fenghe, are also important to see the domino effect of PLA leadership change. Wei was believed to be one of the most prominent members of the PLA, yet rumors of Wei's investigation began a few months later after he was not seen in public, then left his position as Minister of National Defense in March 2023.[14] Li Shangfu succeeded Wei in that position. Wei Fenghe's predecessors in the Rocket Force, Zhou Yaning and Li Yuchao, were also ousted from the party.[15] After Li Yuchao was investigated in July 2023, Wang Houbin took his position as Commander of the Rocket Force.[16] The odd detail is that Wang is a career Navy man going into a completely different branch of the military.

In September 2023, reports of the Li Shangfu investigation emerged, and a month later he was removed.[17] His removal was unexpected and sudden; otherwise, the change would have probably taken place at the regular reshuffling in December, and he wouldn't have succeeded Wei Fenghe earlier in March 2023. By unlikely coincidence, Li Shangfu was replaced by Dong Jun. Wang Houbin served as Deputy Commander of the PLA Navy under Commander Dong Jun. Early in 2024, the Strategic Support Force was disbanded and restructured into separate parts: Aerospace, Cyberspace, Information Support, and Joint Logistics Support Force.[18] Li's vast experience contributing to space systems in the Support Forces is now disconnected from other intelligence collection activities. While it may be similar operationally, leaders of those departments will have less control and influence over operations.

Li Shangfu is likely to have had great influence on the cause of the restructuring of the PLA, which flows down the ranks, but it raises more questions of supervision. Zhang Youxia and He Weidong were meant to be overseeing Li Shangfu's influence and operations, but Zhang was more familiar

Figure 2: Timeline of PLA Personnel Replacement

March 2023: Wei Fenghe leaves position as Minister of National Defense; Li Shangfu takes his spot.

July 2023: Rumors of Wei Fenghe's disappearance. Li Yuchao put under investigation; Wang Houbin takes his spot.

September 2023: Reports of Li Shangfu being investigated.

October 2023: Li Shangfu is removed as Minister of National Defense.

December 2023: Regular military leadership reshuffling. Dong Jun becomes Minister of National Defense.

April 2024: PLA Strategic Support Force is disbanded.

June 2024: Xi Jinping speech at Yan'an conference. Wei Fenghe, Li Shangfu, and Li Yuchao formally expelled from CCP.

Figure 2 shows a timeline of events from the reshuffling and roles of each PLA member.

with Li's role since he was his predecessor; the burden must fall on him. This is a connection that Xi Jinping must have considered. Zhang is one of the most prominent active princelings since his father, Zhang Zongxun, was a founding member of the PLA. Plus, Zhang Youxia is one of the few with combat experience.

In an August 2024 article by Zhang Youxia, he reemphasized China's military priorities while praising and giving credit to Xi's plans.[19] The explicit priorities for the military are to have cohesive joint operations and technology modernization. Despite the praise, which may absolve him of political pressure, at the end of the paper Zhang suggests it would be best to reduce "翻烧饼" which roughly translates to "turning over pancakes" or political purging.[20] This obviously does not match Xi Jinping's actions since he became leader. We know from the Tigers and Flies campaign that constant leadership change is preferable to Xi because a large quantity of factions makes it less likely they can coalesce.

Alternatively, Figure 2 might show a crisis of loyalty in the PLA rather than regular reshuffling. In a speech at the Yan'an conference, Xi emphasized that the military must be loyal to the party and warned senior leaders to reflect on their ideas.[21] Unless Zhang Youxia thinks he will be ousted soon, he doesn't need to insert subtle criticism about political turnover, so it cannot be interpreted as such for now. If any other senior PLA leader thought to insert their ideas, they have likely been deterred by the recent 'pancake flipping' and stark warning by Xi. This turmoil specifically with the PLA, is merely insight into Xi's values, ideas, and methods. Considering cohesive joint operations and technology modernization as military priorities (including loyalty), the most important individuals to achieve these priorities are Zhang Guoqing and Yuan Jiajun.[22] Nonetheless, the PLA is still subordinate to the ideas and decisions of the Politburo since they are closer to Xi.

There is no guarantee that Xi will keep any PLA leader for an extended period of time. Moreover, these personnel changes would affect China's long-term ambitions if there weren't a clear direction for next generation leaders.[23] The Politburo leaders guide long-term strategy, while PLA leaders focus on short-term tactics. From an isolated lens, it might be assumed that China is only focused on naval operations, especially because of escalated tensions throughout the Indo-Pacific. While there is truth in this view, it is limited given the knowledge of newer Politburo members, reshuffling in the PLA, and the proliferation of satellites. To supplement PLA operations in the Indo-Pacific, it must be considered that satellites are the 'eyes' for all domains. After an evaluation of space capabilities, it will be shown how strategy and tactics translate across domains.

PLANS, INTENTIONS, AND CAPABILITIES

On August 4, 2022, China launched a vehicle, codenamed Shenlong, into orbit from the Jiuquan Satellite Launch Center on a Long March 2F rocket. The launch vehicle was later discovered to be a spaceplane, an autonomous reusable vehicle designed like the now-retired U.S. space shuttle.[24] The orbital vehicle flew a mission that lasted 276 days before returning to Earth on May 8, 2023. Shenlong looked identical in design to Boeing's X-37B, the only model of spaceplane operating in the world. However, it wasn't just China's advanced orbital capabilities or its blatant copy of a secret American space vehicle that was a concern. During its flight, Shenlong released several objects that had the technical prowess to move in coordination with the spaceplane's orbit.[25] Although the Chinese news service Xinhua released a statement after the landing, no details were given regarding the operations conducted in orbit, the mysterious objects released, or Shenlong's overall mission. Given the secretive nature of China's spaceplane program, there is widespread concern that Shenlong could be the quiet establishment of China's first co-orbital anti-satellite weapons (ASAT) platform. Co-orbital ASATs are just one of many Chinese orbital space assets that pose a threat to U.S. national security.

The Chinese space threat isn't limited to orbital space, rather it extends to a permanent Chinese presence in the cislunar region (the space between Earth and moon). Both the DoD and NATO recognize space as a new strategic defense domain, stating that "space is integral to the way the [United States] military fights" and will need to be defended from strategic competitors.[26] As explained by the Chief of Space Operations for the U.S. Space Force General B. Chance Saltzman during a Senate Armed Services Committee hearing, evolving priorities have shifted to "fielding combat-ready forces, amplifying the guardian spirit, and partnering to win." General Saltzman went on to say, "When describing space threats, it's important to account for two kinds of threats: first, threats from space assets, and second, threats to space assets."[27] China is widely seen as the pacing challenge when looking at advanced space capabilities and the main competitor that poses the most credible threat to U.S. access to space.

According to China's 2019 Defense White Paper:

> Outer space is a critical domain in international strategic competition … [and its] … security provides strategic assurance for national and social development. In the interest of the peaceful use of outer space, China actively participates in international space cooperation, develops relevant technologies and capabilities, advances holistic management of space-based information resources, strengthens space situation awareness, safeguards space assets, and enhances the capacity to enter, exit, and openly use outer space safely.[28]

The most recent defense white paper adds to this outlook, defining China's presence in space and its ability to produce space assets indigenously, as a symbol of great power status, aiming to be a complete space power by 2040. It states:

> [One of the missions] of China's space program is to protect China's national rights and interests and build up its overall strength…China aims to strengthen its space presence in an all-round manner … to defend national security … advocate for sound and efficient governance of outer space … and to make a positive contribution to China's socialist modernization.[29]

Some key takeaways from the white paper include the following:

- Over four hundred launch attempts were made between 2016 and 2021 and over 700 are planned for 2023.
- China will promote varied space operations ranging from low-earth orbit (LEO) to the cislunar region.
- China will focus on engineering new technologies and applications to test in orbit. These include microsatellites, space debris cleaning, and in-orbit maintenance and repair.

The Chinese Communist Party (CCP) sees itself in a race with the United States and has been investing heavily in China's space capabilities. There is a high degree of political engagement and a whole-of-government approach to winning this race which can be seen in the level of investment and the institutional reorganization of the People's Liberation Army (PLA) military structure. Despite being less than a third of the U.S. budget, China spent an estimated $16 billion in 2021 on its space program. Although accurate budget data are hard to discern, this makes China second to the United States globally in space program appropriation.[30] In 2015, the CCP sought to reform the PLA force structure, shifting from a discipline-centric approach to a domain-centric one, allowing the CCP to have more direct authority over military objectives. Space operations were assigned to the PLA Strategic Support Force (PLASSF), which uses dual-use technology to shift easily from commercial space activities to military space activities.

The role of the PLASSF, according to the Ministry of National Defense is to safeguard national security, "strengthen peacetime-wartime integration" to reduce the amount of time taken to transition to a wartime posture in the event of a conflict, and utilize the 'Three Warfares' of space, information, and psychological warfare.[31] It also has control of the launch and tracking of satellites, applying services such as command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR). The PLASSF also develops and employs China's position, navigation, and timing (PNT), intelligence, surveillance, reconnaissance (ISR), satellite communications (SATCOM), and counter-space operations. It is unclear if the PLA Rocket Force (PLARF), which controls China's missile defense and its ICBMs, will have the authority to utilize terrestrial-based counter-space weapons such as direct-ascent ASATs.

China's interest in space started as far back as the 1970s with the launch of its first satellite, Dong Fang Hong 1, and the subsequent broadcast of the song "East is Red."[32] Project 921-2 was established in 1992 and laid out the plans for successive milestones every ten years starting with an unmanned space mission in 1999. After the successful 2003 manned space flight, China updated Project 921-2 in 2004 to include plans for an orbiting station by 2010 and a permanent station by 2022.[33] As of November 5, 2022, with the launch of the Tiangong Space Station, China has accomplished every space launch achievement over the last 30 years.[34] China performed additional accomplishments with the launch and subsequent landing of the lunar probe, Chang'e-4, on the far side of the moon in 2018. Arguably, all of China's achievements are the result of technical assistance from Russia and/or the theft of U.S. intellectual property. Regardless, the technology, talent, and technical acumen required to operate space-based assets have progressed rapidly within China. Although there is no real distinction between the civil and military arms of the Chinese government, space policy is articulated by two organizations. Under the direction of the Ministry of Industry and Information Technology, the State Administration for Security, Technology, Industry, and National Defense (SASTIND) manages and coordinates

space activities as well as oversees the link between space technology and military applications. The China National Space Administration (CNSA), operating under the SASTIND, is responsible for directing manned and unmanned missions in orbit and beyond, and maintaining the Long March and Tiangong programs.[35]

IN-ORBIT OPERATIONS

The number of active satellites currently in orbit reached 7,702 as of May 2023. The People's Republic of China (PRC) has the largest number of satellites in orbit second to the United States, with at least 1,397 active satellites being utilized for SATCOM, ISR, PNT, and science and technology (S&T), according to the Defense Intelligence Agency.[36] Despite undertaking more launches and achieving more sophistication in space-related activities, the PRC still lags behind the United States and is attempting to address this difference by providing more autonomy to the Chinese commercial space sector. Although there is a general concern for orbital overcrowding and the possibility of space debris from unintentional collisions, the concern of excess PRC satellite launches lies with the intentions stated by Chinese military strategists. According to a 2020 Chinese article in the *Science of Military Strategy*:

> Space has already become a new domain of modern military struggle; it is a critical factor for deciding military transformation; and it has an extremely important influence on the evolution of future form-states, modes, and rules of war. Therefore, following with interest the military struggle circumstance of space and strengthening the study of the space military struggle problem is a very important topic we are currently facing. Western countries headed by the United States have gained unprecedented war advantages from space.[37]

The PLA has a vested interest in denying the United States and its allies access to space due to past U.S. military successes involving the use of space-based support. Operations Desert Shield and Desert Storm in the 1990s were the first to utilize space-based assets to support ground forces. Surveillance satellites provided General Norman Schwartzkopf's strategic planners with a bird's-eye view of Iraqi military movements. Real-time intelligence and weather satellites provided predictions of visibility and illuminated weaknesses of the Republican Guard.[38] The PLA came to appreciate the effectiveness U.S. space systems but also understanding how reliant the U.S. military has been on space-based support for warfighting success. If the PRC can neutralize or deter U.S. space-based support, the PLA would face limited resistance if it were to increase gains in the South China Sea or make a move on Taiwan. In other words, U.S. military reliance on space means the PLA has an interest in strategic deterrence. Defense is the primary driver of PLA strategy and attacking first to deter or prevent U.S. interference is consistent with the PLA doctrine of 'Active Defense' or offensive defense and decisive defense. Active defense is used as a justification to ensure "the peaceful use of outer space" as stated in the 2019 Defense White Paper. The PLA views space as an offense-dominant domain which increases the incentive for a preemptive attack to protect its interests.[39] This is because, in space, the offense is less costly than the defense. PLA military writings have identified vulnerabilities in China's space assets, namely that Chinese satellites could be affected by hostile counter-space capabilities.[40]

What exactly are China's counter-space capabilities? This will be explained in greater detail in the next section. Counter-space weapons are part of a PLA strategy to counter U.S. military capabilities in the hopes of diminishing a U.S. response during a regional conflict. Counterspace weapons are the most effective way of denying, degrading, or disrupting adversarial space-based assets offensively or defensively.

COUNTERSPACE CAPABILITIES

This section examines the various counter-space and ASAT capabilities that the PRC employs. To date, only four countries have tested any type of ASAT in orbit throughout recent history: the United States, Russia, China, and India, respectively. There are four categories of counter-space weapons that will be examined in order of the permanency of damage: kinetic physical, non-kinetic physical, electronic, and cyber.[41]

1. Kinetic Physical ASATs use some type of kinetic action to create physical and irreversible damage to an asset. There are three types:

> a. Direct-Ascent ASATs: These are terrestrially-based kinetic objects or kinetic kill vehicles (KKV), such as missiles, that can target satellites in orbit.[42] China conducted a direct-ascent ASAT test in January 2007 and launched a ballistic missile at a non-operational weather satellite, the Fengyun-1C, which destroyed the satellite, creating more than 3,000 pieces of debris that are still in orbit.[43] Additional tests were conducted in 2010, 2013, and 2014, without creating debris. In May 2013, PLARF launched a direct-ascent missile reaching an altitude of 10,000 kilometers (km), prompting concerns

that China could launch attacks on low-earth orbit (LEO) and medium-earth orbit (MEO) satellites.

b. Co-orbital ASATs: These are space-based kinetic objects that target orbital satellites. Essentially, any intentional collision of one satellite with another could be considered a co-orbital ASAT attack.[44] With co-orbital ASATs, a kinetic object can be launched into orbit with the sole purpose of following, colliding, or attaching itself to a targeted satellite, disabling it, or pushing it into an unfavorable trajectory. In December 2021, the Chinese satellite Shijian-21 docked with Compass G2, a malfunctioning Beidou satellite, and used a robotic arm to drag Compass into a graveyard orbit above geosynchronous orbit (GEO) at 35,785 km in altitude. Shijian-21 released Compass and returned to its original orbit. This would be considered a complete co-orbital ASAT test intended to dispose of a defunct satellite.[45] Moving a satellite to line up with another satellite involves a very sophisticated technical capability called rendezvous and proximity operations (RPO) which is analyzed in the next section. These maneuvers offer another potential risk as more satellites enter Earth's orbit.[46]

c. Ground Station Attack: These are missile strikes that target ground stations that transmit data to orbiting satellites. With ground stations affected, satellites can descend into a decaying orbit and burn up in the atmosphere.[47]

2. Non-kinetic physical ASATs cause physical damage or degradation to targets without relying on physical contact. These ASATs do not result in destruction and in some cases are reversible. Some examples include:

a. Lasers: These can be ground-based or space-based and are used to dazzle or blind the optics of a satellite by overwhelming the circuitry. If a laser is more than 100W, it can cause permanent damage to satellite sensors. Any wattage higher than this could physically damage the parts of the satellite.[48] In 2006, China used a ground-based laser to dazzle a U.S. optical surveillance satellite, possibly an LEO satellite at 600 km.[49]
b. High-powered microwaves: These can be used to disrupt a satellite's electronics, corrupt data, or cause damage to electrical circuits.[50]
c. Electromagnetic Pulse: The EMP from a nuclear device could be used to cause significant disruption to satellite electronics and the radiation could damage circuitry. However, both the 1963 Limited Test Ban Treaty and the 1967 Outer Space Treaty prohibit the testing, placement, or usage of nuclear weapons in the atmosphere or space.[51]

3. Electronic Warfare ASATs can temporarily disrupt or deceive RF signals and transmissions.

a. Uplink/Downlink Jamming: This is the most common form of electronic attack, where either a signal from the source or the signal being transmitted from a satellite is interrupted or garbled. China is proficient at Global Positioning System (GPS) jamming, having both fixed and mobile terrestrial jammers. In November 2019, several reported incidents of GPS jamming originated from the port of Shanghai.[52]
b. Spoofing: This is an attack that tricks the receiver into believing a fake signal produced by the attacker is the real signal. Meaconing is a rebroadcast of a time-delayed encrypted signal without altering the data. Decryption isn't required because only the timing of the signal is being altered. In July 2019, over 300 ships in the Huangpu River were affected by spoofing in a single day, causing their reported positions to jump every few minutes.[53]

4. Cyberattacks target the data and the systems of satellites responsible for transmitting. Cyberattacks can be used to monitor data traffic patterns, intercept data, or insert corrupted data into a system. This is the only ASAT that can target stations, satellites, and systems equally.[54]

IN-ORBIT OPERATIONS: RPOS AND SPACEPLANES

As mentioned earlier, RPOs are an intentional change to an object's trajectory to bring it close to another object in space. According to the Secure World Foundation and released US Space Force tracking information, the number of Chinese satellites conducting RPO maneuvers has increased due to the emergence of robotic and autonomous technology.[55] If a satellite needed to get close to another for a co-orbital attack, the offending satellite would first have to conduct an RPO maneuver to synchronize orbits with the target. Many satellites that have this capability utilize an apogee kick motor (AKM), which is an alternate power source used to maneuver a satellite into another orbit. AKMs are detached before entering a new orbit so the debris does not interfere with the maneuvered satellite. Several Chinese satellites including the Shijian-21, Shijian 12-1, and Shijian 12-2 released what looks like AKMs

before entering GEO.[56] The release of upper-stage AKMs suggests all satellites launched within the last three years have RPO capability. Every Shijian satellite that's been observed has conducted RPOs and released smaller objects that are either microsatellites or orbital debris.[57] If co-orbital ASATs are such a risk, why are RPOs allowed at all?

Put simply, there are two main reasons RPOs would be used to get close to another satellite: to fix it or to follow it. Satellites must conduct RPOs to enable advanced applications like on-orbit servicing, assembly, and manufacturing.[58] On-orbit servicing refers to the repair of one satellite by another in orbit. An added difficulty in determining the intentions behind RPO maneuvers is the fact that RPOs are required for space debris removal. As of 2021, there are over 27,000 pieces of debris in orbit, most being over ten centimeters in diameter.[59] Even a five-centimeter object can punch a hole through the thermal covering of the ISS robotic arm.[60] It's estimated if active debris removal starts with five large intact objects annually, like defunct satellites, it would take 200 years for the debris population to stabilize in LEO alone. This doesn't account for the anticipated 16,000 microsatellites and constellations that will be launched over the next 10 years.[61] The State Council, SASTIND, and CNSA have echoed this sentiment, as with the Aolong-1 demonstration, using the need for space debris removal to get unnecessarily close to U.S. and allied satellites for unknown reasons.[62] A paper by Chinese researchers suggested using RPO maneuvers to plant small explosive charges in the nozzle of another satellite; this would be a perfect example of dual-use technology in action.[63]

Another concern is how difficult it is to observe RPOs from Earth, especially when looking at comms satellites in GEO. Because GEO needs to be a specific distance from Earth (30,000 km) it has become very crowded, making it hard to identify if satellites are collocated or being followed. This illustrates the difference between cooperative and non-cooperative RPOs. An example of a cooperative RPO between collocated satellites is the French-Italian Athena Fidus satellite and the Pakistani Paksat-1R, both inhabiting the same area in GEO.[64] Communication between the two space programs provides trust through transparency of movement. The PRC does not provide this level of transparency, offering no clarification on satellite operations or intentions. It is prudent to assume that RPO maneuvers are ASAT maneuvers if they're non-cooperative.

The Shenlong spaceplane, known as the Chongfu Shiyong Shiyan Hangtian Qi by the CNSA, is a concern not for its RPOs, but for what it released in orbit. According to tracking data from the U.S. Space Force's 18th Space Defense Squadron (18 SDS), after two months in LEO, China's spaceplane raised its orbit and released an object that conducted co-orbital maneuvers.[65] It is unclear when the object was released, but 18 SDS noticed the matching orbits of both Shenlong and the new object on October 31, 2022. A private firm called LeoLabs, which provides space situational awareness (SSA) data using a network of object trackers, confirmed evidence that Shenlong and the mystery object, labeled Object J, conducted a series of RPOs and at least two capture/docking operations, occurring between November to December 2022 and again in January 2023.[66] LeoLabs' analysis suggests Object J had "propulsive capability" and utilized formation flying with Shenlong. The purpose of the RPOs was not clarified by the China Aerospace Science and Technology Corporation (CASC), however, CASC released a statement claiming the spaceplane project "will provide a more convenient and inexpensive way to access space for the peaceful use of space in the future."[67]

The RPOs and secondary objects released from Shenlong do not automatically equate to a co-orbital ASAT platform. Even the U.S. X-37B launched several sub-satellites on its previous missions, and a lack of public tracking cannot verify if it utilized similar RPOs. However, it does prove that China has the technological capability and understanding to establish co-orbital ASAT platforms. It should be noted that when the X-37B was launched, the Chinese government expressed a lot of concern, in multilateral discussions on space security, that the X-37B could be utilized as an orbital weapon. If we look at China's space program from a Chinese national security perspective, it is understandable to think that the Chinese would match every U.S. operation in space with a perceived defensive goal. Pursuing a co-orbital ASAT test or establishing the infrastructure necessary to conduct co-orbital ASAT operations in the future is a good investment if your main adversary is a technological powerhouse in the space industry. As Secure World Foundation's Brian Weeden asked, "How much is China echoing what they've heard us talking about for a long time, and how much is independently motivated?"[68]

COUNTERSPACE THREATS AND CONFLICT

The risks associated with counter-space threats are that U.S. satellites currently have no defense against an ASAT attack. Most U.S. satellites operate in LEO which is 300-2,000 km in altitude. These satellites include mostly ISR and GPS, for remote sensing, imagery, and meteorology.[69] With LEO and GEO becoming more crowded, satellites in this orbit are

easy pickings for an ASAT attack. Satellites in GEO are susceptible to co-orbital ASATs or electronic warfare and cyberattacks. GEO is mainly populated with SATCOM and U.S. early missile warning satellites. With China's application of dual-use technology, it is becoming more difficult to discern non-cooperative RPOs that could disrupt function. All of China's commercial Yaogan satellites are 'PLA-operated' even though China denies using commercial satellites to collect intel.[70]

In the event of a reunification with Taiwan, China would rely less on space-based assets due to the proximity of Taiwan to the mainland. While terrestrial-based assets would likely be sufficient, China may still want to deter the United States from interfering. A conflict in the South China Sea would require more space-based support due to its size and the distance from the mainland. A conflict over the Spratly or Scarborough Shoal could tempt China to conduct a preemptive strike on U.S. satellites to deny power projection before a fight. It would be prudent of China to assume the United States is committed to intervention and would dismiss political and economic risks to seize on the opportunity to "blind or deafen" the United States. Striking first is always preferable to absorbing the first blow.[71] There is, of course, a global risk if kinetic ASAT activities were conducted in orbit. The debris from a destroyed satellite, let alone many, would create a cascade of space junk known as the Kessler Syndrome. Not even China wants this as it would affect launch capabilities and disrupt the space economy. However, three asymmetries favor China in this way.[72]

1. The United States relies on the space economy much more than China does.
2. The U.S. military is currently much more dependent on space access than China.
3. U.S. allies are just as reliant on American space-based capabilities.

China has had a lower overall investment in space, even though this is changing in the near term. If a preemptive first strike occurs, regardless of kinetic, electronic, or cyber means, it would benefit the PLA by knocking out the United States early and lowering the cost of war. Targets in LEO and GEO would disrupt U.S. SATCOM and ISR in the Indo-Pacific.

STRATEGIC PARALLEL WITH THE INDO-PACIFIC

In identifying the turmoil within the CCP/PLA and their capabilities, Xi Jinping has not shifted his focus from space in grand strategy; however, it raises questions about their operations after the disbandment of the PLA Strategic Support Force. The operational structure would need to be redone by someone with knowledge of their functions. As a consequence of ousting Li Shangfu, who heavily influenced the structure of that branch, Xi must rely on the CMC to oversee the new independent arms. Alternatively, if Xi had planned to shift priorities, then he wouldn't have ousted Li before the military leadership reshuffling period. Assuming space continues to be a priority for military modernization, they will rely on naval tactics because the PLA Navy are the most active against foreign nations. However, Xi may reveal his strategic hand by relying on naval strategy for all domains, including space.

Since China and the PLA lack experience in war when compared to the United States, they will be cautious to escalate tensions and do so when convenient. This is seen in by the gray zone tactics used in the Indo-Pacific against countries like Taiwan and the Philippines. China will be assertive and provocative without beginning an armed conflict because their capabilities are not up to par with the United States (despite their rapid growth). China does not attempt to hide that they are unwilling to start a war yet. If they were fully prepared and willing, then they would have attacked Taiwan by now.

'Salami slicing' has been their strategy of choice because it cautiously uses slow coercion to advance their influence. The following example is from Professor Zhang Weiwei of Fudan University. His insight is not meant to show new information, nor be a beacon of credibility, rather an internal signal from Chinese academics of what is already observable to outside observers. The professor spoke of the important absence of the word "peaceful" from the phrase 'peaceful reunification' about Taiwan from Li Qiang's March 2024 work report.[73] He added that the new strategy is about creating a gray-zone between war and a peaceful takeover. This does not require armed forces at the initial stage; it may come in the form of a blended civilian-military pressure. Earlier in 2024, there was a fishing boat from China that crossed Kinmen waters and tried to avoid detection before it tipped over.[74] There was initial speculation that one of the fishermen appeared to be PLA Navy Seargent, Chen Zujun. The importance of this example is not the accuracy of the report, rather it is the idea that such an incident is possible and can be repeated.

Beyond the civil-military fusion tactic, Zhang Weiwei suggests that the Chinese Coast Guard can board Taiwanese boats and ask for paperwork while claiming they are rightfully suspicious of the boat for crossing

waters, and it will show how serious they are about territory and boundaries.[75] These types of actions can culminate in their favor because small incidents can play into public perception and won't want to be seen as the aggressors if conflict breaks out. Zhang uses the analogy of 'boiling water' to highlight the end-goal of gray-zone tactics; the water heats up just before boiling and China will choose when to make it boil. They will continue escalating tensions while attempting to save face. China can control the temperature of the boiling water by using friendly, yet provocative rhetoric, followed by intimidation from their military.

Similar gray-zone tactics are being used against the Philippines. China's claim of the Nine-Dash Line overlaps with the Philippines' Exclusive Economic Zone (EEZ) which creates tension for shoals throughout the South China Sea. In previous decades, there were only a handful of tense incidents between the two countries. Recently, tensions have risen unlike previous decades. In 2024, China has increased its focus on Scarborough Shoal and the Spratly Islands. Both countries have used civilian, coast guard, and naval boats/ships to contest Sabina, Second Thomas, and Scarborough Shoals.[76] To highlight one example of coercion; in August 2024, the Philippines reported 40 Chinese ships prevented two of their boats from conducting a humanitarian mission to resupply the Philippine Coast Guard vessel, Teresa Magbuana, at Sabina Shoal.[77] The Philippines had to send helicopters over to complete the mission.

Incidents that occur with Taiwan and the Philippines foreshadow potential tactics China can use in space. This is crucial because of the manner China takes ownership over claims they make. We can draw a parallel to a race to the moon; the United States has not been for a while and China has yet to go, but if China land there before the United States in upcoming years, then they may be compelled to change the status quo. Furthermore, if they establish a base on the moon, then they are capable of setting standards and establishing Chinese as a communication language throughout space.[78] Knowing that the civil-military fusion tactic is slow and coercive enough to fit China's strategic ambitions, it can be applied to all domains including space.

China's satellites are quickly catching up with the United States in terms of quality, but not quantity. As China expands its use of satellites, it will become increasingly reliant on them—just like the United States. In anticipation of that goal, they will want to change the status quo to their benefit. They can implement the boiling water strategy similar to their methods throughout the Indo-Pacific. Additionally, they can create a narrative of openness to change rules through international institutions (as is done with the UN Security Council) while potentially deterring U.S. satellite operations. Individuals like Zhang Guoqing make the possibility easier for China to sell satellites and ASAT technology to their allies like Iran and others in the Global South. If China holds leverage over said country, it can coordinate intelligence collection with those satellites and deter U.S. satellite operations with their ASATs.

While a gray-zone strategy is likely to be used for space operations in the short term (the next few years), the long term depends on how far behind they are to U.S. space capabilities and how much leverage they've gained by changing the status quo. As previously mentioned, China is prioritizing modernization and Xi Jinping's frequent leadership reshuffling is not slowing down operations yet. That is why PLA leadership can only be used to analyze the near future and not long-term behavior while governing leadership is consistent with a long-term vision.

U.S. SHORT AND LONG-TERM APPROACHES

In response to Xi Jinping's ambitions, short and long-term strategies are needed. A potential short-term strategy involves building defenses on the satellites themselves and enhancing SSA or space domain awareness. Satellites can receive limited protection from non-kinetic ASATs, like HPMs and EMPs, using electromagnetic shielding. Filtered optical receivers or shutters that close upon detection of lasers are another option that can protect satellites from dazzling or blindness.[79] When it comes to SSA data sharing, it is important to have effective identification and understanding of any factors associated with the space domain. Private firms such as LeoLabs, HawkEye 360, or Slingshot all offer services that are used in conjunction with USSF capabilities to enhance space domain awareness. More reliance on these private firms can create more transparency with orbital movements and non-cooperative RPOs. For example, the U.S. Air Force is capable of tracking objects greater than 10 centimeters, whereas LeoLabs can track objects as small as two centimeters using S-band radar.[80] Relying on allied space-based and ground-based assets is an advantage that China does not have. Data-sharing in SSA will help allies respond or support in the event of an attack. Similarly, Japanese ground stations are readier to respond to an orbital threat in a Taiwan conflict. Allied capabilities should be used to augment U.S. capabilities.

A potential long-term strategy involves updating international treaties, greater investment and reliance on commercial launch vehicles, and additional sanctions on PRC aerospace firms. The United States must lead any attempt to update the Outer Space Treaty. China always tries to control the narrative, and the United States needs to be seen as setting the ideal for the peaceful use of space. This can be done by spearheading a complete ASAT ban treaty with clarification on the definition of a weapon and

a detailed list of acceptable space operations. A hybrid arms control treaty would also be effective in allowing non-cooperative RPOs so long as they didn't pass a certain proximity. Some space weapons could be banned, but dual-use functions that lie in the gray zone would need to be controlled through a self-defense clause only allowable after a treaty violation.[81]

The United States could also include language that recognizes the difference between cooperative and non-cooperative RPOs and enforces 'Keep-Out Zones' or a 'Zone of Non-Interference' that only surrounds the space asset. This might go against Article VIII in the Outer Space Treaty which states that only an object in space can be controlled, not the surrounding area. This language needs to be updated to reflect the reality of the times. A 'Keep-Out Zone' would not prevent an ASAT of any kind, but a mechanism to enforce a common law in space would be the first step to establishing norms and standards.[82] The United States has started this with the Artemis Accords, a set of principles that seeks to establish multilateral cooperation, standards, and practices for lunar exploration.[83] There should also be a framework for asteroid and lunar mining. Luxembourg started developing a regulatory and legal framework to establish ownership of minerals extracted from asteroids.[84] Such long-term strategies pertain to the CCP beyond Xi Jinping's lifetime leadership.

NOTES

[1] Although factional battles within the CCP have been a historically regular practice, neither the Jiang Zemin nor Hu Jintao factions have reached this level of domination; this is Xi Jinping's attempt to rearrange CCP factional politics.
Guoguang Wu, "New Faces, New Factional Dynamics: CCP Leadership Politics Following the 20th Party Congress," *China Leadership Monitor* (2022). *See also* Bonny Lin, Brian Hart, Matthew P. Funaiole, Samantha Lu, "China's 20th Party Congress Report: Doubling Down in the Face of External Threats," *Asia Society* 2022 (showing a word counter of key phrases, and an assessment of the content from the 20th Party Congress compared to the previous Party Congress's. The switch shows a decreased focus on economic issues).
[2] Guoguang Wu, "Aerospace Engineers to Communist Party Leaders: The Rise of Military-Industrial Technocrats at China's 20th Party Congress," *Asia Society* (2023).
[3] Anti-corruption is a loose term because the party and government systems operate regularly with a certain amount of corruption. It's about corruption being inconvenient for a party leader. The article provides an interactive database of CCP officials and affiliates who have been involved in Xi Jinping's anti-corruption campaign from 2012 – 2018. This anti-corruption campaign is commonly referred to as the Tiger and Flies campaign; the tigers are the prominent individuals while the flies are their subordinates. David M. Barreda, et al., "Visualizing China's Anti-Corruption Campaign," *ChinaFile* (2018).
[4] 张又侠, "持续深化国防和军队改革（学习贯彻党的二十届三中全会精神）," 人民网 - 人民日报, August 9, 2024, http://politics.people.com.cn/n1/2024/0809/c1001-40295362.html; 李强, "李强作的政府工作报告（摘登）," 新华网, March 5, 2025, http://www.news.cn/politics/20250305/c51c68c485fa4c3f9d4c54751c715aba/c.html.
[5] The label "potential successor" is not exclusive to one person.
[6] Not all changes in the "current" and "ousted" categories are parallel or connected. It serves merely as a list to reference because of the many names. The leadership changes which are connected are highlighted in the timeline of Figure 2.
[7] Norinco's connection to Iran has been well noted since they were sanctioned by the United States in 2003.
"US punishes firms in Iran and China," *BBC News*, 2003. Xi sent Zhang Guoqing to Ebrahim Raisi's funeral to which Mohammad Mokhber expressed his gratitude for sending Zhang specifically. It is almost certain that Zhang would be the one who was heavily involved in any dialogue over weapons with Iran.
[8] AVIC is known to be one of the largest defense contractors in the world that produces essential parts, such as parts for the Beidou satellite system. J.J. Long, Thomas Corbett, and Dan Shats, "Organization of the Aviation Industry Corporation of China (AVIC)," China Aerospace Studies Institute (2024).
[9] Jane Cai, "China places former chairman of top aircraft maker AVIC under investigation for corruption," *South China Morning Post*, 2024.
[10] Project 921 became the China Manned Space Program/Agency. Project 921/1 was Shenzhou's first crewed flight. The Shenzhou missions are foundational to the China Manned Space Agency.
[11] While rumors in Chinese news outlets can be telling of a narrative that opposing factions want to create, they can also be indicators of deception from the leading faction or contain some element of truth. In some cases, rumors can better serve as an indicator of volatility (rather than truth) in whichever industry is mentioned.
[12] Lei Zhao, "PLA Says Chief of Its Arms Wing Replaced," *China Daily*, September 19, 2017, https://www.chinadaily.com.cn/china/2017-09/19/content_32187194.htm.
[13] Ibid.
[14] SCMP Reporters, "Chinese anti-corruption investigators target top PLA Rocket Force generals, sources say," *South China Morning Post*, 2024.
[15] Reports of Zhou's ousting did not appear until the December 2023 military reshuffling most likely because he left his post and prominence in the 2021 reshuffling and was succeeded by Li Yuchao.
[16] Li Yuchao's two deputies Liu Guangbin and Zhang Zhenzhong were also ousted.
[17] There has been a reshuffling in military leadership positions that has occurred every two years in December on odd-numbered years. The last one was in December 2023 and the next is expected to be in December 2025.
[18] Chen Zhou, ed., "Chinese PLA Embraces a New System of Services and Arms: Defense Spokesperson," *China Military*, April 19, 2024, http://eng.chinamil.com.cn/CHINA_209163/TopStories_209189/16302105.html#:~:text=There%20are%20four%20services%2C%20namely%20the%20Army%2C%20the%20Navy%2C%20the%20Air%20Force%20and%20the%20Rocket%20Force%2C%20and%20four%20arms%2C%20including%20the%20Aerospace%20Force%2C%20the%20Cyberspace%20Force%2C%20the%20Information%20Support%20Force%20and%20the%20Joint%20Logistics%20Support%20Force.
[19] Zhang Youxia, "Continue to deepen defense and military reform (study and implement the spirit of the Third Plenary Session of the 20th CPC Central Committee)," *People's Daily Online*, 2024.
[20] Zhang Youxia uses the phrase "翻烧饼" or turning over pancakes as an idiom for political purging. The idea is better described as "pancake flipping," a Chinese idiom (chengyu "成語"). 张又侠, "持续深化国防和军队改革（学习贯彻党的二十届三中全会精神）," 人民网 - 人民日报, August 9, 2024, http://politics.people.com.cn/n1/2024/0809/c1001-40295362.html; 上官酒瑞, "小常识与大道理｜为什么说乱"翻烧饼"是治国理政的大忌？" *The Paper*, 2022, https://www.thepaper.cn/newsDetail_forward_18926550.
[21] Xinhua, "Xi Focus: Xi stresses PLA's political loyalty at a crucial meeting held in old revolutionary base," *Xinhua News*, 2024.

[22] Although loyalty is a legitimate factor for Xi Jinping, open-source information does not allow such an assessment of relationships.
[23] Recently, Guoguang Wu of the Asia Society analyzed the rising stars of the CCP who are near their early 40s. He found that among those who are promoted faster, the number of technocrats is growing in comparison to previous generations. More specifically, many of them are alumni of Tsinghua University, a school known to have the best STEM program in China, and it's Xi Jinping's alma mater. Graduates from Tsinghua are shown to be outperforming all other schools showing a possible sense of reliability by those alumnae to the party. The most important observation of the trend is the network and make-up of the party for future generations. With rapid leadership change, observers often wonder who will be next. The entire article by Guoguang Wu gives a thorough analysis of the growing trend. Most importantly, he includes a table with all the names and details of the individuals from the analysis in Appendix I, Guoguang Wu, "The Rise of CCP Young Elites and Xi Jinping's "Tsinghua New Army," Asia Society, February 12, 2025, https://asiasociety.org/policy-institute/rise-ccp-young-elites-and-xi-jinpings-tsinghua-new-army#rising-stars-who-are-the-youngest-mid-level-cadres--20467.
[24] Mike Wall, "US Military's X-37B Space Plane Lands, Ending Record-Breaking Mystery Mission," Space.Com, November 12, 2022,. https://www.space.com/space-force-x-37b-space-plane-otv-6-mission-ends; Brian Weeden, "Current and Future Trends in Chinese Counterspace Capabilities," *Proliferation Papers*, no. 62, (November 2020).
[25] Andrew Jones, "China's Spaceplane Conducted Proximity and Capture Maneuvers with Subsatellite, Data Suggests," *SpaceNews*, May 11, 2023, https://spacenews.com/chinas-spaceplane-conducted-proximity-and-capture-maneuvers-with-subsatellite-data-suggests/.
[26] U.S. Department of Defense, "Space Integral to the DoD Way of War, Policy Chief Says," n.d., https://www.defense.gov/News/News-Stories/Article/Article/3465982/space-integral-to-the-dod-way-of-war-policy-chief-says/.
[27] Chance Saltzman, "To Receive Testimony on the United States Space Force Programs in Review of the Defense Authorization Request for Fiscal Year 2024 and the Future Years Defense Program, Before the Subcommittee on Strategic Forces of the Senate Committee on Armed Services," 118th Congress, Statement. n.d.
[28] "China's National Defense in the New Era," The State Council Information Office of the People's Republic of China, accessed on September 20, 2019, http://www.xinhuanet.com/english/2019-07/24/c_138253389.html
[29] "China's Space Program: A 2021 Perspective," The State Council Information Office of the People's Republic of China, accessed on December 1, 2023. https://english.www.gov.cn/archive/whitepaper/202201/28/content_WS61f35b3dc6d09c94e48a467a.html
[30] "China in Space: Ambitions and Possible Conflict Ambitions and Possible Conflict," www.jstor.org, n.d. https://www.jstor.org/stable/26333878.
[31] "China's Growing Military Space Prowess: Institutions and Capabilities," China Aerospace Studies Institute, September 2020.
[32] "China in Space: Ambitions and Possible Conflict Ambitions and Possible Conflict," www.jstor.org, n.d., https://www.jstor.org/stable/26333878.
[33] Ibid.
[34] Daisy Dobrijevic, and Andrew Jones, "China's Space Station, Tiangong: A Complete Guide," Space.com, August 15, 2023, https://www.space.com/tiangong-space-station.
[35] "China in Space: Ambitions and Possible Conflict Ambitions and Possible Conflict." www.jstor.org, n.d., https://www.jstor.org/stable/26333878; "China's Growing Military Space Prowess: Institutions and Capabilities," China Aerospace Studies Institute, September 2020; Weeden, "Current and Future Trends in Chinese Counterspace Capabilities."
[36] "Challenges to Security in Space: Space Reliance in an Era of Competition and Expansion," www.dia.mil/Military-Power-Publications, Defense Intelligence Agency, March 2022.
[37] RAND Corporation, "Scorecard 7: U.S. Counterspace Capabilities Versus Chinese Space Systems," in *Forces, Geography, and the Evolving Balance of Power, 1996-2017* (Santa Monica, CA: RAND Corporation, 2017), 227-43; "Challenges to Security in Space: Space Reliance in an Era of Competition and Expansion," www.dia.mil/Military-Power-Publications, Defense Intelligence Agency, March 2022; and RAND Corporation, "Scorecard 8: Chinese Counterspace Capabilities Versus U.S. Space Systems," in *The U.S.-China Military Scorecard*, 245–58 (Santa Monica, CA: RAND Corporation, 2017).
[38] "China's Growing Military Space Prowess: Institutions and Capabilities," China Aerospace Studies Institute, September 2020.
[39] "Offensive Defense: People's Liberation Army Logic of Preemption in Space People's Liberation Army Logic of Preemption in Space." www.jstor.org, n.d., https://www.jstor.org/stable/48711882.
[40] Mark Stokes, Gabriel Alvarado, Emily Weinstein, Ian Easton, Project 2049 Institute, and Pointe Bello, "China's Space and Counterspace Capabilities and Activities," The U.S-China Economic and Security Review Commission, March 30, 2020. https://www.uscc.gov/research/chinas-space-and-counterspace-activities; RAND Corporation, "Scorecard 7: U.S. Counterspace Capabilities Versus Chinese Space Systems," in *Forces, Geography, and the Evolving Balance of Power, 1996-2017* (Santa Monica, CA: RAND Corporation, 2017), 227-43.
[41] Weeden, "Current and Future Trends in Chinese Counterspace Capabilities"; and Kari A. Bingen, et al. "Space Threat Assessment 2023," Center for Strategic and International Studies, April 2023, www.csis.org/analysis/space-threat-assessment-2023.
[42] Ibid.
[43] Ashley J. Tellis, "India's ASAT Test: An Incomplete Success," Carnegie Endowment for International Peace, April 15, 2019, https://carnegieendowment.org/2019/04/15/india-s-asat-test-incomplete-success-pub-78884; "Challenges to Security in Space: Space Reliance in an Era of Competition and Expansion," www.dia.mil/Military-Power-Publications, Defense Intelligence Agency, March 2022.
[44] Bingen, et al., "Space Threat Assessment 2023."
[45] Andrew Jones, "China's Shijian-21 Towed Dead Satellite to a High Graveyard Orbit," *SpaceNews*, February 22, 2023., https://spacenews.com/chinas-shijian-21-spacecraft-docked-with-and-towed-a-dead-satellite/; Secure World Foundation, "Global Counterspace Capabilities: An Open Source Assessment," Secure World Foundation, April 2023, https://swfound.org/counterspace/.
[46] Bingen, et al. "Space Threat Assessment 2023"; "Challenges to Security in Space: Space Reliance in an Era of Competition and Expansion," www.dia.mil/Military-Power-Publications, Defense Intelligence Agency, March 2022.
[47] Ibid.
[48] Weeden, "Current and Future Trends in Chinese Counterspace Capabilities."
[49] Ibid.
[50] Todd Harrison, Kaitlyn Johnson, and Makena Young, "Defense Against the Dark Arts in Space: Protecting Space Systems from Counterspace Weapons," Center for Strategic and International Studies, February 2021. https://www.csis.org/analysis/defense-against-dark-arts-space-protecting-space-systems-counterspace-weapons.
[51] Ibid.
[52] Weeden, "Current and Future Trends in Chinese Counterspace Capabilities."
[53] Ibid.
[54] Harrison, et al, "Defense Against the Dark Arts in Space: Protecting Space Systems from Counterspace Weapons."
[55] "Mitigating Noncooperative RPOs in Geosynchronous Orbit,"

www.jstor.org, n.d. https://www.jstor.org/stable/48711887.
[56] Harrison, et al, "Defense Against the Dark Arts in Space: Protecting Space Systems from Counterspace Weapons"; Mitigating Noncooperative RPOs in Geosynchronous Orbit," www.jstor.org, n.d. https://www.jstor.org/stable/48711887.
[57] Ibid.
[58] Secure World Foundation, "Global Counterspace Capabilities: An Open-Source Assessment."
[59] "About Space Debris," n.d. https://www.esa.int/Space_Safety/Space_Debris/About_space_debris.
[60] Chris Daehnick and Jess Harrington, "Look out below: What Will Happen to the Space Debris in Orbit?" McKinsey & Company, October 1, 2021, https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/look-out-below-what-will-happen-to-the-space-debris-in-orbit.
[61] "Space Arms Control: A Hybrid Approach a Hybrid Approach," www.jstor.org, n.d. https://www.jstor.org/stable/26430818.
[62] Harrison, et al, "Defense Against the Dark Arts in Space: Protecting Space Systems from Counterspace Weapons."
[63] Stephen Chen, "Chinese Scientists Build Anti-Satellite Weapon That Can Cause Explosion Inside Exhaust," *South China Morning Post*, October 21, 2021, https://www.scmp.com/news/china/military/article/3153174/chinese-scientists-build-anti-satellite-weapon-can-cause.
[64] "Mitigating Noncooperative RPOs in Geosynchronous Orbit," www.jstor.org, n.d. https://www.jstor.org/stable/48711887.
[65] Andrew Jones, "China's Spaceplane Conducted Proximity and Capture Maneuvers with Subsatellite, Data Suggests," *SpaceNews*, May 11, 2023, https://spacenews.com/chinas-spaceplane-conducted-proximity-and-capture-maneuvers-with-subsatellite-data-suggests/.
[66] Ibid.
[67] Daniel Shats and Peter W. Singer, "Don't Buy China's Hypersonic Head-Fake. Its Spaceplanes Are Racing Ahead," *Defense One*, December 22, 2021, https://www.defenseone.com/ideas/2021/12/dont-buy-chinas-hypersonic-head-fake-its-spaceplanes-are-racing-ahead/359705/.
[68] "China's Cislunar Space Ambitions Draw Scrutiny," www.jstor.org, n.d., https://www.jstor.org/stable/27023019.
[69] RAND Corporation, "Scorecard 7: U.S. Counterspace Capabilities Versus Chinese Space Systems," in *Forces, Geography, and the Evolving Balance of Power, 1996-2017* (Santa Monica, CA: RAND Corporation, 2017), 227-43.
[70] Ibid.
[71] Offensive Defense: People's Liberation Army Logic of Preemption in Space People's Liberation Army Logic of Preemption in Space," www.jstor.org, n.d., https://www.jstor.org/stable/48711882.
[72] Ibid.
[73] "Regarding Taiwan, Why Doesn't the US Worry China?" The China Academy, May 24, 2024. https://thechinaacademy.org/regarding-taiwan-why-doesnt-the-us-worry-china/.
[74] Cheng Xinying, "他們隸屬南海戰區? 金廈翻船事件生還者遭起底 疑解放軍扮福建漁民," Yahoo! News, February 25, 2024, https://tw.news.yahoo.com/%E4%BB%96%E5%80%91%E9%9A%B8%E5%B1%AC%E5%8D%97%E6%B5%B7%E6%88%B0%E5%8D%80%E9%87%91%E5%BB%88%E7%BF%BB%E8%88%B9%E4%BA%8B%E4%BB%B6%E7%94%9F%E9%82-%84%E8%80%85%E9%81%AD%E8%B5%B7%E5%BA%95--%E7%96%91%E8%A7%A3%E6%94%BE%E8%BB%8D%E6%89%AE%E7%A6%8F%E5%BB%BA%E6%BC%81%E6%B0%91-033111561.html.
[75] "Regarding Taiwan, Why Doesn't the US Worry China?" The China Academy, May 24, 2024, https://thechinaacademy.org/regarding-taiwan-why-doesnt-the-us-worry-china/.
[76] Cryil Ip, "Chinese coastguard takes aim again at Philippines over South China Sea shoal clashes," South China Morning Post, December 5, 2024, https://www.scmp.com/news/china/diplomacy/article/3289558/chinese-coastguard-takes-aim-again-philippines-over-south-china-sea-shoal-clashes.
[77] Tessa Wong and Joel Guinto, "Sabina Shoal: The new flashpoint between China and the Philippines," BBC News, August 30, 2024, https://www.bbc.com/news/articles/cp3d4rz922do.
[78] Dean Cheng also mentions the potential competition among the International Lunar Research Station (IRLS) and ARTEMIS despite them not being parallel. Bonnie Glaser and Dean Cheng, "China's Ambitious Civilian Space Program," China Global, German Marshall Fund, February 4, 2025, https://www.gmfus.org/news/chinas-ambitious-civilian-space-program.
[79] Ibid.
[80] "Mitigating Noncooperative RPOs in Geosynchronous Orbit," www.jstor.org, n.d. https://www.jstor.org/stable/48711887.
[81] "Space Arms Control: A Hybrid Approach a Hybrid Approach," www.jstor.org, n.d. https://www.jstor.org/stable/26430818.
[82] "Mitigating Noncooperative RPOs in Geosynchronous Orbit," www.jstor.org, n.d. https://www.jstor.org/stable/48711887; "Space Arms Control: A Hybrid Approach a Hybrid Approach on JSTOR," www.jstor.org, n.d. https://www.jstor.org/stable/26430818.
[83] United States Department of State. "Artemis Accords - United States Department of State," December 1, 2023. https://www.state.gov/artemis-accords/.
[84] "China in Space: Ambitions and Possible Conflict Ambitions and Possible Conflict," www.jstor.org, n.d. https://www.jstor.org/stable/26333878.

Abiel Alvarenga is a former Graduate Fellow at the Center for Energy Science and Policy (CESP). He has a master's degree in International Security from George Mason University and focuses his research on Indo-Pacific relations. His research continues to seek to combine an understanding of human incentives and the use of advanced technologies.

Carlos Alatorre has a master's degree in Statecraft and National Security Affairs from the Institute of World Politics (IWP). His research broadly focused on China's military efforts pursuing emerging technologies, and specifically the PLA's plans, intentions, and capabilities for operating in space. He currently works as a videographer and content editor for IWP's media department and continues his research on China's operations in orbit and cislunar space.

The Future Dangers of Imported Microchips—Why America Must Take Control of Semiconductor Production

by **Matelier Numbi and Gaston Elongha**

INTRODUCTION & BACKGROUND

This article explores the growing security risks associated with foreign-manufactured microchips. It focuses on their potential to compromise American national security, critical infrastructure, and technological sovereignty. Semiconductors have been powering everything from military defense systems, communication networks, and healthcare systems, all with an increased dependence on foreign sources, especially from countries with competing geopolitical interests, which pose significant threats to the United States. Many case studies highlight vulnerabilities such as hardware backdoor incidents, the illegal export of semiconductor technology to China, and the impact of U.S. export controls on Chinese semiconductor firms. These incidents demonstrate how foreign-manufactured microchips can be exploited for espionage, military advantage, and economic disruption.

This article proposes a comprehensive multifaceted solution that joins together the National Semiconductor Security Framework (NSSF), the U.S. *National Cybersecurity Strategy*, and the U.S. *National Security Strategy*, and the National Institute of Standards and Technology (NIST) framework to support domestic semiconductor manufacturing, as well as promote stricter supply chain audits, international regulatory cooperation, resilient cybersecurity, and advanced detection technologies. This would reduce U.S. dependency on potentially hostile foreign sources and help secure the U.S. semiconductor supply chain from internal and external threats.

Modernization for integration capabilities has drastically changed the microchip manufacturing landscape. Microchips have become the backbone of all critical systems—from military defense to economic infrastructure and even consumer services,[1] a situation that has led to a significant increase in performance while also becoming cost-effective and maintaining process efficiency. From a geopolitical standpoint, looking at the increased usage in the United States—not to mention dependence on foreign-manufactured microchips, our dependence on foreign semiconductor chips raises significant national security issues. Relying on foreign-manufactured semiconductors runs far beyond traditional cybersecurity risks because some integrated microchips may be manufactured with embedded malicious code that can later serve as backdoors for adversarial countries to leverage maliciously, presenting a severe danger to U.S. national security. While most U.S. semiconductor chips are imported, these vulnerabilities pose a real risk that could significantly damage not only military operations but also U.S. or civilian infrastructures, and even American sovereignty.

Moreover, since integration typically comes with artificial intelligence (AI) capabilities, there are also emerging threats that include AI manipulation of microchips, remote sabotage, and the breaking of systems encryption through the use of quantum computing.[2] There is, therefore, an urgent need for the United States to promote in-house chip manufacturing to remain competitive while also ensuring its security and reducing foreign chip dependency. Firstly, this article highlights the security threats and vulnerabilities introduced by foreign-manufactured microchips. Secondly, this article proposes useful ways for securing competitive and domestically manufactured microchips.

The National Semiconductor Security Framework (NSSF) offers a limited approach to guide internal and external threat management involving the manufacture of microchips[3]; nonetheless, the United States lacks a comprehensive or multifaceted solution to manage the risks introduced by foreign-produced microchips.[4] Recent discussions have focused on identifying the threats without providing enough actionable strategies. Looking at the AI-driven backdoors in microchips, for example, such chips can intelligently escape[5] from traditional detection and self-learn patterns that are later leveraged by adversaries to sabotage critical infrastructure, such as healthcare and the energy grid.

Initially, this article reviews existing literature on the microchip landscape, manipulation, and threats, especially when leveraged with AI for backdoors, remote control, and sabotage. The article also uses case studies that illustrate cases in which microchips and AI were leveraged for malicious activities. This article then examines various frameworks to develop a multifaceted security approach that will promote domestic chip manufacturing and also mitigate against both internal and external threats. The case studies explain why the United States must remain at the forefront of this race by developing secure, local semiconductors. Secure domestic production capabilities are essential to close this vulnerability gap against adversary countries. Strengthening U.S. control over the production and security of its critical semiconductor technologies can help shield the country from foreign manipulation and protect its national interests.

LITERATURE REVIEW

The indispensability of semiconductors is tied to the risks they introduce when imported from rival countries. That indispensability (see figure 1) illustrates, for example, microchips powering military defense systems and communication networks, energy grids, and healthcare technologies.[6] The risks are introduced due to the high level of imports and a dependency on foreign-manufactured semiconductors. As the research draws from existing literature and research, this section examines the challenges and dangers of foreign-manufactured semiconductors—including AI-driven manipulation of microchips, remote-controlled sabotage of microchips, the peril from quantum computing, and the U.S. response to the increasing semiconductor security crisis.

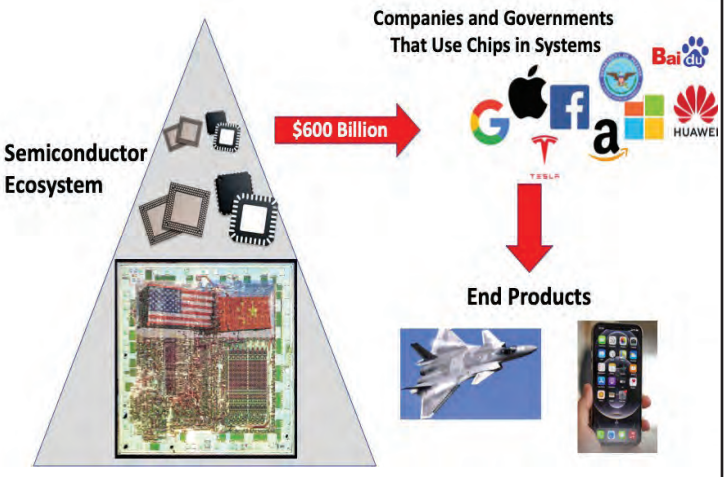


Figure 1: The Semiconductor Ecosystem[7]

AI-POWERED MICROCHIP MANIPULATION

Semiconductor microchips, especially with AI-embedded functionality, have revolutionized the manufacturing industry. Embedded AI chips can adapt and process increasingly complex tasks. However, that comes with a cost as it may create vulnerabilities that can be exploited by adversaries. Scholars have investigated the dangers of AI microchips, in particular microchips, with backdoors or self-programming capabilities.[8]

Beyond hardware backdoors, self-programming microchips are also a growing risk. Depending on external stimuli such as environmental conditions, these chips can resistively alter their own functionality.[9] This raises serious risks to national security, while also forging a way in which this capability can be used in many applications like edge processing and AI computing. For instance, a U.S. telecommunication microchip embedded with a self-programming pattern may initially follow the expected pattern but later activate unnecessary data transmission protocols and thereby compromise sensitive information.[10] Self-modifying chips can also evolve over time, bypassing security checks and staying undetected until causing considerable damage.

REMOTE-CONTROLLED SABOTAGE OF MICROCHIPS

Remote control sabotage of semiconductors, for instance, is another critical issue. More sophisticated ways of manipulating microchips are being invented that do not require infiltrating networks or software systems, making traditional hacking methods increasingly outdated.[11] One of the most serious such threats involves other parties gaining such remote access to microchips via radio frequency (RF) and disabling or manipulating critical systems, and not realizing it.

Janjua (2024) detailed the risks of RF-enabled microchips that can be operated remotely by adversaries. Detection and prevention can be impossible, largely because these chips are not activated until a specific signal is sent.[12] This presents a great danger in military applications because RF-enabled chips (see figure 2) can be inserted into missile guidance systems, drones, and encrypted communication networks, allowing an adversary to interfere with systems in real-time, sabotaging military operations.[13] Such vulnerabilities can

leave the U.S. defense sector highly exposed to remote interference from adversarial nations, particularly China and Taiwan, which currently dominate semiconductor manufacturing.

FIGURE 2: WIRELESS MICROCHIP REMOTE CONTROL[14]

Moreover, remote-controlled sabotage can be used against civil infrastructure, apart from military operations. Remotely disabling or changing the microchips embedded in critical systems such as energy grids, healthcare networks, and transportation networks could lead to significant disruption.[15] In energy systems, for example, microchip compromises could lead to blackouts, or undermined energy pricing, and in medical devices, such as pacemakers or insulin pumps, catastrophic failure. Krivic and Defraigne (2024) urged better detection and verification systems that identify and disable these threats before they can be used.[16]

THE QUANTUM COMPUTING THREAT

As quantum computing technology progresses, the risks posed by quantum-powered microchips have become more pronounced. Quantum chips, unlike traditional semiconductors, run on quantum mechanical principles like superposition and entanglement, providing exponentially more powerful computations.[17] Quantum computing is a promising tool for scientific and technological breakthroughs, but it comes with unique cybersecurity issues, including cryptographic and information security.

Quantum-enabled exploits could thus be embedded into semiconductors used in U.S. military defense systems, as warned by Bardt, Röhl, and Rusche.[18] By using quantum-powered microchips, an adversary could defeat conventional encryption methods, making sensitive government, military, or financial data open to theft or manipulation. Foreign adversaries could also exploit these vulnerabilities to access classified information or disrupt an autonomous weapon.[19] The result could lead to military conflict. This is not a hypothetical situation, evidenced by the 2018 incident in which Chinese operatives reportedly gained access to supply chains and implanted malicious chips into U.S. servers.[20] These threats will become more sophisticated and harder to detect as quantum computing develops.

The finance sector is extremely vulnerable to the advent of quantum microchips. This is because financial transactions and sensitive data could be exposed to cyberattacks enabled by quantum computing that could render current encryption methods obsolete. Krivic and Defraigne (2024) addressed the possibility that malware using quantum acceleration could be used to disrupt the economy, for example, by targeting banking networks.[21]

THE U.S. RESPONSE TO SEMICONDUCTOR SECURITY RISKS

Foreign-manufactured semiconductors are a growing threat, and the United States must act decisively to maintain its technological sovereignty and national security. Several scholars argue that the United States must prioritize growing domestic semiconductor manufacturing capabilities to mitigate reliance on foreign sources, especially from hostile or adversarial countries such as China and Taiwan.[22] Kawar stated that the *CHIPS and Science Act*, a legislative push to increase domestic semiconductor production and secure supplies, is vital.[23] The legislation would invest in domestic semiconductor manufacturing facilities while preventing foreign adversaries from interfering with critical technologies. This would help protect national security, as well as promote domestic self-sufficiency in the semiconductor industry.

Domestic manufacturing alone will not be enough to eliminate the entire spectrum of semiconductor security threats. Spigarelli and Sampaolo argue that the United States must also require tight controls and security procedures for imported semiconductors.[24] This includes building state-of-the-art verification devices, including AI-based detection systems, which can find chips on the verge of being integrated into critical infrastructure. It will also be necessary to collaborate with international allies, including Japan, South Korea, and members of the European nations to diversify silicon semiconductor supply chains and pare back risks that come from over-dependence on any one foreign source.

CASE STUDIES

2018: The Supermicro Hardware Backdoor Incident

Supermicro, a top U.S. server producer, experienced a critical security breach in 2018, revealed later by its supply chain team to have been Chinese in origin.

It was found that Chinese operatives had introduced tiny microchips embedded into motherboards before they were shipped to Supermicro. Qualified as hardware backdoors, these chips would have allowed Chinese operatives to gain unauthorized access to sensitive data and systems hosted in Supermicro servers in use by organizations.[25] Many major U.S. technology firms, government agencies, and defense contractors had operated unknowingly with compromised servers.

The threat of the embedded microchips was undetectable to cybersecurity teams. This incident alone demonstrates how the global supply chain is susceptible to foreign use for espionage or as an attack vector during a conflict. This backdoor incident illustrates the need for rigorous security protocols and comprehensive supply chain audits to mitigate against this kind of high-powered attack.[26] In response, many organizations started revising procurement processes, thinking about implementing more rigorous security measures, and searching for new sources for vital hardware components. Additionally, the incident spurred more U.S. government interest in the risks facing its national security interests with foreign-manufactured hardware and the need for more oversight.[27] In other words, the United States needs a comprehensive National Cybersecurity Strategy (NCS) to ensure a national security posture that is resilient to cyberattacks threatening national security and critical infrastructure.[28]

2019: U.S. Export of Semiconductor Technology to China

In 2019, Yi-Chi Shih, an electrical engineer, was convicted of conspiring to illegally export semiconductor chips with missile guidance applications to China. Shih had obtained integrated circuits that had been meant for the military and transferred them to Chinese entities without the required export licenses.[29] The chips were designed for use in China's missile guidance systems, thus improving its military strength. The case underscores the perils of the unauthorized transfer of extremely sensitive technology and how such exports could boost the militaries of adversarial nations. This incident illustrates why strict export controls are needed; the United States must prevent the unauthorized dismantling of advanced technology from being repurposed for military applications.[30] This induced a review of the existing security policies and the adoption of additional, more effective security measures in protecting sensitive technologies. At the same time, it could have served as a tale about what can go wrong in the global supply chain and the need to secure intellectual property to avoid having it exploited by foreign powers.

This adds to the *National Security Strategy*, parts two and three, which emphasize that the United States must invest in its strength and global priorities. The *National Security Strategy* explained that the United States must maintain a competitive edge, modernize its military, and maintain its overall national power. The United States must also out-compete rival countries such as China and Russia while forging overall rules when it comes to cybersecurity, technology, and trading and economic rules.[31]

2022: U.S. Export Controls on the Chinese Semiconductor Industry

The latest U.S. export controls announced in October 2022 aimed at cutting off China's access to advanced semiconductor technologies. The regulations aimed to prevent China from acquiring high-end computing chips to make advances in manufacturing supercomputers and semiconductors.

The export controls were aimed to restrict China's ability to develop technologies that could be used to improve its military prowess and technological proficiency, but in such a way as not to harm U.S. national security and foreign policy interests. This was one facet of a larger effort to preserve U.S. technological dominance, as stated in the *National Security Strategy*, to prevent the transfer of vital technologies to adversaries.[32] The action raised tensions between China and the United States, with China asserting it was opposed and accusing the United States of practicing political protectionism in advanced technology. Several semiconductor companies operate worldwide, which means the restrictions had a substantial impact on global supply chains.[33] This development accentuates geopolitical dimensions of semiconductor technology and the strategic nature of controlling access to advanced technologies as one of the aspects of international relations.

ANALYSIS AND SOLUTIONS

The case studies illustrate the range of risks that foreign-manufactured semiconductors pose to national security, each pointing to critical vulnerabilities in global semiconductor supply chains, especially when exploited by adversarial nations for espionage, military advantage, or economic disruption.[34] These cases show the need for heightened security in semiconductor manufacturing, and further, the need for domestic semiconductor manufacturing.

The case studies illustrate a serious gap in current cybersecurity practices, leaving critical infrastructure vulnerable to attack, all impacting national security and

reducing competitive advantage. With the vulnerabilities introduced by foreign-manufactured chips, traditional software-based security is tied to the motherboard or embedded into the hardware rather than the application.[35] Therefore, this matter requires much more stringent scrutiny and control of the semiconductor supply chain, particularly when the chips are sourced from foreign manufacturers.

Another venue is preventing any uncontrolled exfiltration of U.S. semiconductor technology to direct rival countries such as China and Russia. This is critical for protecting critical domestic sectors, national security, and U.S. intellectual property through the enforcement of export control law.[36] Direct export of sensitive technology to adversarial countries can threaten U.S. national security, military edge technology, as illicit of any high technology component, such as semiconductors and chips can enhance a rival nations' military capabilities and shift the balance of power.[37]

The case studies also examined the U.S. export controls that are aimed at limiting rivals like China to access advanced semiconductor technologies,[38] highlighting the geopolitical and economic implications of technological engagement. The restrictions are intended to safeguard national security, preventing China from enhancing its semiconductor manufacturing capabilities. However, they also strain international relations and disrupt global supply chains,[39] illustrating the complexities of technological interdependence in a global economy.[40] While export control laws are necessary for national security, they underscore the need for international collaboration to establish frameworks that prevent the proliferation of sensitive technologies to adversarial nations.

These case studies show that the security risks to semiconductor chip production are complex and inseparable from cybersecurity and international trade. The case studies also stress the necessity of a holistic, comprehensive supply chain approach to safeguard the semiconductor supply chain.[41] A single solution will not suffice; rather, the United States must adopt a layered approach that includes improved supply chain oversight, strengthened export controls, international cooperation, and investment in domestic semiconductor manufacturing.[42]

THE NEED FOR A MULTIFACETED SOLUTION

This article proposes a multifaceted solution framework to address certain vulnerabilities and threats posed by foreign-manufactured microchips and helps to establish domestic and self-sufficiency (see figure 3). The multifaceted framework proposal includes the NIST—Cybersecurity Framework Version 2.0 Semiconductor Manufacturing Profile[43]—in support of the National Semiconductor Security Framework (NSSF). Added to that, the *National Cybersecurity*[44] and *National Security Strategy*[45] help ensure resiliency, a competitive position, and enhance international collaboration and standardization. Moreover, this proposed multifaceted framework would focus on securing the production and distribution of semiconductors and controlling the movement of sensitive semiconductor technologies across the U.S. border.

This multifaceted approach builds on the strength of each entity stated in Figure 3 to ensure self-sufficiency, cybersecurity, competitiveness, export controls and

FIGURE 3: PROPOSED SOLUTION FOR SEMICONDUCTORS PRODUCTION AND EXPORT

national security. The NSSF would consist of several key components. First, **Domestic Manufacturing Incentives** would help strengthen domestic semiconductor manufacturing to reduce reliance on foreign-manufactured chips. This alone could help mitigate against risks from foreign interference and help secure critical infrastructure against sabotage and espionage.[46] Second, there should be **Enhanced Supply Chain Transparency and Security Audits** with routine software and hardware component checks. In the case of import or export, a semiconductor manufacturers should be subject to a rigorous background check to mitigate any possible foreign interference or association.

Third, **International Semiconductor Regulation and Cooperation,** aligned with the *National Security Strategy*, could establish an international procedure joined with standards that will establish the safe semiconductor technology transfer with other nations.[47] Promoting these joint efforts will prevent illegal exports and the sharing of critical technologies, as well as agreements to share intelligence on potential threats. Fourth, **Advanced Detection Technologies** should be used to scan using AI-powered security tools and semiconductors to mitigate vulnerabilities.[48] This would help mitigate hardware backdoors that align with the NIST, *National Security Strategy*, and NCS will enhance resiliency and defense landscape.

CONCLUSION

The increasing reliance on foreign-manufactured semiconductors presents significant risks to national security, economic stability, and technological sovereignty. The case studies examined highlighted threats posed by reliance on foreign semiconductors to national security and critical infrastructure, with the threats to the U.S. geopolitical position, sovereignty, and technological leadership. The United States must address threats raised by the illicit export of semiconductor technology to China, exports by Chinese semiconductor firms, and vulnerabilities inherent in semiconductor supply chains. The threats showed the potential consequences and security gaps introduced by the reliance on foreign-manufactured semiconductors.

The exposure to these risks can lead to espionage, sabotage, and geopolitical manipulation that could leave critical infrastructure and technological advancement vulnerable. The study proposed a comprehensive multifaceted strategy, appropriate for a multifaceted threat, that can help protect domestic manufacturing with strict security considerations for export or technology sharing with foreign countries. The proposed comprehensive solution was developed through a National Semiconductor Security Framework (NSSF), which would include measures such as enhanced domestic manufacturing, stricter supply chain audits, international regulatory cooperation, and advanced detection technologies.

The *National Security Strategy* provides the foundation and is then supported by the National Cybersecurity Strategy (NCS) and the NIST Cybersecurity Framework Version 2.0 Semiconductor Manufacturing Profile—customized NIST guidelines for semiconductor industry-specific risks. The *National Security Strategy* provides a strategic framework that outlines national priorities and objectives, ensuring that semiconductor security is integrated into the broader context of national defense and security. The NCS, on the other hand, offers critical insights into cybersecurity measures that can be applied within the semiconductor sector, addressing vulnerabilities and enhancing resilience against cyber threats.

Together, these frameworks aim to safeguard national infrastructure, maintain U.S. technological superiority, and foster international collaboration to address the evolving challenges posed by semiconductor security. By leveraging the strengths of the NIST-customized guidelines for semiconductor risks, *National Security Strategy,* and NCS with the NSSF, this proposed solution is a robust and comprehensive approach to securing semiconductor supply chains, contributing to national security and economic stability.

NOTES

[1] H. Bardt, K.H. Röhl, and C. Rusche, "Subsidizing Semiconductor Production for a Strategically Autonomous European Union?" *The Economists' Voice*, 19(1) (2022), 37-58.
[2] C.P. Brief, "Sustaining US Competitiveness in Semiconductor Manufacturing," (2022).
[3] J. Lynn, *Cybersecurity Framework Version 2.0 Semiconductor Manufacturing Profile* (2025), https://doi.org/10.6028/nist.ir.8546.ipd.
[4] J.V. Camps and A. Saz-Carranza, "The European Chips Act: Europe's Quest for Semiconductor Autonomy," *Center for Global Economy and Geopolitics* (2023), 10-17.
[5] X. B. K. Hah, "Security and Supremacy: An Examination of the US-China Technological Rivalry in The Semiconductor Industry," *Malaysian Journal of International Relations*, 12(1) (2024), 140-160.
[6] Tech, *Securing the Supply Chain,* February 4, 2025, https://www.techinsights.com/case-study/securing-supply-chain.
[7] Steve Blank, *The Semiconductor Ecosystem,* January 25, 2022, available from: https://steveblank.com/2022/01/25/the-semiconductor-ecosystem/

[8] K. Stroh, "The Overlooked Security Risks of Onshoring Chip Production," *Supply Chain Dive*, December 19, 2023, https://www.supplychaindive.com/news/security-risks-of-onshoring-chip-production-opinion/702629/; A.H.C. Hung, "Chip Legislative Endeavors in the United States and European Union: A Comparative Analysis Based on China's Disruptive Production Technologies," *U. Ill. JL Tech. & Pol'y* (2024), 297; S. Shivakumar and C Wessner, *Semiconductors and National Defense: What Are the Stakes?*, Center for Strategic and International Studies, June 8, 2022, https://www.csis.org/analysis/semiconductors-and-national-defense-what-are-stakes.

[9] Sajjad, *Adapting to Change – Exploring the Challenges and Opportunities in Semiconductor Manufacturing for the Next Decade*. Nanogenius, November 21, 2024, https://nanogenius.in/case-study/adapting-to-change-exploring-the-challenges-and-opportunities-in-semiconductor-manufacturing-for-the-next-decade/

[10] K. Jacobsen, "Microchips and Public Policy–The Political Economy of High Technology," *British Journal of Political Science*, 22(4) (1992), 497-519.

[11] A.B. Janjua, "Analysis of Semiconductor Competition as New Dimension of Super-Power Rivalry Between US and China," *Pakistan Social Sciences Review, 8(*2) (2024), 300-311.

[12] A. Ramesh, "De-risking Semiconductor Supply Chains," Hinrich Foundation Report (2023), https://pacforum.org/wp-content/uploads/2023/09/De-risking-semiconductor-supply-chains-Rob-York-Akhil-Ramesh-Hinrich-Foundation-September-2023.pdf.

[13] J. Kawar, "The CHIPS and Science Act: The United States' Race for Semiconductor Sovereignty."

[14] Microchip Technology Inc., *DM182017-4: Development Tool* (2023), retrieved from https://www.microchip.com/en-us/development-tool/dm182017-4

[15] S. Krivic and J.C. Defraigne, "Semiconductor autonomy of the EU in the context of the China-Taiwan conflict: Is the EU going to be self-sufficient?"

[16] R.R. Lamsal, A. Devkota, and M. S. Bhusal, "Navigating Global Challenges: The Crucial Role of Semiconductors in Advancing Globalization," *Journal of The Institution of Engineers (India): Series B*, 104(6) (2023), 1389-1399.

[17] P.A. Purohit, "Chip Wars: The Struggle for Semiconductors Supremacy," *Air Power Journal*, 19(2) (2024), 21-42.

[18] H. Bardt, K.H. Röhl, and C. Rusche, "Subsidizing Semiconductor Production for a Strategically Autonomous European Union?" *The Economists' Voice*, 19(1) (2022), 37-58.

[19] F. Spigarellia and G. Sampaolo, "Semiconductors dominance and global supply chain: de-coupling or simply de-risking?" (2023).

[20] Politics of Defence, *Semiconductors and National Security in the 21st Century: Risks of Foreign Dependency - Politics to Defense*, December 11, 2024, https://politicstodefense.com/semiconductors-and-national-security-in-the-21st-century-risks-of-foreign-dependency/.

[21] Christopher Miller, *Chip War: The Fight for the World's Most Critical Technology* (New York: Simon and Schuster, 2022).

[22] T. Force, "High Performance Microchip Supply," *Annual Report. Defense Technical Information Center* (DTIC, 2005).

[23] K. Flamm, *Mismanaged Trade?: Strategic Policy and the Semiconductor Industry* (Washington, DC: Brookings Institution Press, 2010).

[24] S.F. Sadiq, Competition in the production of Electronic Microchips (Semiconductors) as an issue in US–China relations (2023).

[25] R.R. Lamsal, A. Devkota, and M.S. Bhusal, "Navigating Global Challenges: The Crucial Role of Semiconductors in Advancing Globalization," *Journal of The Institution of Engineers (India): Series B*, 104(6) (2023), 1389-1399.

[26] D. Ernst, *Supply Chain Regulation in the Service of Geopolitics: What's Happening in Semiconductors?* (No. 256) (2021), CIGI Papers.

[27] C.P. Bown, "How the United States marched the semiconductor industry into its trade war with China," *East Asian Economic Review*, 24(4) (2020), 349-388.

[28] U.S. President, *National Cybersecurity Strategy Implementation Plan: Version 2* (2024), https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/05/National-Cybersecurity-Strategy-Implementation-Plan-Version-2.pdf

[29] C. Brown, G. Linden, and J.T. Macher, "Offshoring in the Semiconductor Industry: A Historical Perspective," [with comment and discussion] in *Brookings Trade Forum* (pp. 279-333). (Washington, DC: Brookings Institution Press, 2025).

[30] J. Mark and D.T. Roberts, "United States–China Semiconductor Standoff: A Supply Chain under Stress," Atlantic Council (2023), 23.

[31] U.S. President, *Biden-Harris Administration's National Security Strategy* (2022), https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

[32] M.D. Platzer and J.F. Sargent, *US Semiconductor Manufacturing: Industry Trends, Global Competition, Federal Policy*, R44544 (Washington, DC: Congressional Research Service, 2016).

[33] Platzer and Sargent, *US Semiconductor Manufacturing*.

[34] C.P. Bown and D. Wang, "Semiconductors and Modern Industrial Policy," *Journal of Economic Perspectives*, 38(4) (2024), 81-110.

[35] S. Donnelly, "Semiconductor and ICT Industrial Policy in the US and EU: Geopolitical Threat Responses," *Politics and Governance*, *11*(4) (2023), 129-139.

[36] S.M. Khan, A. Mann, and D. Peterson, "The Semiconductor Supply Chain: Assessing National Competitiveness," *Center for Security and Emerging Technology*, 8(8) (2021), 1-98.

[37] M.T. Ciani, "Foreign Investment and National Security: Navigating Heightened Scrutiny of US, EU and UK Cross-Border Deals," *National Law Review* (2024), https://natlawreview.com/article/foreign-investment-and-national-security-navigating-heightened-scrutiny-us-eu-and

[38] EXIGER, *Chip Challenges: Semiconductors and Supply Chain Risks*. Exiger, January 2, 2025, https://www.exiger.com/perspectives/chip-challenges-semiconductors-and-supply-chain-risks/.

[39] M. Hutchinson, "America's Semiconductor Dependence: A Ticking Time Bomb for National Security," *The Defense Post*, November 21, 2024, https://thedefensepost.com/2024/11/21/us-semiconductor-dependence-national-security/

[40] A. Keiser, *The Supply Chain Risks of Foreign-made Technologies*, RealClearPolicy. November 2024, https://www.realclearpolicy.com/2024/11/01/the_supply_chain_risks_of_foreign-made_technologies_1069337.html

[41] J.A. Lewis, *Risks in the Semiconductor Manufacturing and Advanced Packaging Supply Chain* (Washington, DC: Center for Strategic and International Studies, 2021), https://www.csis.org/analysis/risks-semiconductor-manufacturing-and-advanced-packaging-supply-chain

[42] S. Patil, *Expanding National Security Risks from Foreign-Manufactured Hardware*, Observer Research Foundation (January 31, 2025), https://www.orfonline.org/expert-speak/expanding-national-security-risks-from-foreign-manufactured-hardware

[43] National Institute of Standards and Technology, *NIST* Internal Report *8546:* Cybersecurity Framework Version 2.0 Semiconductor Manufacturing Profile (2025), https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8546.ipd.pdf.

[44] U.S. President, *National Cybersecurity Strategy Implementation Plan: Version 2* (2024), https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/05/National-Cybersecurity-Strategy-Implementation-Plan-Version-2.pdf

[45] U.S. President, *Biden-Harris Administration's National Security*

Strategy (2022), https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

[46] B. Martin, et. al. *Supply Chain Interdependence and Geopolitical Vulnerability: The Case of Taiwan and High-End Semiconductors* (Santa Monica, CA: RAND, 2023), https://www.rand.org/pubs/research_reports/RRA2354-1.html

[47] M. Min, "Chip Security: Reconciling Industrial Subsidies with WTO Rules and National Security Exception," *Harvard National Security Journal* (2025), https://harvardnsj.org/2025/01/12/chip-security-reconciling-industrial-subsidies-with-wto-rules-and-national-security-exception/

[48] OECD Science, *Vulnerabilities in the semiconductor supply chain*. OECD (2024), https://www.oecd.org/en/publications/vulnerabilities-in-the-semiconductor-supply-chain_6bed616f-en.html.

Matelier Numbi is an MBA candidate at Southern Utah University with a concentration in Project Management. He is a Project Manager at MCM Engineering2 and serves as the Fundraising Chairman for the National Society of Leadership and Success (NSLS). He holds a Bachelor's degree in Electrical and Electronics Engineering from Southern Utah University (SUU). His research focuses on the integration of artificial intelligence in business, particularly in facilitating managerial decision-making.

Gaston Elongha is a PhD candidate in cybersecurity at Marymount University. He is focusing on Cybersecurity and defensive AI. His research explores the intersection of artificial intelligence and cybersecurity across critical sectors including national security, healthcare, and beyond. As an experienced cybersecurity expert and passionate advocate for technological innovation, he is committed to developing proactive strategies to safeguard against current and emerging cyber threats.

2024 Night of Heroes Keynote Speakers:

Lieutenant Karen Gibson, USA, (RET)

Rear Admiral Paul Becker, USN, (RET)

Social Media and Algorithms Growing Far-Right Masculinities and White Supremacy

by **Yenting Lin**

INTRODUCTION

Hate speech and hate crimes are rising at an alarming rate, fueled in large part by social media platforms that provide extremist groups with an easily accessible space to spread their ideologies. According to the 2023 Hate Crime Statistics Report published by the Federal Bureau of Investigation (FBI), there were 11,834 reported hate crime incidents in 2022, marking a 7 percent increase from the previous year.[1] The 2022 Domestic Terrorism Report, published by the U.S. Department of Justice (DoJ) states that over 60 percent of domestic terrorist incidents in the past decade were linked to white supremacist and far-right extremist ideologies.[2] The UN Office on Drugs and Crime (UNODC) has also warned that social media serves as an accelerant for extremism, increasing recruitment efforts by 400 percent in the last five years.[3]

Social media fueled hate speech through algorithmic recommendations that prioritize engagement over content moderation. Research from the Department of Homeland Security indicates that far-right propaganda spreads three times faster on social media than traditional news media, making it difficult for law enforcement agencies to intervene before radicalization escalates into violence.[4] The Southern Poverty Law Center has documented a 33 percent rise in online hate groups since 2019, demonstrating how digital platforms continue to be used for extremist purposes.[5] The Center for Strategic and International Studies reports that white supremacist attacks in the United States increased by 55 percent over the past decade, with most attackers radicalized online.[6] The 2022 Buffalo supermarket shooting is a prime example, in which an 18-year-old, influenced by white supremacist beliefs on 4chan, targeted a predominantly black community and killed 10 people.[7] Similarly, the 2019 El Paso Walmart shooting, which resulted in 23 deaths, was driven by anti-immigrant rhetoric. The shooter posted a manifesto online minutes before the attack, referring to "The Great Replacement" conspiracy theory.[8]

The "Great Replacement" conspiracy theory falsely claims that elites are orchestrating the demographic replacement of white populations through immigration. A 2023 study by the Institute for Strategic Dialogue found that discussions around this theory increased by 500 percent on far-right Telegram channels between 2016 and 2022.[9] This article examines how social media algorithms contribute to the radicalization of users into far-right extremist ideologies, with a particular focus on platforms like Telegram, X (formerly Twitter), and Instagram. The purpose of this article is to analyze the role of algorithmic amplification in the spread of white supremacist narratives and to evaluate the policy, legal, and intelligence gaps that hinder effective countermeasures.

In addition to its public policy focus, this article directly engages with the priorities of the U.S. intelligence community (IC). As domestic extremism increasingly migrates to online platforms, the IC faces new challenges in tracking and countering radicalization in real-time. This paper contributes to that conversation by evaluating how algorithmic amplification, encrypted communications, and decentralized extremist networks complicate traditional intelligence practices. By examining the role of OSINT, interagency collaboration, and machine learning tools, the article offers insight into how intelligence frameworks must evolve to address the growing digital dimensions of far-right extremism.

THE DIGITAL ECOSYSTEM OF FAR-RIGHT EXTREMISM

Far-right extremist groups such as The Base, Atomwaffen Division, and the Proud Boys actively exploit social media to recruit new members and communicate using coded language. According to a RAND Corporation study, these groups use a mix of ironic memes, dog whistles, and encrypted messaging platforms to radicalize individuals. Slogans such as "White Genocide," "Race War Now," and "Reclaim America" are frequently circulated in online extremist communities.[10]

Social media platforms such as Twitter (now X), YouTube, and Reddit have facilitated the rapid spread of far-right masculinist ideologies. A study by The Center for Countering Digital Hatefound that far-right influencers and misogynistic extremist groups

saw a 54 percent increase in engagement on YouTube between 2019 and 2023, largely due to the platform's recommendation algorithm.[11] This phenomenon, referred to as the "algorithmic radicalization pipeline," is particularly effective in attracting young men to misogynistic and white supremacist narratives.[12]

According to a Harvard Kennedy School study, these platforms serve as recruitment grounds for "lone wolf" attackers who consume content linking perceived gender to broader racial conspiracy theories.[13] The "Manosphere" theory refers to the digital subculture that promotes anti-feminist, hypermasculine ideologies. Many young men radicalized online transition from general misogynistic beliefs into white supremacist movements, believing that feminism and multiculturalism threaten Western civilization.[14] The Incel Terrorism theory is based upon studies from the International Centre for Counter-Terrorism indicate that incel forums have become breeding grounds for mass shooters.[15] Several perpetrators of mass violence, including the 2018 Toronto van attack and the 2022 Buffalo supermarket shooting, were influenced by incel and white supremacist ideologies spread online. The "Great Replacement" Theory is a conspiracy theory, promoted on Telegram, Gab, and Twitter accounts, and it claims that immigrants and minorities are systematically replacing white men.[16] It has inspired multiple acts of terrorism, including the 2019 Christchurch Mosque shootings and the 2022 Buffalo attack.

ALGORITHMIC AND EXTREMIST PROPAGANDA

A major challenge in combating far-right digital extremism is the role of social media algorithms in recommending extremist content. Research from the Shorenstein Center at Harvard University found that Facebook's algorithm disproportionately recommended extremist content to users who had interacted with mildly controversial political material.[17] There were three important findings: The first involved YouTube's Auto-Play Feature: A 2023 study by The Stanford Internet Observatory found that YouTube's recommendation algorithm increased exposure to extremist content by 35 percent after a user initially engaged with videos discussing male disenfranchisement or nationalist ideologies.[18] The second involved Twitter and Coded Language: Extremist groups use coded hashtags and dog-whistle phrases to evade moderation. The Atlantic Council's Digital Forensic Research Lab identified a 35 percent increase in the use of "soft radicalization" techniques, such as humor and irony, to spread far-right messages.[19] The third involved Facebook Groups and Disinformation Networks: The European Commission's 2023 report on online extremism revealed that private Facebook groups dedicated to far-right ideologies grew by 67 percent from 2020 to 2023, illustrating how platforms provide radical networks.[20]

This leads to several important research questions: How can the U.S. government regulate online extremism while balancing First Amendment protections? How do existing legal and policy frameworks—such as Section 230—limit efforts to moderate extremist content on social media? How might international models of social media regulation inform a more effective U.S. policy approach?

GOVERNMENT STRUGGLES TO REGULATE ONLINE EXTREMISM

The First Amendment of the U.S. Constitution protects freedom of speech, making it difficult to regulate online content unless it directly incites violence, where social media platforms are not legally required to remove hate speech. Section 230 of the Communications Decency Act further shields tech companies from liability, preventing victims of extremist violence from suing platforms that host radicalizing content.[21] The Matthew Shepard and James Byrd Jr. Hate Crimes Prevention Act expanded hate crime protections but did not address the online dissemination of extremist propaganda.[22]

The U.S. Supreme Court ruled that social media platforms secure a big win against government regulation. In *Twitter v. Taamneh* (2023) the Court ruled that social media platforms cannot be held liable for terrorist content unless they actively aid terrorist activities.[23] Platforms are not responsible for user-generated content unless direct complicity is proven. In *Gonzalez v. Google* (2023) the Court examined whether YouTube's algorithmic amplification of extremist content constitutes material support for terrorism. The ruling favored Google, emphasizing that platforms are not legally liable for how their algorithms promote content.[24] In *Missouri v. Biden* (2023) the Court highlighted tensions between government pressure on social media platforms and constitutional protections against state-imposed censorship. The ruling limited the federal government's ability to force platforms to remove content, complicating counter-extremism efforts.[25]

Think tanks have different perspectives on countering extremism. The Brookings Institution recommends mandatory transparency reports for social media companies to disclose how algorithms promote radicalizing content.[26] The Carnegie Endowment for International Peace advocates for expanded digital literacy programs to prevent youth radicalization. The Council on Foreign Relations suggests that tech companies be legally required to implement AI-driven content moderation to flag extremist content more effectively. The Southern Poverty Law Center warns that far-right extremist groups are becoming increasingly decentralized, using apps to bypass social media bans.[27]

U.S. INTELLIGENCE EFFORTS TO COMBAT DIGITAL EXTREMISM: OSINT

The FBI, Central Intelligence Agency (CIA), and Department of Homeland Security (DHS) employ open-source intelligence (OSINT) techniques to track extremist activities across social media platforms and dark web forums. However, privacy laws and encryption technology continue to limit their ability to monitor extremist content. According to the Office of the Director of National Intelligence, OSINT monitoring contributed to 42 percent of domestic terrorism case leads in the past two years.[28]

Despite this, intelligence officials report that up to 75 percent of online extremist discussions occur on encrypted platforms like Telegram and Signal, making real-time interventions difficult.[29] Federal law enforcement agencies have urged Congress to expand legal authorities for tracking encrypted communications, but these efforts face opposition from privacy advocacy groups.[30] The National Counterterrorism Center (NCTC) and Cybersecurity and Infrastructure Security Agency (CISA) have applied machine learning algorithms to detect online extremism and radicalization patterns. CISA's Threat Analysis System (TAS) processed 8.2 million extremist-related social media posts in 2023, marking a 47 percent increase from 2021.[31] Machine learning models developed by the FBI Cyber Division have improved the detection of extremist propaganda by 61 percent, but challenges remain in identifying coded hate speech and meme-based radicalization.[32]

The United States has worked through some intelligence liaison partners, such as the Five Eyes Intelligence Alliance (United States, the United Kingdom, Canada, Australia, and New Zealand), the International Criminal Police Organization, and the United Nations Counterterrorism Committee to track digital extremist networks that operate beyond U.S. borders.

REAL-LIFE INTELLIGENCE OPERATIONS AND CASE STUDIES

There are several useful examples that illustrate how the government can combat digital extremism. In a real-life case, the FBI, CIA, and DHS coordinated to disrupt white supremacist networks operating on the dark web. The operation resulted in the shutdown of three neo-Nazi propaganda sites and the identification of over 2,000 extremist-linked accounts. The Pentagon's Project Sentinel, an AI-powered extremist tracking system, successfully flagged 742 high-risk individuals, leading to preventive interventions by federal agencies. The DoJ launched a cybersecurity-focused unit, Cybersecurity Task Force for Online Radicalization, in the National Security Division (NSD) to track the digital financing of extremist groups, which led to the freezing of $3.7 million in cryptocurrency linked to domestic terrorist cells.[33] In 2023, the Joint Terrorism Task Force (JTTF) successfully infiltrated private Telegram groups that neo-Nazi groups coordinated real-world attacks. This led to six arrests and the prevention of a planned attack on a government building.

Community Awareness programs can play a key role in preventing radicalization before it escalates into violent extremism. These programs focus on educating local law enforcement, schools, and community leaders on the warning signs of radicalization. The DoJ reported in 2023 that CAPs led to the early identification of 389 individuals at risk of violent extremism, preventing potential domestic terror threats.[34] One of the most notable CAP initiatives is "Don't Be a Puppet," an online tool designed to help young people recognize recruitment tactics used by extremist groups. Since its launch, the program has reached over 1.2 million students and educators nationwide.[35] Despite its success, critics argue that CAPs require more funding and better coordination with digital platforms to counteract online radicalization effectively.

COMMUNITY EFFORT: NGOS PUBLIC AWARENESS CAMPAIGNS & EDUCATION

Empowering communities through education and public awareness is essential for countering the spread of online far-right extremism and hate speech. Non-governmental organizations (NGOs) and academic institutions have been instrumental in launching comprehensive educational programs and awareness campaigns to build resilience against digital radicalization.

The Anti-Defamation League (ADL) has implemented the "Best Practices for Challenging Extremism" initiative, which trains over 10,000 educators annually on identifying and countering hate speech in schools. Additionally, the Institute for Strategic Dialogue (ISD) has developed the "Be Internet Citizens" program, which will reach over 150,000 students in the United States and the UK by 2023, teaching critical thinking and digital literacy skills to resist extremist propaganda. The Global Project Against Hate and Extremism (GPAHE) has launched the "Words Matter" campaign, which uses social media ads and YouTube videos to debunk far-right conspiracy theories.

PRIVATE SECTOR SOLUTIONS: BIG TECH COMPANY

Governments typically rely on social media companies, NGOs, and private cybersecurity firms to combat online extremism. There have been a range of promising initiatives. Tech companies such as Meta, Google, and Twitter have used AI-driven moderation tools to remove hate speech and extremist content. A 2023 report by Google's Jigsaw division found that AI-powered filters removed 82 percent of flagged extremist content within minutes of detection. However, these systems can still fail to detect 40 percent of coded extremist content, highlighting ongoing challenges. The Global Internet Forum to Counter Terrorism (GIFCT) was originally founded by Facebook, Microsoft, Twitter, and YouTube; this coalition works alongside U.S. intelligence agencies to share digital fingerprints of extremist content. In 2023, GIFCT reported removing 14.5 million pieces of extremist material from online platforms.

Platforms have also begun de-prioritizing extremist content through Digital Identity Verification and shadowbanning, reducing its reach without outright censorship. TikTok's shadowbanning policy led to a 70 percent reduction in far-right extremist engagement within a year of implementation. However, civil liberties groups have raised concerns about overreach and potential biases in these measures. Finally, there have been helpful partnerships between Think Tanks and NGOs. Organizations like the Anti-Defamation League (ADL), Southern Poverty Law Center (SPLC), and the Center for Strategic and International Studies (CSIS) have conducted independent research and provided policy recommendations to tech companies and lawmakers. The ADL's 2023 "Hate on the Internet" report called for stricter algorithmic transparency and enhanced AI monitoring of extremist content.[36]

INTERNATIONAL COMPARISON

The European Union (EU), as well as several foreign countries, offer alternative examples of regulatory frameworks that can address online extremism. The EU adopted a 2023 Digital Services Act that requires platforms to remove hate speech within 24 hours or face significant fines. It also mandates algorithmic transparency and enhanced content moderation policies. While effective in Europe, this model faces challenges in the United States due to First Amendment protections, that limits government intervention in online speech. Germany adopted a 2017 statute, the NetzDG Law, that requires social media platforms to report extremist content to law enforcement and holds companies criminally liable for failing to remove harmful content. While this approach has strengthened accountability in Germany, it conflicts with Section 230 in the United States, which shields platforms from liability for user-generated content.

The United Kingdom adopted a 2023 Online Safety Act that requires platforms to assess and mitigate algorithmic risks associated with extremist content. It also mandates transparency in content moderation policies. Adopting a similar framework in the United States would require significant regulatory reforms and potentially new federal oversight agencies. Taiwan has AI-Powered Disinformation & Hate Speech Tracking; this allows Taiwan to leverage AI-driven fact-checking systems and government-backed digital identity verification to track and mitigate the spread of online extremism. While this model has successfully reduced misinformation, implementing similar measures in the United States may raise privacy concerns and face public resistance.

POLICY RECOMMENDATIONS

There are several actions that the new Trump administration could adopt. Section 230 of the Communications Decency Act could be amended to require social media companies to implement more rigorous content and transparency for algorithmic recommendations. The administration could adopt new legislation on algorithmic accountability; this mandate could require social media platforms to conduct annual transparency reports. The administration could expand OSINT capabilities for the FBI and CIA by allocating increased funding for AI-driven OSINT tools. Next, the administration could strengthen the National Counterterrorism Center (NCTC); this could enhance inter-agency cooperation to track far-right networks across state lines. There could be new federal grants

for digital literacy programs; the administration could establish a Digital Resilience Fund to support NGO-led educational initiatives. The administration could encourage partnerships between federal agencies and academic institutions to develop evidence-based against extremist ideology.[37] Finally, the administration could create data-sharing agreements; such agreements could set up Secure Data Exchange Programs between the DOJ, DHS, and tech companies.

CHALLENGES & CONCLUSION

The January 6, 2021, attack on the U.S. Capitol demonstrated how social media algorithms and far-right networks can escalate online extremism into real-world violence, with platforms like Parler, Facebook, and Telegram witnessing a 230 percent surge in far-right content before the attack.[38] President Donald Trump's pardon of nearly 1,600 convicted persons in January 2025 has further emboldened extremist factions and undermined public trust in the government's ability to combat domestic terrorism. The FBI and CIA face limitations due to legal restrictions and a lack of sufficient resources to monitor the scale of online extremism. Efforts to address domestic extremism face substantial legal barriers, including First Amendment protections and the limitations of Section 230 of the Communications Decency Act. Moreover, the CIA is legally barred from conducting domestic surveillance under the 1947 National Security Act.

The new Trump administration also poses a challenge to combat online terrorism: First, there are proposed cuts in the federal budget. Federal agencies have faced reductions in digital surveillance funding. The Cybersecurity and Infrastructure Security Agency (CISA) has reported that these cuts will reduce proactive monitoring capabilities by 30 percent.[39] Second, there are legal barriers to online surveillance: The Constitution limits how intelligence agencies monitor social media content, making it more difficult to track radicalization before it leads to violence. Privacy advocacy groups have filed lawsuits challenging expanded surveillance programs.[40] Third, there have been shifting priorities under the new leadership: The FBI and DoJ are refocusing efforts on state-sponsored cyber threats, potentially diverting resources away from domestic extremism investigations. Lawmakers have raised concerns that this shift may increase the risk of far-right violence going undetected.

With new leadership at the FBI and DoJ, the U.S. government must confront the ongoing challenge of balancing freedom of speech with national security. The future of counter-extremism policy will likely depend on a combination of stricter social media regulation, enhanced intelligence efforts, and international cooperation. Without a comprehensive policy response that balances constitutional rights and national security, far-right extremism will continue to threaten democratic institutions and public trust in the United States.

NOTES

[1] Federal Bureau of Investigation, *Hate Crime Statistics Report* (Washington, DC: FBI, 2023).
[2] U.S. Department of Justice, *Domestic Terrorism Analysis Report* (Washington, DC: DoJ, 2022).
[3] UN Office on Drugs and Crime, *Global Extremism and Social Media Analysis* (Vienna: United Nations, 2023).
[4] Department of Homeland Security, *Threat Assessment Report on Online Extremism* (Washington, DC: DHS, 2023).
[5] Southern Poverty Law Center, *Hate Groups and Digital Extremism: Annual Report* (Montgomery, AL: SPLC, 2023).
[6] Center for Strategic and International Studies, *U.S. Domestic Terrorism Trends: 2013-2023* (Washington, DC: CSIS, 2023).
[7] U.S. Department of Justice, *Domestic Terrorism Analysis Report* (Washington, DC: DoJ, 2022).
[8] Federal Bureau of Investigation, *Hate Crime Statistics Report* (Washington, DC: FBI, 2023).
[9] Institute for Strategic Dialogue, "Tracking the Spread of the 'Great Replacement' Theory on Social Media," 2023.
[10] RAND Corporation, *The Role of Online Communities in Far-Right Radicalization* (Santa Monica, CA: RAND Corporation, 2022).
[11] Center for Countering Digital Hate, "Deadly by Design: TikTok's Algorithm Fuels Eating Disorder Crisis," 2022.
[12] R. Lewis, "The Algorithmic Radicalization Pipeline: How Recommendation Systems Drive Extremism Online," *Journal of Digital Media & Society* 12(3) (2023): 45-62.
[13] Harvard Kennedy School, "Digital Radicalization and Algorithmic Reinforcement," (Cambridge, MA: Harvard University, 2023).
[14] D. Ging, "From Misogyny to White Supremacy: Online Radicalization and the Threat to Democracy," *Journal of Media & Politics* 15(2) (2023): 112-130.
[15] International Centre for Counter-Terrorism, "Incel Terrorism: Online Radicalization and Mass Violence," ICCT Research Report (2023).
[16] Anti-Defamation League, "The 'Great Replacement' Theory: How a Racist Conspiracy Thrives Online," ADL Research Report, 2024.
[17] Center on Media, Politics and Public Policy, "Facebook's Algorithm and its Role in Recommending Extremist Content," Harvard University (2024).
[18] Stanford Internet Observatory, "YouTube's auto-play and the amplification of extremist content," Stanford University (2023).
[19] Atlantic Council's Digital Forensic Research Lab, "Soft Radicalization: The Use of Humor and Irony in Far-Right Messaging," The Atlantic Council, 2023.
[20] European Commission, "Report on Online Extremism: Growth of Far-Right Networks on Social Media," European Commission, 2023.
[21] *Communications Decency Act*, 47 U.S.C. § 230 (1996).
[22] *Matthew Shepard and James Byrd Jr. Hate Crimes Prevention Act*, 18 U.S.C. § 249 (2009).
[23] *Twitter, Inc. v. Taamneh*, 598 U.S. (2023).
[24] *Gonzalez v. Google LLC*, 598 U.S. ___ (2023).
[25] *Missouri v. Biden*, 83 F.4th 350 (5th Cir. 2023).
[26] Brookings Institution, "Mandatory Transparency Reports: Regulating Algorithmic Amplification of Extremist Content on Social Media Platforms," Brookings, 2024.

[27] Southern Poverty Law Center, *The Year in Hate & Extremism* (2023).
[28] Office of the Director of National Intelligence, *The IC OSINT Strategy 2024-2026* (2024).
[29] Office of the Director of National Intelligence, *The IC OSINT Strategy 2024-2026* (2024).
[30] Electronic Frontier Foundation, "Federal Surveillance and Encrypted Communications: The Ongoing Debate," EFF Policy Report, 2024.
[31] Cybersecurity and Infrastructure Security Agency, *Threat Analysis System Annual Report: Trends in Extremist Content Online* (Washington, DC: U.S. Department of Homeland Security, 2023).
[32] Harvard Kennedy School, *Advances and Challenges in AI-Driven Extremism Detection* (Cambridge, MA. Harvard University, 2024).
[33] U.S. Department of Justice, *Domestic Terrorism Analysis Report* (Washington, DC: DoJ, 2022).
[34] U.S. Department of Justice, *Domestic Terrorism Analysis Report* (Washington, DC: DoJ, 2022).
[35] U.S. Department of Justice, *Domestic Terrorism Analysis Report* (Washington, DC: DoJ, 2022).
[36] Anti-Defamation League, "Hate on the Internet: The Need for Algorithmic Transparency and AI Monitoring," 2024.
[37] Harvard Kennedy School, "Developing Evidence-Based Strategies Against Extremist Ideologies," 2024.
[38] U.S. Department of Justice, "Investigation of Digital Platforms and Extremist Content Preceding January 6," (Washington, DC: U.S. Government Publishing Office, 2022).
[39] U.S. Department of Justice, "Cybersecurity and Infrastructure Security Agency Budget Impact Analysis," (Washington, DC: DoJ, 2024).
[40] "Privacy Groups Challenge Expanded Surveillance Programs," BBC News, 2024.

Mr. Yenting Lin is currently pursuing a Master of Public Policy at George Mason University, supported by a Dean's Fellow Award. He holds a B.A. and B.S. degree from National Chung Cheng University.

2024 NMIF Scholarship Recipients

Unitary Executive Theory, Original Intent, and the Commander-in-Chief Authority to Use Military Force

by **LTC Johnny B. Davis, U.S. Army Reserve**

The modern era has seen the rise of the Unitary Executive Theory, which holds that the Constitution's Article II executive gives the President unchecked Commander-in-Chief (CINC) authority to use military force. The Unitary Executive Theory goes against the original intent of the Founding Fathers. The 1776 Declaration of Independence justified the foundation of a new republic in response to the King's abuses of power and violations of the rule of law.[1] The Founding Fathers' chief concern was guarding against executive abuses. The reassurance that George Washington, known for his moderation in exercising power, persuaded the founders to create an executive branch.[2] The original intent of the President's CINC authority was to give the President operational authority over the nation's military policy.[3] However, executive power is subject to congressional authority and direction, while the decision to take the nation to war is reserved for Congress. The President has sole authority only for immediate response to attacks upon the United States or under treaty obligations.[4]

The Unitary Executive Theory holds that the President has complete executive branch authority and that his CINC authority is not subject to congressional authority except in some limited situations. The proponents argue that the President can use military force in other nations without congressional authorization. Congressional authority is restricted to merely defunding a military operation that Congress disapproves of.[5] However, defunding a military operation already in progress is inherently dangerous and politically risk, rendering it a near-meaning restriction.

BACKGROUND FOR THE COMMANDER-IN-CHIEF AUTHORITY

Article II does not set forth the specific powers that flow from CINC authority. At the same time, Article I gives Congress specific powers to punish crimes on the high seas, declare war, grant letters of Marque and reprisal, raise and support armies, create a navy, regulate military forces, call forth the militia, and provide for the organization and discipline of the militia.[6] The Unitary Executive Theory proponents stress Article II, vesting the President with executive authority.[7] The authority is subject to congressional checks such as congressional control of declaring war, authority to regulate the military, and complete fiscal authority.[8]

Presidential authority is rooted in the example of George Washington's leadership in the Revolutionary War as CINC of the Continental Army.[9] The title of CINC originated in the English Civil War, and the founding fathers understood its meaning. Parliament chose the CINC, who was required to obey Parliament's orders. Washington wrote to the Continental Congress seeking permission for many wartime decisions and waited for Congress's approval before implementing his proposals. He did so despite many difficulties created by congressional control.[10]

The 1776 Declaration of Independence justified the foundation of a new republic by pointing to the King's abuses of power and violations of the rule of law.[11] The Founding Fathers were central to avoiding executive abuses. Therefore, they created a chief executive with limited authority, primarily as the CINC of the nation's military forces. However, even the CINC was subject to congressional regulation, and only Congress authorized the creation, size, and equipping of the nation's armed forces.[12] Professor John Yoo, formerly an attorney advisor with the Office of Legal Counsel at the Department of Justice, is a leading advocate for the Unitary Executive Theory. He claims that the Unitary Executive can be justified using original intent. He most often cites Hamilton's arguments in *Federalist* 74 for energy in the executive branch and a "single hand." Hamilton discusses the prosecution of war: "Of all the cares or concerns of government, the direction of war most peculiarly demands those qualities which distinguish the exercise of power by a single hand."[13]

Hamilton was not, however, arguing that the Constitution provided broad authority for the President to be free from congressional regulations. He defended

the constitutional convention's decision to reject a plural executive branch. A three-person executive branch based on the Roman Republic's Trivium had been proposed and rejected at the Constitutional Convention.[14]

Hamilton addressed the arguments of anti-federalists who opposed the creation of a presidency. He addressed the balance of authority between the President and Congress. Many Anti-Federalists wished to keep Congress in sole charge of the federal government and allow Congress to oversee any agencies without any Executive branch of government.[15]

Article II gives the President, as CINC, operational and tactical military control.[16] Congress can regulate the military in substantive ways, including using force.[17] Article I gives Congress the authority to declare war, raise and support armies, create a navy, regulate military forces, call forth and regulate[18] The Constitution restricted law-making authority to Congress and the purse's power. The legislative branch was intended to be the most potent branch to protect liberty. The legislative branch remained dominant throughout the 19th century, and presidents generally respected the constitutional limits on their authority.[19]

The Civil War tested the boundaries of presidential command-in-chief authority. President Abraham Lincoln faced the modern questions of lawful and unlawful combatants, fighting an insurgency, and respecting the rule of law on the home front. Lincoln respected the limits on his authority and upheld the original intent of limited CINC authority and respect for Congress's authority.[20] Lincoln faced the greatest crisis of the American Republic yet respected the limits of his power.

Lincoln understood that the law of war governed his conduct of the war. Reacting to the horrific nature of the war, Lincoln sought to strengthen the rule of law over the Union Army. He directed that the law of war be put into a formal code of military regulations, leading to the creation of the Lieber Code.[21]

When the Civil War began, Congress was not in session. Lincoln made several dramatic moves to preserve the nation. A blockage on Southern ports was proclaimed, which was justified because it was a civil war, and the Southern states were part of the nation.[22] Lincoln recognized the Southern states as belligerents and thus complied with the requirements of the laws of war.[23]

Lincoln's most controversial presidential power use was suspending the writ of habeas petitions of persons arrested by the military for helping the Confederacy. Lincoln authorized generals to detain persons without conforming to the standard procedural requirements.[24] Lincoln permitted the disregard of judicial orders to produce persons.[25] Lincoln insisted that he only had the authority to take this action because Congress was out of session, and the nation's preservation was at stake. He accepted that his actions were subject to the will of Congress.[26]

Congress ratified Lincoln's actions in 1861, except for suspending the habeas corpus. However, in 1863, Congress enacted a statute that authorized some restrictions on habeas corpus but less than Lincoln requested.[27] Lincoln accepted the congressional regulation. However, the Supreme Court ruled that not even Congress could authorize the military detention of civilians in *Ex parte Milligan*.[28]

In *Milligan*, Chief Justice Samuel Chase concurred in the Court's opinion and strongly defended Congress' broad war regulation powers over the executive branch.[29] Chase's concurrence was widely cited as the correct assessment of congressional military authority. Chase added dictum that congressional authority extended to all matters regarding the war "except such as interferes with the command of the forces and conduct of campaigns," which remained with the President.[30]

Chase's opinion referred to the type of discretion recognized as belonging to the President from the founding of the Republic and nothing more. The Constitution's original intent for limited CINC authority was upheld through the great crisis of the Civil War.

THE RISE OF IMPERIAL PRESIDENTIAL POWER

President Woodrow Wilson led America into World War I, which served as a key point in the rise of imperial presidential authority. On the surface, this continued the traditional practice of Congress authorizing war since President Wilson sought and received a Declaration of War. However, the intent of the intervention in World War I was not to protect American interests but rather to pursue Wilson's ideological goals.[31]

President Franklin Roosevelt respected the limits of presidential CINC authority during World War II. Congress passed the Neutrality Act of 1939, forbidding the sale of military equipment to warring nations unless the nation paid in advance and transported the equipment on their vessels. President Roosevelt turned

over 50 destroyers to England in exchange for bases in the British colonies in Bermuda and the Caribbean. Roosevelt's actions complied with the statute, represented proper use of his diplomatic authority under Article II, and did not abuse his CINC authority.[32]

In June 1950, President Harry S. Truman deployed American military forces to Korea in response to North Korea's invasion of South Korea without seeking congressional approval or a declaration of war. Between 200 and 300 American military advisors were present in Korea at the time of the June 1950 invasion.[33] However, Tuman never argued that the military intervention was conducted to protect the advisors.[34]

Truman did obtain a U.N. Resolution authorizing the use of force in Korea, which gave some legal support to the intervention. However, the Charter of the United Nations is not self-executing treaty like many of America's mutual defense alliances, such as the North Atlantic Treaty Organization (NATO). Secretary of State Dean Acheson argued that Truman's CINC authority allowed him to deploy military forces to Korea.[35] Truman established the formal claim of Unitary Executive theory power under President Richard M. Nixon.

Congress supported the war by enacting conscription, authorizing the calling up of reserves, and fully funding it. However, it was the first significant conflict in which Congress had not enacted statutory authorization. Thus, Congress was, in effect, undercutting its authority by implicitly supporting the war but not granting statutory authorization and, with it, war goals and appropriate limits to military operations.[36] The lack of a clear war goal contributed to conflicts between the President and military over operations, which ended the war in a stalemate and hurt American prestige.

Truman's broad claim of CINC authority set the stage for abuses of power on the domestic front. The steelworkers went on strike during the Korean War, which could have threatened war production. Truman had authority under the Taft-Hartley Act to stop the strike but did not choose to invoke that congressionally authorized act. Instead, Truman used his CINC authority only to justify the seizure of control over the steel industry. In 1952, in the *Youngstown vs. Sawyer* case, the Supreme Court ruled against Truman's action but without a clear majority opinion as to why Truman's action was unconstitutional. [37]

Justice Robert H. Jackson's concurring opinion in the *Steel Seizure* case is the most widely cited and valuable for modern CINC issues. Justice Jackson warns that proper purpose does not justify an unconstitutional act. Justice Jackson set forth a three-part test for presidential authority acts. The first is when a president acts under congressional authorization, and then the President's authority is at its greatest. The second is when a President acts only on his authority but not in conflict with Congress. Justice Jackson warned that executive and congressional powers may overlap and that a president must respect congressional authority. Third, a president's authority is weakest when he goes against Congress's expressed or implied will.[38]

Justice Jackson warns that proper purpose does not justify an unconstitutional act. Jackson's concurrence embraces legislative authority to regulate CINC authority and goes against the unitary executive theory. He understood the threat of abuse of CINC power and the threat of excessive claims of executive authority posed to the Republic.[39] Jackson's warnings should be heeded today.

The Vietnam War sparked a conflict between President Nixon and Congress. In 1971, Congress forbade Nixon from carrying out military operations in Cambodia. Nixon bombed Cambodia in defiance of Congress, and Congress cut off funds for U.S. ground operations in Cambodia.[40] Congress also passed the 1973 War Powers Resolution to limit presidential authority to use force. Its central provision required that if a president deployed American forces to a combat zone, he must seek congressional approval before leaving them in a combat zone for more than ninety days.[41]

The claims of preclusive authority came to full fruition after the end of the Cold War. George H.W. Bush claimed preclusive powers, such as the ability not to enforce aspects of the law, which he contended impinged on his authority as CINC. Bush issued a signing statement for the National Defense Authorization Act of 1991 in which he stated that Congress had gone too far in requiring the executive branch to give notice to Congress of changes in specific special access programs.[42]

President William Clinton continued the strong preclusive power claims as Bush. In 1999, Clinton deployed troops in Kosovo far longer than the War Powers Act limits without obtaining congressional approval. Congress did nothing in response. No direct challenge to the statute's constitutionality was made, but it failed to restrain the President's use of military power without congressional approval. Further, a pattern was developing in which Congress failed to defend its

authority. Thus, the boundaries of CINC's authority to use military force were pushed further, helping set the stage for future sweeping claims of President George W. Bush.[43]

The George H.W. Bush administration claimed preclusive authority to act free of congressional regulation, including previously enacted statutes that conflicted with what he wanted to do as CINC. Congress authorized military operations against those responsible for the September 11, 2001, attacks in the 2001 Authorization for Use of Military Force (AUMF). In a signing statement on the AUMF, Bush stated that he did not need authorization from Congress for his military responses to the attacks. President Bush objected to the statutory restrictions in dozens of signing statements and asserted the authority to not comply with laws when they conflicted with his preclusive CINC.[44]

President Bush requested authorization from Congress, which would have given him the legal authority to overthrow the government of Iraq and occupy the nation. Congress only gave Bush limited authorization to take necessary military action to get rid of the weapons of mass destruction. Bush also sought authorization from the United Nations Security Council to use force. However, the United Nations (U.N.) Resolution 1441 only gave authority to halt Iraq's weapons of mass destruction program and "restore the peace." No authority was provided for overthrowing a sovereign government or occupying Iraq.[45]

The Bush administration also made an additional argument, citing the 1990-1991 era resolution against Iraq to justify the invasion of Iraq. U.N. Resolution 678 authorized the use of force back in 1990 to expel Iraqi forces from Kuwait. However, its objectives had been achieved, and the resolution was no longer in effect. U.N. Resolution 687 was the authority that was in place, and it imposed sanctions on Iraq after the war for its failure to comply with United Nations Resolution 686, which required Iraq to its weapons of mass destruction program, cooperate with United Nations Weapons inspectors, and that the Iraqi stop its human rights abuses of its citizens. However, it did not provide for the use of force, an invasion of Iraq, the overthrow of its government, or the occupation of Iraq.[46] Arguably then, the United States lacked authority from the U.N. Security Council for the invasion.

The Bush administration claimed that international law did not apply to his CINC authority. Therefore, the President could interpret the United Nations resolution as authorizing the overthrow of the Iraq regime and the occupation of Iraq. The Founding Fathers stated many times that the President was, like the nation, bound to uphold customary law, which the nation had recognized and had to abide by treaties. Fifteen Supreme Court cases have held that Presidents must comply with the recognized customary international law.[47]

The Bush administration argued that preclusive executive CINC authority allowed the administration to broadly interpret the congressional authorization to permit the overthrow of the Iraq regime and the occupation of Iraq. Such a broad interpretation goes against the plain text of the authorization and the Constitution's original intent.[48] The Bush administration's claims were not supported by history or legal precedent. Presidents have limited executive power to act in times of necessity when it would be infeasible to obtain legislative permission because Congress is unavailable. However, the President must respect congressional will and not use their power to start conflicts against the will of Congress.[49]

Candidate Barack Obama ran for President on a platform of opposition to the 2003 invasion of Iraq and the Bush administration's claims of imperial presidential authority. Almost from the start of his administration, Obama further expanded Bush's claims of authority. Obama claimed broad authority in signing statements, interpreting status, pushing new regulations, and using military force.[50]

In March 2011, the Obama administration claimed the authority to use military force without congressional authorization, a self-defense claim, or under treaty obligation. Obama claimed the authority to use force in Libya based solely on a presidential determination that United States interests were at stake and that he believed military force was required. No president had ever made such a claim, and even Truman and Bush pointed to the legal authority of United Nations resolutions.[51]

The United Nations Security Council passed Resolution 1973 authorizing NATO to enforce a no-fly zone in parts of Libya and other "necessary actions to protect refugees." The resolution did not authorize military intervention to impact the struggle on the battlefield or the overthrow of Libya's sovereign government. The Obama administration further used this resolution to support its intervention, claiming it acted solely to protect refugees.[52]

The Charter of the United Nations does not authorize military intervention to overthrow a sovereign government. President Obama made the false claim that Resolution 1973 authorized his actions. He also claimed that his CINC authority allowed him to intervene based on his determination to use military force in the nation's best interests. Obama built on the legacy of Bush and demonstrated that he lacked any regard for the limits of his authority and was willing to violate both international law and the Constitution in his exercise of Command in Chief authority.[53]

In 2016, as a presidential candidate, Donald Trump was critical of America's extensive involvement in foreign conflicts. However, President Trump pushed the claims of CINC authority to use military force further than any prior President. He launched military strikes in Syria without any new congressional authority and did not claim any act of Congress authorized it. The Trump administration only cited his CINC authority and did not attempt to justify it under international law. A few officials later defended the strike as a humanitarian mission, which harkens to Obama's arguments, but that was never an official legal argument.[54]

In 2020, the Trump administration carried out the targeted military killing of Iranian Revolutionary Guard General Soleiman. The Trump administration justified it as an extension of the 2002 Authorization to Use Force (AUMF) in Iraq. The other basis was the CINC's authority to use force to defend military personnel. The latter argument may represent a valid basis but sets a dangerous precedent.[55]

The AUMF was limited to doing what was necessary to stop Iraq's weapons of mass destruction and in no way related to the present-day situation. Presidents should respect restraints on their authority and should not seek to warp authorizations to apply unrelated situations.

The redeployment of forces in Iraq after the 2011 withdrawal was not done with a new authorization. Thus, a president could position forces in conflict areas and then start a war to protect them, making constitutional limits on CINC meaningless.[56]

In 2019, Congress invoked the 1973 War Powers Act and passed a resolution requiring American military forces to withdraw from Yemen and end active American involvement in combat. Trump vetoed the resolution and continued military operations. The clash showed that the War Powers Act was impotent. The Trump administration's actions further eroded congressional oversight over the use of military force.[57]

President Joe Biden adopted Obama's view of CINC's authority to use military force. However, he did not entirely reject congressional oversight as did President Trump and did not hold Congress in open disdain like Trump.[58] Trump is about to retake office, and his views of the Presidency have grown stronger. He has won his fight for presidential immunity for official acts and is sending signals that he may challenge congressional dominance over fiscal matters.[59]

IMPERIAL PRESIDENTIAL POWER THREATENS THE REPUBLIC

The Founding Fathers understood the long-standing practice of English monarchs fighting undeclared wars based only on the King's authority. They realized that the root of so many needless conflicts was the abuse of authority by the Monarchs of England. They wanted to prevent America from having the same history. Wars were meant to be fought only with Declarations, and the power to Declare war was restricted to Congress. Thus, through Congress, the American people would decide if a war was necessary and just.[60]

The modern presidential claims for imperial power are rooted in Wilson's ideas. Thus, the roots of the unitary CINC authority to use military force are absent from the Constitution and are founded in the 19th-century German school of philosophy. George Hegel taught that the state is a metaphysical reality that is not restrained by the rule of law or outside limitations like natural law. Thus, a President can wage war just because his will is war[61]

The Unitary Executive Theory has expanded to the point that modern Presidents claim the authority to wage war at will, similar to European old monarchs. Trump even rejects congressional overreach and may challenge congressional fiscal authority. Even more importantly, it has damaged the foundations of the American Republic. The American Republic may be on the brink of the existential crisis that the Unitary Executive Theory claims created.

CONCLUSION

The Founding Fathers established Commander-in-Chief and executive authority based on the model of George Washington. The original intent of the President's CINC authority gives the President operational authority over the nation's military and foreign policy. However, the power is subject to congressional authority and direction, and Congress's decision to take the nation war is reserved. CINC and

executive power were not intended to allow the President to initiate the use of force other than immediate national defense.

Woodrow Wilson introduced ideological foundations into American political thought and practice, which would later surface and displace the original intent. The Unitary Theory took hold after the end of the Cold War. George H.W. Bush made sweeping claims of executive authority during the Gulf War and his broad claims of presidential authority. Congress began to concede authority. George W. Bush openly asserted the Unitary Executive Theory during the War on Terrorism.

President Obama pushed the boundaries to the point of claiming that based on a presidential assertion of national interest, the President could use force and even overthrow a sovereign government without congressional approval. Trump now asserts that the complete CINC should use military force at will and take necessary steps to facilitate the use of force, including reprogramming money, and rejects congressional oversight.

Broad claims of presidential authority are dangerous to the Republic and the interests of a sound American foreign policy. The Imperial Presidential power view is unconstitutional, results in bad policy, and leads to a general pattern of presidential abuse of power both in international affairs and domestically. Returning to the original limited presidential power to take the nation to war is vital for sound public policy, the Republic's health, and the nation's future.

NOTES

[1] Thomas Jefferson, "Draft of the Declaration of Independence," (Washington, DC, National Archives), https://www.archives.gov/founding-docs/declaration-transcript.
[2] David J. Barron and Martin S. Lederman, "The Commander in Chief at the Lowest Ebb – Framing the Problem, Doctrine, and Original Understanding," *Harvard Law Review* Vol. 121 (January 2008), 770-773.
[3] Ibid.
[4] Michael A. Genovese, *Presidential Prerogative Imperial Power in an Age of Terrorism* (Stanford, CA: Stanford University Press, 2011), 93-99.
[5] Jeffrey Crouch, Mark J. Rozell, and Mitchel A. Sollenberger, *The Unitary Executive Theory A Danger to Constitutional Government* (Lawerence, KS: University Press of Kansas 2020), 2-3 and 107-108.
[6] U.S. Const. art. I, § 8.
[7] U.S. Const. art. II, § 2 and 3.
[8] Julian P. Boyd, *The Papers of Thomas Jefferson.* (Princeton, NJ: Princeton University Press 1958), 595-598.
[9] 2 Journals of the Continental Congress, 1774–1789, 1796. https;//memory.loc.gov/ammenm/amlaw/lwjclink.html.
[10] B. Logan Beirne, "Battle Royale: George v. George v. George: Commander-in-Chief Power," *Yale L. & Policy Review* Vol. 26, (Fall 2007), 285-289.
[11] Thomas Jefferson, "Draft of the Declaration of Independence," (Washington, DC: National Archives), https://www.archives.gov/founding-docs/declaration-transcript.
[12] Barron and Lederman, "The Commander in Chief," 770-773.
[13] John Yoo, *War by Other Means; An Insider's Account of the War on the Terror* 120 (New York: Atlantic Monthly Press 2006), 120-122.
[14] Christopher R. Berry & Jacob E. Gersen, *The Unbundled Executive*, University of Chicago Law School Public Law and Legal Theory Paper Series, Paper No. 214, (2008), http://ssrn.com/abstract=1113543.
[15] Alexander Hamilton, *The Federalist* 74 (1788).
[16] Ibid.
[17] *Loving v. United States*, 517 U.S. 748, 772 (1996).
[18] U.S. Const. art. I, § 8.
[19] James McClellan, *Liberty, Order, and Justice: An Introduction to the Constitutional Principles of American Government,* 3rd ed. (Indianapolis: Liberty Fund, 2000), 387-392, 400-405.
[20] Burrus M. Carnahan, "Lincoln, Lieber, and the Laws of War: The Origins and Limits of the Principle of Military Necessity," *American Journal of International Law*, Vol 92 (April 1998), 218-222.
[21] Ibid.
[22] Jochem H. Tans, "The Hapless Anaconda: The Union Blockage 1861-65," *The Concord Review* (1994), 14-16.
[23] Ibid.
[24] James D. Richardson, *Compilation of the Messages and Papers of the President Vol* 7 (Washington, DC: United States Congress 1897), 3227-3232.
[25] *Ex parte Merryman*, 17 F. Case 144 (1861).
[26] Richardson, *Compilation of the Messages,* 3227-3229.
[27] *Ex parte Milligan,* 71 U.S. 136-42 (1866).
[28] Ibid., 126-32.
[29] Ibid., 133-41.
[30] Ibid., 139.
[31] Jonah Goldberg*, Liberal Fascism* (New York: Doubleday Broadway Publishing Group, 2007), 290-297.
[32] Martin Gibert, *Churchill, and America* (New York: Free Press Publishing 2005), 200-206.
[33] Jack James, "North Koreans Invade South Koreans," *UPI Archives*, June 25, 1950. https://www.upi.com/Archives/1950/06/25/North-Koreans-invade-South-Korea/1012416555294/
[34] Dean Acheson, *Present at the Creation* (New York: W.W. Norton & Company 1969), 412-418.
[35] Ibid.
[36] Geoffrey Corn, Jimmy Gurule, Eric Talbot Jensen, and Peter Margulies, *National Security Law Principles and Policy,* 2nd ed. (New York: Wolter Kluwer 2019), 65-67.
[37] *Youngstown vs. Sawyer*, 343 U.S. 579, 580-589 (1952).
[38] Ibid., 637-652.
[39] Ibid., 634-636.
[40] Francis D. Wormuth, "The Nixon Theory of the War Power: A Critique," *Cal. Law Review* vol. 60, (1972), 633-640.
[41] War Powers Resolution of 1973 (50 U.S.C. 1541-48).
[42] Michael A. Genovese, *Presidential Prerogative Imperial Power in an Age of Terrorism* (Palo Alto, CA: Stanford University Press, 2011), 98-103.
[43] Jack Goldsmith*, The Terror Presidency: Law and Judgment Inside the Bush Administration* (New York: W.W. Norton & Company, 2007), 36-39.
[44] Ibid.
[45] Michael N. Schmitt, "The Legality of Operation Iraqi Freedom under International Law," *Journal of Military Ethics*, vol. 3 (2004), 83-88.
[46] Murphy, *Assessing the Legality*, 187-193.
[47] Jordan J. Paust, *Beyond the Law: The Bush Administration's*

Unlawful Responses in the "War" on Terror, (Cambridge, UK: Cambridge University Press, 2007), 18-27.
[48] U.S. Const. art. II, § 1, cls. 1 and § 2, cls. 1–2.
[49] James P. Pfiffner, *Power Play the Bush Presidency and the Constitution* (Washington, DC: Brookings Institute Press, 2008), 30-35 and 57-65.
[50] Genovese, *Presidential Prerogative,* 98-105.
[51] Mariah Zeisberg, *War Power: The Politics of Constitutional Authority* (Princeton, NJ: Princeton University Press, 2013), 250-255.
[52] Pierre Thielborger, "The Status and Future of International Law after the Libyan Intervention," *Goettingen Journal of International Law*, vol 4 (2012), 22-28.
[53] Ibid.
[54] Michael N. Schmitt and Christopher M. Ford, "Assessing U.S. Justifications for Using Force in Response to Syria's Chemical Attacks: An International Law Perspective," *Journal of National Security Law & Policy* vol 9 2017), 285-287, 303.
[55] Stephen Jackson, "An Imperfect War: The Legality of the 'Soleimani Strike' and Why the Biden Administration Should Adopt Its Precedent for Future Operations in Iraq and Afghanistan," *Penn State Journal of Law and International Affairs* Vol 11 (Jan 2023), 44-45.
[56] Crouch, Rozell, and Sollenberger, *The Unitary Executive*, 112-115.
[57] Mark Lander and Peter Baker, "Trump Vetoes Yemen Resolution," *New York Times* (April 16, 2019), https://www.nytimes.com/2019/04/16/us/politics/trump-veto-yemen.html.
[58] Michael N. Schmitt, "President Biden's First Use of Force and International Law," *Articles of War* (March 2021), https://lieber.westpoint.edu/president-bidens-first-use-of-force-and-international-law/.
[59] Elizabeth Goiten, "How Trump Could Deploy Military for Mass Deportations," *Brennan Center for Justice* (December 2004), https://www.brennancenter.org/our-work/research-reports/how-trump-could-deploy-military-mass-deportation.
[60] Michael P. Scharf & Paul R. Williams, *The Law of International Organizations: Problems and Materials*, 3d ed. (Durham, NC: Carolina Academic Press, 2013), 541-547; Sean D. Murphy, "Assessing the Legality of Invading Iraq," 92 *Georgetown Law Journal*, (vol 92, 2004), 174-177; Olivia Ambler & Shirley V. Scott, "Does Legality Matter? Accounting for the decline in U.S. Foreign Policy Legitimacy Following the 2003 Invasion of Iraq," *European Journal of International Relations*, vol. 13 (2007), 71-76.
[61] Rozell Crouch and Sollenberger, *The Unitary Executive* Theory, 6, 125-129, and 162; Magee, Malcolm D. *What the World Should Be* (Waco, TX: Baylor University Press, 2008), 6; Woodrow Wilson, *Constitutional Government in the United States* (New York: Columbia University Press, 1908), 43-44; see George F. W. Hegel, *The Philosophy of History*, translated by J. Sibree (New York: Willey Book Co., 1837).

Lieutenant Colonel Johnny B. Davis (U.S. Army Reserve) is an International and Constitutional Law Attorney, Attorney Advisor with the Army SJA Office - Fort Meade, a Liberty University professor with the Helms School of Government, and an Army Reserve Judge Advocate General Corps officer.

NMIF Board of Directors: LTG (USA, Ret) Mary A. Legere, Chair and LTC (USA, Ret) Steve Iwicki, President

Human Intelligence in Ancient Times: Nothing New under the Sun

by **Alfredo Ribeiro Pereira and Cesar Augusto Silva da Silva**

INTRODUCTION

Espionage is as old as human beings and has been used in politics, diplomacy, and war.[1] Its main objective is to obtain data not available through other means, and thus assist the state's decision-making process, allowing for better decision-making and the consequent survival and prevalence of the state. Said in a poetic way, "Spies are the ears and eyes of Princes."[2] Since humans invented writing, there are records of espionage, whether in myths, in the Bible or in books of doctrine. But in ancient times there were no technological means for obtaining data, only human sources, so ancient espionage was largely human intelligence—HUMINT.[3]

This article seeks to identify the HUMINT techniques used in ancient times, which are still used today.[4] The study presents an inductive approach, which starts from data to infer a general truth. And the procedure used is the bibliographic monograph. Monographic, as it "consists of the study of certain individuals [...] with the purpose of obtaining generalizations,"[5] and bibliographical, as it is "carried out based on already published material."[6] This article addresses prehistory and examines passages from mythology, the Bible, and the works of Sun Tzu, Kautilya, and al-Mulk, that refer to espionage, identifying the HUMINT techniques still used today.

PREHISTORY

The need to obtain information to ensure survival has been a constant in humanity since prehistoric times, having emerged in the first human groups, even before the emergence of the state. According to Mithen, "the gathering of information from the natural environment is an activity in which all modern hunter gatherers engage," as well as prehistoric hunters looked for tracks, observed animals, and used them as clues to the whereabouts of other species.[7]

In addition to information about the natural environment, survival also depended on gathering information about other human groups. It is credible to suppose that the same actions applied to animals (tracking and veiled observation)[8] were also applied to other human groups, and the interrogation[9] of captives and recruitment[10] were also applied.

MYTHS

Since ancient times, there have been records about the use of espionage in obtaining data to support foreign policy goals and military operations.[11] The first reference to espionage in human history might be the Mesopotamian poem "Enki and Inanna." Enki is the "god of technical skills, organized planning, abundance, and knowledge," and his cult "spread during the third millennium BC over southern Mesopotamia." Inanna is the Sumerian goddess of love and war.[12] The poem narrates the theft of the "ME" (divine force) by Inanna, after Enki gets drunk.[13] Inanna went to the city of Abzu and invited Enki to a beer-drinking contest, in which he got drunk.[14] "Inanna steals all the ME that she needs to establish her cult in Uruk from the temple in Eridu. Enki sends several demons after her but he finally has to accept the transfer of the divine powers from Eridu to Uruk."[15] Clearly, there are elements of an espionage operation in which Inanna uses her sex appeal to approach Enki, get him drunk, and thus obtain the secrets he kept. So, these secrets are used politically.[16]

Another myth that refers to the theft of secrets is the Greek myth of Prometheus. In fact, there is an interesting parallel between Enki and Prometheus; both are the creators of humanity, both oppose the reigning deity to protect and instruct humanity, and both use trickery to do so. Prometheus tricks Zeus into helping humanity, as found in the fifth-century BC Greek tragedy.[17] "Prometheus steals a flame from the gods and gives it to the humans himself. Zeus, in turn, ties the Titan to a rock, drives a wedge through his chest, and sets an eagle to the daily task of "gnawing his undying liver."[18]

One could say that this myth is about industrial espionage because the flame can be understood as the technology of the production and use of fire, which was very important for mankind's development. The use of fire helped "man to not only cook his food and make agricultural implements but also to create weapons of war with hard metals

like bronze, copper, and iron." Hence, by giving fire, Prometheus also gives civilization to mortals.[19] The myth also indicates the sad fate of the spies who are discovered and captured. Imprisonment, torture, and death are the end. However, Prometheus' fate is even worse, as he does not have the relief of death.

THE BIBLE

There are also several references to spying in the Old Testament's five books of Moses.[20] In Genesis, Joseph, who was then the governor of Egypt, falsely accused his brothers, who had gone there to buy food, of being spies and arrested them.[21] The very choice of the espionage charge indicates that spying was a current practice and concern at that time. In Numbers, the Lord commands Moses to send spies, one from each tribe, to spy out Canaan: "And Moses sent them to spy out the land of Canaan," Moses asked them to see the land, the people, the cities and the agriculture.[22] In modern terms, it is the sending of an operational team to carry out a reconnaissance[23] operation in Canaan, seeking geographic, military, political, and socio-economic information. These reconnaissance operations were also conducted at Jaazer and other places.[24]

Unfortunately for some, Israel's reconnaissance operations did not end well: "And when king Arad the Canaanite, which dwelt in the south, heard tell that Israel came by the way of the spies; then he fought against Israel, and took some of them prisoners."[25]

In the book of Joshua, another espionage operation is reported, and elements of counterintelligence,[26] recruitment, and exfiltration[27] are clearly identified in the report: "And Joshua the son of Nun sent out of Shittim two men to spy secretly, saying, go view the land, even Jericho. And they went, and came into a harlot's house, named Rahab, and lodged there."[28]

The presence of foreigners gathering information draws attention, and the government is warned and promptly seeks to neutralize the threat: "And the king of Jericho sent unto Rahab, saying, bring forth the men that are come to thee, which are entered into thine house: for they be come to search out all the country."[29] The governor's prompt response, of trying to capture the spies, shows once again that the practice and concern with espionage have been commonplace since ancient times. Rahab deceives the persecutors, hides the spies, and helps them escape. But first, she proposed a deal, for having saved their lives, that they would spare her and her family and belongings. "And that ye will save alive my father, and my mother, and my brethren, and my sisters, and all that they have, and deliver our lives from death."[30] This is an exfiltration agreement. When the final attack on Jericho takes place, the Israelites fulfil the agreement, and Joshua sends those spies to safely extract Rahab, her family, and possessions, "because she hid the messengers, which Joshua sent to spy out Jericho."[31]

Recruitment through coercion[32] is also found in the Bible, for example in the book Judges, when reporting the attack on Bethel. Joseph sent his men, "the spies saw a man come forth out of the city," they forced him to show the entrance into the city, in exchange for being spared." And when he shewed them the entrance into the city, they smote the city with the edge of the sword; but they let go the man and all his family."[33]
In the second book of Samuel, in which a conspiracy to seize power is described, there is a reference to the use of spies to influence[34] the population: "But Absalom sent spies throughout all the tribes of Israel, saying, as soon as ye hear the sound of the trumpet, then ye shall say, Absalom reigneth in Hebron."[35] In the first book of Chronicles, a suspected espionage causes an incident that leads to war.[36] In Judges, and in the first book of Samuel, there are also other references to men sent to spy.[37]

The New Testament also makes direct reference to espionage. Jesus Christ himself was the target of spying actions with a political purpose, according to the Gospel of Luke: "And they watched[38] him, and sent forth spies, which should feign themselves just men, that they might take hold of his words, that so they might deliver him unto the power and authority of the governor."[39] The passage in which the Pharisees ask Jesus, "Is it lawful to give tribute unto Caesar, or not?"[40] resembles a Sting Operation, because they created an opportunity for Jesus to commit the crime of preaching against paying taxes to the Romans, hoping that he would incriminate himself by answering the question.[41]

Judas' betrayal that led to Jesus' arrest can also be analysed from the perspective of tradecraft.[42] In Matthew, Chapter 26, there is a "walk-in"[43] action:

> Then one of the twelve, called Judas Iscariot, went unto the chief priests. And said unto them, what will ye give me, and I will deliver him unto you? And they covenanted with him for thirty pieces of silver. And from that time, he sought opportunity to betray him.[44]

The passage that narrates the arrest of Jesus shows an operational action of spotting the target: "Now he that betrayed him gave them a sign, saying, whomsoever I

shall kiss, that same is he: hold him fast. And forthwith he came to Jesus, and said, Hail, master; and kissed him. […] Then came they, and laid hands-on Jesus, and took him."[45]

DOCTRINAL WORKS

Since the emergence of the first works on state administration, war, and international relations, several scholars have referred, directly or indirectly, to espionage.

Sun Tzu

Around 512 BC, Sun Tzu, "a famous general, philosopher and military strategist in ancient China," wrote the book *The Art of War*, which focused on military strategy.[46] *The Art of War* is a classic work on military strategic principles and applications."[47] "So important was this text that over the millennia it's been translated into many languages, updated and adapted to describe everything from the internal workings of sales processes to investment strategies to modern politics."[48]

The book has thirteen chapters, and the last one is dedicated exclusively to espionage: The Use of Spies.[49] Note that the author is an espionage enthusiast and advocates its use in both war and peace (just as it is today): "27. […] Spies are the most important element in war [….]" "18. Be subtle! Be subtle! And use your spies for every kind of business."[50] The chapter begins by warning about the economic and social costs of war and that going into battle without information about the enemy to save money is "inhumanity":

> 2. […] Hostile armies may face each other for years, […]. This being so, to remain in ignorance of the enemy's condition simply because one grudges the outlay of a hundred ounces of silver in honours and emoluments, is the height of inhumanity.[51]

Just like back then, even today, espionage plays an important role in ensuring the best decision-making and saving resources and lives. For Sun Tzu, prior knowledge is what allows the achievement of victory: "4. Thus, what enables the wise sovereign and the good general to strike and conquer, and achieve things beyond the reach of ordinary men, is foreknowledge."[52] And he points out that "6. Knowledge of the enemy's dispositions can only be obtained from other men." There were obviously no technical means at that time.[53]

According to the author, there are five classes of spies. And a secret system that uses them is the sovereign's most important faculty.[54] The first class of spies mentioned by Sun Tzu is the class of local spies, which is nothing more than the use of the inhabitants of the place. Nowadays, it is said "local civilian debriefing operations," which are "the process of questioning cooperating local civilians to satisfy intelligence requirements."[55] Locals inhabitants play an important role in war and "civil-military cooperation must be strengthened."[56] The support of the population is essential to guarantee an information flow.[57] They can provide data about the environment, the population itself, the government, and enemies. Even today, it is important to access "the population and establishes a rapport with key persons in the area, and develops sources to work with on a regular basis."[58]

The second class mentioned is the use of inward spies, who are the officers of the enemy army.[59] Recruiting them can provide valuable information, and the higher the rank, the higher the value of the information, and of course, the higher the cost.

Double agents are also cited as a class; Sun Tzu nominated them as converted spies and highly valued their importance.[60]

> Double agents hold a unique and crucial position in the realm of intelligence and counterintelligence. By providing access to the inner workings, plans, and secrets of an enemy or target organization, double agents can significantly influence the outcome of military, political, and economic conflicts.[61]

Another class of spies presented in the book are doomed spies[62] to do "certain things openly for purposes of deception,[63] and allowing our own spies to know of them and report them to the enemy."[64] Deception operations have always had a crucial importance in intelligence, especially at war, as Sun Tzu himself said, "all warfare is based on deception."[65]

The last class pointed out is that of surviving spies, which are nothing more than "those who bring back news from the enemy's camp."[66] Those who have left their countries or organizations can provide information about them.[67] Having reached a safe location, they can provide more compromising information than they would have provided at home. The author emphasizes the importance of treating and remunerating recruits well:

> 14. Hence, it is that with none in the whole army, there are more intimate relations to be maintained than with spies. None should be more liberally rewarded (…), […] 16. They cannot be properly managed

> without benevolence and straightforwardness, […] 21. The enemy's spies who have come to spy on us must be sought out, tempted with bribes, led away and comfortably housed. Thus, they will become converted spies and available for our service. […] 25. The end and aim of spying in all its five varieties is knowledge of the enemy; and this knowledge can only be derived, in the first instance, from the converted spy. Hence, it is essential that the converted spy be treated with the utmost liberality ….[68]

Espionage cases in the United States, over a 30-year period, show amounts paid to spies in the tens of thousands of dollars, reaching 2.5 million in the Aldrich Ames case.[69] Of course, there are also cases of spies who worked for free for ideological reasons, but since ancient times, money has been one of the main motivations for spying. It is no coincidence that the acronym MICE (i.e., money, ideology, compromise, and ego),[70] which describes the typical motivations for spying.

Sun Szu also stresses the importance of secrecy: "14. (…) In no other business should greater secrecy be preserved." [71] And "19. If a secret piece of news is divulged by a spy before the time is ripe, he must be put to death together with the man to whom the secret was told."[72] The importance of safely preserving state secrets remains fundamental to state security.

Since its publication, "until present days, Sun Tzu and *The Art of War* have been recognized as one of the most important Chinese cultural inheritances." This text has been influential in "military activity, business management, social administration, operating decisions" and so on.[73] Sun Tzu was very objective in his work, approaching the importance of espionage and its possibility of use in all state businesses, the advantages of its use, the different types of agents and their employment, their recruitment, the analysis of the data obtained, the need for secrecy and the importance of targeting the highest decision-making levels. Espionage techniques like debriefing, recruiting, double agent operations, deception, bribery, and secrecy can be identified in his book.

Chanakya Kautilya

Chanakya Kautilya (370 – 283 BC) was a political and military adviser to the first Mauryan Emperor,[74] "Chandragupta Maurya (317–293 BC), who defeated the Nanda kings (several related kings trying unsuccessfully to rule India together), stopped the advance of Alexander the Great's successors, and first united most of the Indian subcontinent in the empire."[75] His book The *Arthashastra* ("The Science of Politics") is a political and military discourse written in prose, containing three Chapters that also deal with espionage and the importance of spies.[76] The main theme is the national security of a state, and internal and external factors of national security start from the very beginning to the end of the book.[77]

The book makes repeated reference to the use of spies. The *Arthashastra* describes the use of spies in internal and external actions, and in political, military, and police actions. His intention to spy on all places and all social classes is evident, as Kautilya suggests that various classes of spies should be formed to seek information surreptitiously, from mendicants to farmers and merchants, from prostitutes to religious, and so on. "All these spies shall be very quick in the dispatch of their work."[78] "The Collector-general shall employ spies disguised[79] as [practitioners of various occupations/ professions] and send them abroad into the country for espionage.[80]

The author even proposes an espionage service financed by the sovereign, which is economically self-sustaining while serving as a cover story: "This spy, provided with much money and many disciples, shall carry on agriculture, cattle-rearing, and trade on the lands allotted to him for the purpose. Out of the produce and profits thus acquired, he shall [pay the agents sent to spy]."[81] It is interesting to note that the practice of setting up "companies" as cover for espionage operations is ancient. To prevent betrayal, the author proposes a series of sting operations to tempt ministers with power, money, sex, and even a sense of justice.[82]

The author warns that the spy agency must conduct these operations, and the king must never make himself the object of the character test of his advisors.[83] The creation of the internal service of espionage and the selection of personnel are mentioned. The writer emphasizes that to act in this activity, loyal agents with the intellectual capacity to interpret the targets must be sought. He also underlines the need for moral and financial recognition of the agent:

> Assisted by the council of his ministers tried under espionage, the king shall proceed to create spies (…) A skillful person capable of guessing the mind of others is a fraudulent disciple. Having encouraged such a spy with honor and money rewards, the minister shall tell him, "Sworn to the king and myself, thou shalt inform us of whatever wickedness thou fondest in others."[84]

"Honoured by the king with awards of money and titles, these five institutes of espionage (*samstháh*) shall ascertain the purity of character of the king's servants."[85]

Like Sun Tzu, Kautilya prescribes the need to check information received from spies. He suggests checking them by using different sources: "[…] When the information thus received from these three different sources is exactly of the same version, it shall be held reliable. If they (the three sources) frequently differ, the spies concerned shall either be punished in secret or dismissed."[86] This needs to validate information and sources remains in the modern world. "The job of the analyst is, in part, to evaluate raw material and put it in perspective. The analyst receives intelligence material from a variety of sources, […] raw reports from human sources […] are sometimes fragmentary, biased, contradictory, or just plain wrong."[87] Compartmentation[88] is also pointed out in the same Chapter: "Neither the institutes of espionage nor they (the wandering spies) shall know each other."[89]

Kautilya indicates the use of espionage in counterintelligence to identify and neutralize adversary actions, both foreign and domestic: "Spies set up by foreign kings shall also be found out by local spies; spies by spies of a like profession. It is the institutes of espionage, secret or avowed, that set spies in motion."[90] "Those that are angry, those that are greedy, those that are alarmed, as well as those that despise the king are the instruments of enemies. Spies under the guise […] shall ascertain the relationship of such persons with each other and with foreign kings."[91] "The king shall employ his own envoys to carry on works of the above description, and guard himself against (the mischief of) foreign envoys by employing counter envoys, spies, and visible and invisible watchmen."[92]

> Any one of the classmate spies, say (politicians known as) *Ambhíyas*, may allure the prince towards hunting, gambling, liquor, and women, and instigate him to attack his own father and snatch the reins of government in his own hands. Another spy shall prevent him from such acts.[93]

The promotion of foreign interference[94] is advocated by Kautilya:

> The other spies may spread the news that the officer in charge of the wastelands destroys the people and plunders them. Similarly, spies may cause disagreement between the enemy's collector-general and the people […] Spreading the false news […]"[95] "[…] the conqueror's spies should sow the seeds of dissension among them […]"[96] "His spies should often bring home to the mind of the leaders of provinces, villages, castes, and corporations […]"[97]

The *Arthashastra* shows that Kautilya has in-depth knowledge of human psychology. The tactics used by him for clandestine operations, especially those that include spies, use concepts similar to the modern-day psychoanalytical concepts of id, ego, superego, and libido.[98] In conclusion, Kautilya effusively advocates the use of espionage, both at home and abroad, in both war and peace. The operational techniques currently used, such as cover story, infiltration, sting operation, honeypot, foreign interference, recruitment, compartmentalization, and so on, are prescribed by the author for the acquisition and maintenance of political and military power.

Nizam Al-Mulk

Nizam al-Mulk (1018 - 1092) was a military strategist and government administrator. His most popular work, *Siyasat-nama* ("The Book of Government"),[99] discusses the government approaching political, financial, military, bureaucratic, managerial, religious, sociological, and justice aspects.[100] "His book sums up two thousand years of Iranian experience in statecraft."[101] Al-Mulk devoted a Chapter to the use of spies (Chapter XIII - On sending spies and using them for the good of the country and the people),[102] both for use in the kingdom and abroad. He stressed its importance for political and military security. As Kautilya preached, Al-Mulk also preaches the use of disguised spies in various social classes, from beggars to merchants, including religious. The role of espionage in preparation for political and/or military action is explicit in his work.

> Spies must constantly go out to the limits of the kingdom in the guise of merchants, travelers, Sufis, pedlars, and mendicants, and bring back reports of everything they hear so that no matters of any kind remain concealed, and if anything (untoward) happens it can in due course be remedied.[103]

Like Kautilya, the author also stresses the need for the espionage work to be carried out by loyal people and the need for continuous training of agents: "This Chapter has dealt with spies; and this work must be in the hands of trustworthy people. Get such men continually be prepared and sent to various parts for various tasks."[104] Nothing different from today's reality. Intelligence activities must be conducted by reliable personnel who are continually trained and updated.

Greek and Roman Authors

Ancient Greek and Roman authors also report the use of spies to assist in the decision-making process. The works of Thucydides,[105] Plutarch,[106] Julius Caesar,[107] and in the *Historia Augusta* collection,[108] present passages with reference to methods such surveillance, recruitment, infiltration, and cover story.

CONCLUSION

Rulers have, since the dawn of humanity, used espionage, aiming to support decision-making in political and military actions. Human survival has depended on obtaining information about other human groups. Surveillance, interrogation, and recruitment were used from the earliest times.

From the moment humans began to make written records, acts of espionage began to be recorded. Mesopotamian and Greek mythology present passages in which secrets, associated with power and/or technology, are taken from their holder by their peers using deception and trickery. The first reference to espionage in written records is probably the Mesopotamian poem "Enki and Inanna," in which Inanna uses her sex appeal to approach Enki, get him drunk, and steal his secrets. The Bible presents multiple passages in which espionage acts are narrated, both in the Old and New Testaments. Even Jesus Christ was a target of spying, and God commanded Moses to send spies. Reconnaissance, recruitment through coercion, exfiltration, influence, sting operation, "walk in" and spotting target can be identified in the holy book.

From the moment the earliest books were written on state administration, war, or international relations, the use of espionage and its importance for the decision-making of rulers have been pointed out, and HUMINT techniques have been considered. Sun Tzu, in *The Art of War*, reveals himself to be an enthusiast of espionage, recommending its use for all purposes and even affirms that spies are the most important elements in war, having devoted an entire chapter to the subject. Techniques like debriefing, recruiting, double agent operations, deception, bribery, and secrecy can be identified in his book.

The writers extend across varying cultures and times—typically make similar points. In the book *Arthashastra*, Kautilya preaches the use of espionage, both internally and externally, in the defense of the state and government, mentioning in detail various operational techniques, like cover story, recruitment, infiltration, sting operation, honeypot, foreign interference, compartmentalization, disguise, and bribery. Nizam al-Mulk in his book *Siyasat-nama* (The Book of Government), wrote an entire chapter on the use of spies, both abroad and at home, and highlighted their importance for political and military security. The use of a cover story, recruitment, infiltration, and disguise are prescribed in his work. Ancient Greek and Roman authors also refer to surveillance, recruitment, infiltration, interrogation, and the use of a cover story.

Many HUMINT techniques used today can be identified in antiquity and have changed little. After all, the human being, whether executor or target of espionage, remains the same since its emergence. It is not without reason that espionage is known as the "second oldest profession."[109] After all, as the Bible says: "The thing that hath been, it is that which shall be; and that which is done is that which shall be done: and there is no new thing under the sun."[110]

NOTES

[1] "Intelligence activity directed towards the acquisition of information through clandestine means." Mark L. Reagan, *Counterintelligence Glossary -- Terms & Definitions of Interest for CI Professionals (Washington, DC: Department of Defense, 2014), s.v. "Espionage," 130. In other words, the obtaining or attempting to obtain information under false pretenses or clandestinely. "Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land – Hague IV" (The Hague, 18 October 1907), article 29.*

[2] George Herbert, *Herbert's Remains (London: Timothy Garthwait, 1652), 63.*

[3] The North Atlantic Treaty Organization (NATO) defines HUMINT as "intelligence derived from information collected by human operators and primarily provided by human sources." *NATO Glossary of Terms and Definitions (AAP-6), (North Atlantic Treaty Organization, 2021) v.s. "HUMINT," 65. In other words, "HUMINT is intelligence obtained from people." Michel Herman, "Collection Sources" in Michel Herman, Intelligence Power in Peace and War ed. (Cambridge, UK: Cambridge University Press, 1996), 61. And there are a variety of HUMINT types, for example: (1) "Recruited 'assets', or people who are enticed or coerced into providing information, either knowingly or surreptitiously; (2) "Walk ins," or assets who, for personal, ideological or financial reasons, volunteer to provide information about their countries or organizations, while remaining in place and concealing their cooperation; (3) Defectors and émigrés, who provide information about their countries or organizations, after leaving and finding sanctuary with an intelligence service; (4) Liaison services, or members of foreign intelligence organizations that knowingly agree to Exchange information [...]" "Human Intelligence and 11 September," Strategic Survey 104, no. 1 (2004): 28.*

[4] Some passages point to police techniques, although our focus is espionage, we will not shy away from pointing out some police techniques that appear in old books.

[5] Marina de Andrade Marconi, Eva Maria Lakatos, *Fundamentos de Metodologia Científica 5. ed. (São Paulo: Ed. Atlas, 2003) p.109.*

[6] Cláudia Regina Silveira. *Metodologia da pesquisa. 2 ed. (Florianópolis: Publicações do IF-SC, 2011).*

[7] Steven J. Mithen, "Looking and Learning: Upper Palaeolithic Art and Information Gathering," *World Archaeology 19, no.3 (1988): 297.*

[8] Equivalent to Surveillance, the following and observing targets without being noticed. William R. Johnson, and William Hood, "How to manage

physical surveillance," in *Thwarting Enemies at Home and Abroad: How to Be a Counterintelligence Officer (Washington, DC: Georgetown University Press, 2009) 66–80.*

[9] "Interrogation is a conversational process of information gathering. The intent of interrogation is to control an individual so that he or she will either willingly supply the requested information or, if someone is an unwilling participant in the process, to make the person submit to the demands for information". Brian Hoyle, Interrogation. In *Encyclopedia of Espionage, Intelligence, and Security, K. Lee Lerner, Brenda Wilmoth Lerner (ed.) v.2 (Farmington Hills: The Gale Group, 2004), 151.*

[10] Recruitment is "the deliberate and calculating effort to gain control of an individual and to induce him or her to furnish information or to carry out intelligence tasks for an intelligence or CI [counterintelligence] service." *Counterintelligence Glossary, s.v. "recruitment," 270.*

[11] Glenn Sulmasy and John Yoo, "Counterintuitive: Intelligence Operations and International Law," *Michigan Journal of International Law 28, no.3 (2007): 626; Nicholas Eftimiades, "On the Question of Chinese Espionage". Brown Journal of World Affairs 26, no. 1(2019): 125.*

[12] Hannes D. Galter, "The Mesopotamian God Enki/Ea", *Religion Compass 9, no.3 (2015): 66–9. https://compass.onlinelibrary.wiley.com/doi/epdf/10.1111/rec3.12146*

[13] Rodrigo Cabrera, "The Three Faces of Inanna: An Approach to her Polysemic Figure in her Descent to the Netherworld", *Journal of Northwest Semitic Languages 44, no.2 (2018):60.*

[14] Michèle Louise Meijer, "Identifying Borrowings between Eastern Mediterranean Cults: A Methodology Based on a Comparison of Cultic Practices for Ištar and Meter," (PhD thesis, Vrije Universiteit, 2021), 165.

[15] Galter, "The Mesopotamian God, 69.

[16] As sex is a very powerful basic human need, no wonder this is widely used in espionage. In the 16th century, Machiavelli already pointed out that "men are driven by two principal things, either by love or by fear" (Niccolo Machiavelli, *The Discourses on Lyvi (Chicago: University of Chicago Press, 1996), 263). There is even a specific type of operation that exploits the need for sex: honeypot or honey trap operations. They consist of "the use of attractive male and/or female agents to lure strategically placed victims into their trap and, in turn, cause them to compromise secrets." James Welch, Behind Closed Doors: Sex, Love and Espionage: The Honeypot Phenomenon (American Military University, 2012), 1.*

[17] D. Pugazhendhi, "Greek, Tamil and Sanskrit: Comparison between the Myths of Prometheus, Sembian and Sibi," *Athens Journal of Philology 8, no.3 (2021):159.*

[18] Daniel Luttrull, "Prometheus Hits 'The Road': Revising the Myth," *The Cormac McCarthy Journal 8, no.1 (2010): 17.*

[19] Pugazhendhi, "Greek Tamil and Sanskrit," 159.

[20] Marco Cepik, "Sistemas nacionais de inteligência: origens, lógica de expansão e configuração atual", *DADOS – Revista de Ciências Sociais 46, no.1(2003): 114 (in Portuguese).*

[21] Gn. 42:1-17. King James Bible Online - KJBO (2022).

[22] Num. 13:17-19 (KJBO).

[23] "A mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an adversary or to obtain data concerning the meteorological, hydrographical or geographic characteristics of a particular area." *NATO Glossary (2021) v.s. "Reconnaissance," 109.*

[24] Num. 21:32 (KJBO).

[25] Num. 21:1 (KJBO).

[26] "Counterintelligence (CI) is a broader term than Counter-espionage (CE)." W. Thomas Smith Jr., *Encyclopedia of the Central Intelligence Agency (Nova York: Facts On File, 2003), s.v. "Counterintelligence," 66. CI is "Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or their agents, or international terrorist organizations or activities (Counterintelligence Glossary, s.v. "Counterintelligence", 55). Counterespionage (CE) is the offensive, or aggressive, side of counterintelligence. It involves the identification of a specific adversary and knowledge of the specific operation he is conducting. US Senate. Senate Report # 94-755 (aka Church Committee Report), Book I, 26 April 1976, 166. https://www.intelligence.senate.gov/sites/default/files/94755_I.pdf*

[27] Exfiltration is "a clandestine rescue operation designed to get a defector, refugee, or operative and his or her family out of harm's way". *Counterintelligence Glossary, s.v. "Exfiltration," 135.*

[28] Josh. 2:1 (KJBO).

[29] Josh. 2:2-3 (KJBO).

[30] Josh. 2:12-14 (KJBO).

[31] Josh. 6:22-23, 25 (KJBO).

[32] Recruitment through coercion is commonly used in the police environment, through threats of arrest, so "in order to avoid or at least lessen the effects of prosecution" people became informants. J. Mitchell Miller, "Becoming an Informant," *Justice Quarterly, 28, no.2 (2011): 204.*

[33] Judg. 1:23-25 (KJBO).

[34] This passage resembles modern foreign interference, which has affected elections in several countries today. According to the Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions, foreign interference is "clandestine, deceptive, or personally threatening activities by a foreign state, or those acting on its behalf, that are detrimental to the interests" of the target. *Foreign Interference Commission, Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions – Initial Report. 2024, 56.*

[35] 2 Sam. 15:10 (KJBO).

[36] Chron. 19:1-7 (KJBO).

[37] Judg. 18:2; 1 Sam. 26:4 (KJBO).

[38] This Jesus monitoring action can be understood, in modern terms, as surveillance, "systematic observation of a target," *Counterintelligence Glossary, s.v. "surveillance," 310.*

[39] Luke 20:20 (KJBO).

[40] Matt. 22:17 (KJBO).

[41] Sting operations are police operations that provide enticements or opportunities for the targeted offender to commit crimes and be arrested. Graeme R. Newman, *Sting Operations. Response Guides Series No 6, U.S. Department of Justice, 2007. 3.*

[42] "The techniques adopted by spies to conceal their activities [….]" Frederick P. Hitz, *The Great Game: the myth and reality of espionage (New York: Alfred A Knopf, 2004), 66.*

[43] "An individual who voluntarily offers his services or information to a foreign government." *Counterintelligence Glossary, s.v. "walk in," 342.*

[44] Matt. 26:14-16 (KJBO).

[45] Matt. 26:46-50 (KJBO).

[46] Joseph L. Walden, "Sun Tzu: The Art of War and 21st Century Curriculum Development – What Can the Early Asian Philosopher Tell Us About Developing Curriculums in the 21st Century?", *Advances in Social Sciences Research Journal 7, no.10 (2020): 330; Lei Sha, "Translation of Military Terms in Sun Tzu's The Art of War International," Journal of English Linguistics 8, no.1 (2018): 196-7.*

[47] Sha, "Translation of Military Terms," 197.

[48] Vlado Dimovski, Miha Marič, Miha Uhan, et al. "Sun Tzu's 'The Art of War' and Implications for Leadership: Theoretical Discussion," *Organizacija 45, no.4 (2012):151.*

[49] K.S. Vishnu Prabhu and Laxmi Dhar Dwivedi, "A Brief Comparison on 'Espionage' and the Importance of 'Spies' between Kautilya's The Arthashastra and Sun Tzu's The Art of War," *Mediterranean Journal of Social Sciences 6, no.6 S4 (2015):544.*

[50] Sun Tzu, *The Art of War, translated by Lionel Giles M. A. (London: Luzac and Co., 1910). 51-2.*

[51] Ibid., 50.

[52] Ibid.

[53] Ibid.

[54] Ibid., 51.

[55] Department of the Army, *Human Intelligence Collector Operations,*

Field Manual no. 2-22.3 (Washington, DC: Department of the Army, 2006), 1-8.

[56] Bram Champagne, "The United Nations and Intelligence: A Thesis" (Certificate-of-Training in United Nations Peace Support Operations, 2006), 17.

[57] Marcelo Bastos de Souza, "Guerra Irregular no contexto da Estratégia da Resistência," (MSc. Diss., Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2014), 37.

[58] Charles W. Innocenti, Ted L. Martens and Daniel E. Soller, "Direct support HUMINT in Operation Iraq Freedom," *Military Review, 2009, 53.*

[59] Sun Tzu, *The Art of War, 51.*

[60] Sun Tzu, *The Art of War, 51-2.*

[61] Anderton CH, Carter Jr., "Military Alliances," in P*rinciples of Conflict Economics: A Primer for Social Scientists (Cambridge: Cambridge University Press; 2009), 222-245; Apud Giampaolo Servida, "Double Agents: Masters of Deception in a Shadowy World," September 8, 2024.*

[62] Theses doomed spies are a "deception channel, a means by which controlled information can be reliably transmitted to the target." *Counterintelligence Glossary, s.v. "Deception Channel," 103.*

[63] "Any attempt—by words or actions—intended to distort another person's or group's perception of reality" *Counterintelligence Glossary, s.v. "Deception," 102.*

[64] Sun Tzu, *The Art of War, 51.*

[65] Ibid., 8.

[66] Ibid., 51.

[67] "Human Intelligence and 11 September," 2004, 28.

[68] Sun Tzu, *The Art of War, 51-2.*

[69] Defense Personnel Security Research Center, *Espionage Cases: 1975-2004 (Monterey: Defense Personnel Security Research Center, 2004). 2.*

[70] Money, Ideology, Compromise or Coercion, and Ego or Excitement. Randy Burkett, "An Alternative Framework for Agent Recruitment: From MICE to RASCLS," *Studies in Intelligence 57, no.1 (2013): 7-17.*

[71] "The compulsory withholding of knowledge, reinforced by the prospects of sanctions for disclosure" Susan Maret. *On Their Own Terms: A Lexicon with an Emphasis on Information-Related Terms Produced by the U.S. Federal Government. 6th edition, 2016, 361.*

[72] Sun Tzu, *The Art of War, 51-2.*

[73] Sha, "Translation of Military Terms," 195.

[74] Muhammad Saad and Liu Wenxiang, "National Security in Kautilya's Arthashastra: A Content Analysis," *International Journal of Humanities and Education Development 2, no.2 (2020):130.*

[75] Roger Boesche, "Kautilya's Arthasastra on War and Diplomacy in Ancient India," *The Journal of Military History 67, no.1 (2003):10.*

[76] G.S. Aravind and Laxmi Dhar Dwivedi, "Kautilya's The Arthashastra: A Marxist and Psychoanalytical Reading of Select Chapters in Book I," *Mediterranean Journal of Social Sciences 6, no.6 S2 (2015):678.*

[77] Saad and Wenxiang, "National Security in Kautilya's Arthashastra," 138.

[78] Kautilya, *Arthashastra, Translated by R. Shamasastry (Bangalore: Government Press, 1915), 30.*

[79] Disguise is "concealment or misrepresentation of the physical characteristics or true nature or identity of a person or object," *Counterintelligence Glossary, s.v. "Disguise." 119.*

[80] Kautilya, *Arthashastra, 299.*

[81] Ibid., 25.

[82] Ibid., 22, 24.

[83] Ibid., 24.

[84] Ibid., 24-25.

[85] Ibid., 27.

[86] Ibid., 29.

[87] Arthur S. Hulnick, "What's wrong with the Intelligence Cycle," *Intelligence and National Security 21 n.6 (2006): 959–979.*

[88] "The principle of controlling access to sensitive information so that it is available only to those individuals or organizational components with an official 'need-to-know' and only to the extent required for the performance of assigned responsibilities." *Counterintelligence Glossary, s.v. "Compartmentation." 44.*

[89] Kautilya, *Arthashastra, 29.*

[90] Ibid., 30.

[91] Ibid., 32-3.

[92] Ibid., 44.

[93] Ibid., 46.

[94] "Clandestine, deceptive, or personally threatening activities by a foreign state, or those acting on its behalf, that are detrimental to the interests" of the target. Foreign Interference Commission, Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions – *Initial Report (2024), 56.*

[95] Kautilya, *Arthashastra, 552.*

[96] Ibid., 565.

[97] Ibid., 582.

[98] Aravind, "Kautilya's The Arthashastra," 638.

[99] Also named *Siyar al-Muluk ("Manners of the Kings"). Nizam Al-Mulk, The Book of Government or Rules for Kings (Oxfordshire: Routledge, 2002), 12.*

[100] Süleyman Göksoy, "Ethical principles in Nizam Al-Mulk's Siyasatnama book in terms of Turkish management history", *Journal of Pedagogical Research 1, no.1 (2017):77.*

[101] Rose Mary Sheldon, Espionage in the Ancient World: An Annotated Bibliography of Books and Articles in Western Languages (Jefferson: McFarland, 2015), 51.

[102] Al-Mulk, *The Book, 74-87.*

[103] Ibid., 75.

[104] Ibid., 87.

[105] Thucydides, *The History of the Peloponnesian War (Longmans, Green, and Co, 1876).*

[106] Plutarch, *Plutarch's Morals (Arthur Richard Shilleto trans, London: George Bell and Sons, 1898).*

[107] Gaius Julius Caesar, *De Bello Gallico and Other Commentaries (Ernest Rhys, 1915). book I, paragraph XX.*

[108] "Historia Augusta is a late Roman collection of biographies of Roman Emperors, Caesars and usurpers, covering the period from Hadrian to Carus, Carinus and Numerianus, with a gap spanning the years 244 to 253 CE"; Armando Martins and others, "Historia Augusta authorship: an approach based on Measurements of Complex Networks," *Applied Network Science 6, no.50 (2021):2.*

[109] K. S. Cunliffe, "Hard target espionage in the information era: new challenges for the second oldest profession," *Intelligence and National Security 36, no.7 (2021): 1018–1034.*

[110] Ecclesiastes 1:9 (KJBO).

Alfredo Ribeiro Pereira, MSc (USP), is an Associate Researcher at the Intelligence School, Brazilian Intelligence Agency (Esint/ABIN) and has served as an intelligence officer at the ABIN since 2007. He is also a law student at the Federal University of Mato Grasso do sol Brazil. He was awarded with the Friend of the Brazilian Navy medal.

Dr. Cesar Augusto Silva da Silva is an Associate Professor at Law School, at Federal University of Mato Grosso do Sul (Fadir/UFMS), Brazil.

Project DART:
The Anatomy of a Failed Counterintelligence Technical Attack Operation and the Cascading Consequences

by **Aden Magee**

During the Cold War, U.S. Department of Defense (DoD) counterintelligence was regularly overmatched by Soviet bloc intelligence services due to a lack of expertise, experience, centralized coordination, and mission focus. DoD counterintelligence was slow to mature in operational capabilities, due largely to a gap in understanding regarding the threat posed by determined and sophisticated adversaries. This legacy of inferiority was epitomized by the DoD relationship with the Soviet Military Liaison Mission (SMLM) that had been based in Frankfurt, West Germany, from 1947-1990.

By the mid-1980s, Army counterintelligence reached its highest level of capability ever, with specialized organizations neutralizing a series of high-level spies in a highly sophisticated manner.[1] While many still recall this period as the zenith of Army counterintelligence, this has led to a tendency to forget how poorly counterintelligence performed during the nearly four decades preceding this zenith. One operation—Project DART—symbolized Army counterintelligence performance during the Cold War era in Europe, and marked an unfortunate inflection point for Army counterintelligence during that time.

MILITARY LIAISON MISSION HISTORICAL CONTEXT

At the conclusion of World War II, the Allied powers (the United States, Britain, France, and the Soviet Union) agreed to divide Germany into four zones of occupation. In 1947, as the post-war situation began to deteriorate among the Soviets and the other three allies, the United States, Britain, and France signed separate agreements with the Soviet Union to exchange Military Liaison Missions (MLMs) to facilitate communication and transparency. The U.S. MLM (USMLM) was established in the Soviet sector in Potsdam, Germany, and the Soviet MLM (SMLM) was established in the U.S. sector in Frankfurt, Germany. The sides agreed to accredit 14 military members and up to 10 vehicles at each MLM.

As relations between the United States and the Soviets became adversarial, the MLMs rapidly became the most valuable sources of intelligence regarding the status of military forces in the opposing zones of occupation. With the relative freedom of movement and rights of extraterritoriality allowed by the MLM exchange agreement, the USMLM mission shifted primarily to one of intelligence collection by traveling throughout the Soviet sector (referred to as "tours" or "touring") and reporting on their observations (overt human intelligence or HUMINT).[2]

In 1949, the East/West schism became official when the three remaining Allied powers merged their sectors to establish the Federal Republic of Germany (West Germany), and the Soviets responded by declaring their sector as the Democratic Republic of Germany (East Germany). By this point, the only purpose for the boundaries of the four zones of occupation was to define the areas in which each MLM was authorized to operate.

In comparison to the other MLMs (Soviet, British, and French), the USMLM was likely the most aggressive collector of intelligence and rivaled the Allied Joint Interrogation Center network as the U.S. DoD's most prolific source of overt HUMINT during the Cold War. While the SMLM did conduct similar overt HUMINT tours to observe U.S. military activities, they were much less active/aggressive than their U.S. counterparts.[3] This dichotomy could be explained due to the Soviet sector being densely populated with military forces maneuvering freely throughout, while there were many fewer U.S./NATO forces in West Germany, and activity of military interest in the U.S. sector was limited to a relatively small number of restricted training facilities.[4] This disparity in collection activity was significantly increased when the USMLM established a 56-person support headquarters in the U.S. sector of Berlin, which provided enhanced intelligence analysis support and enabled the MLM to rotate in tour personnel and vehicles to conduct multiple and continuous 24/7 collection missions. Still, the SMLM never attempted to replicate such a construct from East Germany (or

Czechoslovakia) and maintained its relatively austere 14-member footprint operating out of Frankfurt, which was 183 miles from the East German border crossing point.

Early developments in the MLM dynamic immediately ingrained the perspective among U.S. Army Europe (USAREUR) intelligence leadership that since the USMLM was more actively and effectively collecting overt HUMINT relative to the Soviets, the MLM exchange agreement was to their marked advantage. Therefore, the USAREUR intelligence leaders were cautious regarding any actions that might cause the Soviets to question the efficacy of the MLM agreement. In addition to these higher-level sensitivities, there were pragmatic reasons for not taking action against the SMLM that might aggravate the Soviets. When U.S. forces took actions against an SMLM tour, such as detaining a vehicle when detected observing military activities, the Soviets (and their East German surrogates) would react by taking escalatory actions against USMLM that would have immediate impacts on intelligence collection operations (and the safety of USMLM personnel). Although there were some restrictions regarding where SMLM tours were allowed to travel, efforts to counter the low-threat activity would never warrant the negative impacts the reaction would have on USMLM operations. As such, there was a strong propensity to allow the assumed-to-be-benign SMLM threat to exist and avoid retaliations that would invariably impede USMLM collection activities.

Following World War II, Army counterintelligence in Europe was administered by the Counterintelligence Corps (CIC). By 1949, all counterintelligence organizations were consolidated under the 66th CIC Detachment, which was redesignated as the 66th CIC Group in 1951. The 66thCIC Group was an administrative headquarters comprised of regional commands responsible for counterintelligence operations in support of the Army commands in their respective regions.[5] Based on this construct, the decentralized CIC regions were responsive to the requirements of commanders and intelligence officers with a tactical combat perspective, but no perspective regarding how a sophisticated foreign intelligence service with an operational platform in their area of responsibility might be expected to operate. The 66th CIC Group Region III area of responsibility included Frankfurt, which was, therefore, the regional command responsible for counterintelligence coverage of the SMLM.[6] However, the SMLM had relative freedom of movement privileges throughout the U.S. sector, which spanned nearly 40,000 square miles and multiple CIC regions.

The MLM agreement was unique among international treaties in that it was not executed or administered by the U.S. Department of State; rather, it was managed under the purview of the DoD and USAREUR. As such, USAREUR restricted any external agency involvement with the SMLM to preclude any actions that might upset the Soviets and impact the USMLM intelligence collection mission in the Soviet sector.[7] Most notably, this restriction was the lone exception to the Central Intelligence Agency's (CIA) worldwide primacy over foreign counterintelligence activities. In addition, USAREUR adamantly enforced U.S. authorities as an occupying power to restrict the West German counterintelligence service from operating against the SMLM. In fact, to prevent any possibility that West German intelligence or security entities would take action against the Soviets, the West Germans were directed to ignore the SMLM and respect their absolute rights of extraterritoriality.[8]

THE ANATOMY OF A FAILED TECHNICAL ATTACK OPERATION

The Allies undertook some major technical collection efforts as the Soviet Communist system began to materialize as an existential threat. Operation GOLD was a large-scale technical operation conducted jointly by the CIA and the British Secret Intelligence Service (SIS) in 1955 to tap into the landline communications of the Red Army headquarters in Berlin using a tunnel from the American zone into the Soviet zone. The KGB discovered the operation through their spy in the SIS, George Blake, but to protect the true source of the compromise, they waited to "discover" the tunnel during a major rain and flooding event in April 1956.[9] The short-lived, 11-month operation collected valuable information from the unwitting headquarters staff, demonstrating that the CIA could execute complex and effective technical collection operations.[10] One year later, USAREUR and the 66th CIC were presented with the opportunity to conduct a much less complex technical collection operation against the SMLM.[11]

In March 1956, USAREUR agreed to build a new SMLM facility for the Soviets.[12] Despite the USAREUR preference to avoid taking actions that might aggravate the Soviets and place the MLM agreement at risk, even the most dovish of officers could not pass on this unprecedented opportunity. The U.S. government would be building a facility for its highly belligerent adversary, from the ground up, with only limited Soviet presence during construction.

On 26 March 1956, HQ USAREUR notified the 66th CIC Group of the plan to construct the new SMLM compound

and requested an assessment of the feasibility of planting surreptitious audio devices in the buildings during construction. In April 1956, the 66th CIC Group agreed with the bugging concept. However, notwithstanding the recent execution of the technically complex and effective Operation GOLD, USAREUR maintained its parochial position that the CIA could not be involved in counterintelligence operations involving the SMLM.

The SMLM complex project was initially planned for completion by September of that year, which would have presented a challenge to execute such a time-constrained technical operation.[13] However, there was a series of delays in 1956 and 1957 due to ongoing negotiations between USAREUR and the Soviets regarding the site for the compound. In late 1957, the sides agreed to the project plan, and the construction plans were finalized in January 1958. At this juncture, USAREUR asked the 66th CIC Group for the status of planning for the technical operation. Inexplicably, there had been no progress in planning for the technical surveillance of the SMLM compound buildings over an extended period of project delays.[14] The construction project broke ground in April. Further delaying the technical planning, the 66th CIC Group waited until it had a copy of the construction plan on 9 May 1958 before directing its Technical Aids Division to provide a feasibility assessment about the installation of clandestine listening devices in the compound.[15] This was the first time, since initially being alerted in March 1956, that technical experts became involved in planning for the operation. On 4 June 1958, the Technical Aids Division provided a report specifying that the 'take' would need to be transmitted by wires embedded on telephone cables, which would need to run from the compound to a nearby 'stakeout' location.[16] Albeit much later than it should have been, the requirement to acquire a stakeout location in the vicinity of the SMLM compound was identified.

The project to bug the SMLM compound was assigned the codename Project DART on 8 July 1958.[17] There was a series of technical meetings from August to October 1958 to discuss the operation. Although the basic parts were coming into place, one key component was not. Technicians could not finalize any plans until they identified the location of the junction box that would transmit the "take" from the compound. The wiring schema from the listening device needed to be configured based on the location of this box, and the location of the box could not be determined until the stakeout location to which the wiring would run was identified. So again, a component of the plan that could have been determined much sooner was that the only suitable stakeout location would be a unit in one of the apartment complexes near the compound. On 30 October 1958, the 66th CIC Group finally authorized Region III to begin the process of acquiring an apartment.[18]

Region III determined that all apartment complexes in the vicinity of the compound were occupied and could not be sublet, so agents started conducting background checks on all occupants to identify a suitable candidate to approach with an offer to cooperate. This lengthy process of securely vetting potential candidates continued for nearly four months. On 24 February 1959, Region III agents approached a German family occupying the desired apartment with a generous offer to relocate them to another apartment, to which the family agreed.[19]

Coincidentally, on the same day of 24 February, Technical Aids Division representatives, who had been disengaged from the project while the apartment issue was being resolved, arrived in Frankfurt for a site assessment of the compound, and readily determined that the construction had progressed beyond the point where listening devices could be installed.[20] The Soviets, who were permitted to observe the construction progress periodically, would have noticed any efforts to deconstruct for the technical operation. In addition, any effort to emplace technical surveillance capabilities after this point would have been apparent to noncleared construction workers.

After this redline determination, there was a flurry of activity to salvage the project and then conduct damage control, but the fact remained that the opportunity for this once-only counterintelligence opportunity was lost. As a face-saving gesture, the 66th CIC Group contended that the apartment remained an important asset that would be attained and used for visual and photographic observation of the SMLM compound.[21] Region III agents then negotiated new occupancy terms with the landlord, and by 10 March 1959, all contracts were signed and money paid to facilitate an occupancy date of 1 May.[22] On 25 March 1959, USAREUR officially canceled Project DART.[23] Although the project was canceled, the apartment continued to be referred to as DART.

After a senior intelligence officer with the USAREUR Deputy Chief of Staff, Intelligence (DCSINT) announced the final decision to terminate Project DART, he provided his candid observations of the project during a concluding meeting with the project leadership team. He expressed his frustration that during a recent visit to the CIC headquarters at Fort Holabird, Maryland, he had been shown 'innumerable' clandestine listening devices that could have been leveraged to make the project successful. The

DCSINT officer accepted a share in responsibility because he admittedly assumed the 66th CIC would understand that a project of this complexity would require that it "pick the best technical brains" available in the United States. He concluded by stating that the Soviets were installing bugs all over the world and in the United States and 'it seemed mighty strange' to him that U.S. counterintelligence could not bug an installation for which the U.S. Army controlled the construction.[24]

The failure to initiate coordination with technical experts early in the planning process had doomed Project DART to failure. Clearly, the 66th CIC Group leadership and Region III were not aware that the stakeout location was the pacing component for the entire operation, and lacked an appreciation for the impact of the delays in gaining this critical component would have on the overall project. Technical experts could have advised in 1956 that the plan would eventually require a nearby stakeout location to receive the take. Even as what should have been a worst-case scenario, had the 66th CIC Group begun the process of securing an apartment when the construction site was determined in late 1957 (rather than late 1958), and had they completed the four-month apartment acquisition process by April 1958 (rather than February 1959), they would have identified the listening post location during the same month as the compound ground-breaking, which would have provided ample time to meet all requirements for the technical operation.

Army counterintelligence negligently botched the unprecedented opportunity to conduct a technical attack operation ("bug") against a Soviet adversary in a facility that was constructed by the U.S. Army Corps of Engineers in West Germany with only limited Soviet supervision. In contrast to Operation GOLD, the effort to plan and execute a much less complex technical operation targeting the SMLM was a complete failure due to a lack of proactive management and expert involvement.

THE DART OBSERVATION POST OPERATION

The abrupt conclusion of Project DART was perceived by the 66th CIC Group as a humiliating failure. This likely led to an overreaction in the near-immediate employment of the newly acquired capability as an observation post to demonstrate that it could provide valuable utility. Region III began continuous surveillance of the SMLM compound on 29 June 1959 while the compound was in the final stages of preparation for occupancy.[25]

SMLM personnel completed their move to the compound between 6 and 9 July. The initial focus of the surveillance was to observe activities immediately before and after occupancy that would disclose any enlightening operations security (OPSEC) measures, such as digging around the buildings, window blanking, or activities indicative of "sweeping" for technical surveillance devices.[26] Other specific observations of interest were items entering the compound that might contain radio or other technical electronic equipment.

The first noteworthy occurrence during the observation post operation was the detection of antenna masts and wires on top of the building housing the communications room on 9 July 1959.[27] The interesting point of this event was that it was not detected by the counterintelligence agents manning the observation post until daylight. This confirmed that the Soviets performed the work during the hours of darkness in a clear effort to avoid observation—an effort that proved successful. This demonstrated that the Soviets wanted to conceal the installation of the antennae and may have indicated that they were already aware or suspicious that the compound was under observation.

On 24 July 1959, counterintelligence agents observed the first indication that SMLM personnel were actively attempting to identify an observation post in the vicinity of the compound, and on 21 August, it was confirmed that the Soviets had identified DART as a U.S. counterintelligence observation post.28 The 66th CIC's compulsive effort to regain credibility by demonstrating that the apartment was a valuable asset resulted in a rushed operation that ended in compromise. In late August 1959, Region III was authorized to terminate 24/7 observation of the SMLM compound.

MIRROR IMAGING AND FALSE ASSUMPTIONS

The Project DART fiasco shaped the USAREUR and 66th CIC approach to the SMLM. Due to the failure, the SMLM was recognized as a sore spot, and the CIC became much less inclined to approach it as one of their primary targets. Logically, if the SMLM were assessed as less of a threat, then Project DART would be considered a less impactful failure. The Project DART debacle had lasting effects on the Army counterintelligence perspective of the SMLM. The tendency to diminish the impact of the failed Operation DART was reinforced by a mindset that disincentivized analysis that questioned the USAREUR position.[29]

Augmenting the USAREUR tendency to downplay the SMLM risk, USAREUR's sensitivities regarding actions that might antagonize the Soviets for fear of retribution against

the USMLM also provided Army counterintelligence some top cover for adopting a relatively hands-off approach. The CIC continued to operate under the regional area support structure, with counterintelligence elements taking direction from USAREUR army combat unit commanders, who viewed the threat from their parochial perspectives. The SMLM was addressed primarily as an OPSEC threat and, therefore, a local, tactical counterintelligence concern.

The USAREUR mindset that solidified regarding the SMLM at this pivotal point is a classic example of the cognitive bias referred to as *mirror imaging*, which is the tendency for an entity to assume an adversary will think and act as it would.[30] Mirror imaging is a mental model that compensates for a lack of facts with assumptions. USAREUR leadership understood the value of the intelligence that the USMLM collected and assumed that this was the obvious manner by which the Soviets would leverage their access in Western Europe. Since the USMLM was such a prolific collector of tactical overt HUMINT, it was assumed this was the same (mirror imaging) threat the SMLM posed. This misapplied logic was compounded by an additional mirror imaging error that reflected a lack of counterintelligence perspective.

Although USAREUR could restrict the CIA from involvement in counterintelligence activities involving the SMLM, the USMLM was bound by CIA jurisdiction over all foreign HUMINT activities. Under CIA purview, U.S. HUMINT was managed under a relatively rigid echelon structure with the CIA conducting strategic (clandestine) HUMINT operations generally associated with recruiting and controlling spies, and the DoD being restricted to tactical, battlefield HUMINT functions such as ground reconnaissance, interrogations, and debriefings. The USMLM was restricted by this paradigm and never considered conducting activities other than overt (tactical) HUMINT collection. Again, USAREUR mirror imaging assumed that Soviet military intelligence viewed the world through the same lens, which it did not.

FAST-FORWARD A QUARTER OF A CENTURY

The USAREUR approach to the SMLM remained relatively consistent until contradicting facts emerged. A series of defectors in the early to mid-1980s exposed the SMLM as a GRU platform conducting clandestine HUMINT and covert operations.[31] After multiple corroborating sources detailed SMLM clandestine HUMINT and covert operations support, USAREUR was compelled to face an inconvenient truth. Over 25 years later, it became apparent that in 1959, the United States defaulted to the wrong course during the Cold War MLM era.

In 1988, in the face of this long-ignored threat, USAREUR finally directed the 66th MI Brigade to establish the capability to conduct counterintelligence operations at the level of sophistication necessary to counter the actual SMLM threat.[32] Lamentably, the capability to execute full-spectrum counterintelligence operations was never effectively deployed against the SMLM before East and West Germany agreed to terms for reunification in 1990, and all operations against the soon-to-be-disestablished SMLM were terminated.[33]

After the end of the Cold War, additional credible sources provided information regarding SMLM covert operations.[34] Based on the multiple credible, independent, and unrelated sources, it is evident that the SMLM operated as a GRU clandestine and covert operations platform while U.S. counterintelligence approached it as a low-level overt HUMINT concern. Perhaps the most consequential aspect of the unmonitored SMLM freedom of maneuver was the key role the SMLMs were reported to have played in preparing for what the Soviets always anticipated as an inevitable war with NATO. USAREUR understood that Soviet doctrine stated they would employ sleeper cells and special operations forces to access man-portable nuclear devices and other weapons caches in support of this imminent invasion.[35] However, like assumptions regarding the believed-to-be benign SMLM intelligence threat, it was assumed that the Soviets leaked this doctrine to spread fear through an aura of invincibility—until it was proven to be true. Potentially most catastrophic of all, the SMLM was confirmed to have supported sleeper cells with agents to be activated before a Soviet invasion to assassinate NATO leaders and delay any decisions to deploy nuclear weapons.[36]

IGNORING THE OBVIOUS

The most remarkable aspect of the entire U.S. and Soviet MLM dynamic was how an absolute lack of strategic counterintelligence perspective engendered an institutional inertia to regard one mission (overt HUMINT) as more important than another (counterintelligence), in a manner that shaped the course of an era. In addition to what should have been intuitively obvious, the indicators were there for decades.

During the MLM era, the 66th CIC managed a central office to receive SMLM sighting reports from USAREUR military units and members when the distinctive SMLM license plate was seen throughout the U.S. sector. USAREUR provided a guard force comprised of West German nationals to operate the compound gate and report to the same office when an SMLM vehicle departed or returned to the compound. Therefore, it was clear that

when an SMLM vehicle departed the compound and was subsequently observed in the vicinity of military activities, it conducted an overt HUMINT tour. Conversely, when vehicles departed the compound and there were no sightings near military activity or no sightings at all, it was known that the purpose of the trip was for non-touring activities. Every year, there were days in the tens to hundreds that the Soviets departed the compound for four hours or less, in what was assessed to be non-tour/non-official travel, for which U.S. counterintelligence had no idea what the destination or purpose of the travel had been. In contrast, SMLM passive overt HUMINT operations in the vicinity of U.S. military forces were conducted very infrequently relative to USMLM collection activities. However, such activities were performed just enough to give the impression that this was a viable mission, which could be considered a unique variation of *cover for action*.[37]

Of any GRU (or KGB) residency worldwide, the SMLM had the greatest capability to service a dead drop in a denied area and transfer the contents by a vehicle with the rights of extraterritoriality to a Soviet bloc country.[38] In contrast to diplomats stationed at extraterritorial locations such as embassies, who had restricted travel areas (usually a 25-mile radius), which would apply to KGB or GRU officers operating out of these platforms, the SMLM had relative freedom of movement over a nearly 40,000-square-mile area. The extraterritoriality rights of SMLM vehicles were never violated by U.S. or West German officials.[39] SMLM personnel traveled from the Frankfurt compound to East Germany on at least a weekly basis in vehicles having absolute rights of extraterritoriality.[40]

In addition to the freedom of movement that facilitated clandestine activities, SMLM compound guard force personnel regularly reported that unidentified individuals entered the compound and met with SMLM officers in the operations building. Walk-ins to Soviet embassies worldwide were a regular means by which traitors volunteered their services to spy, and GRU and KGB officers regularly met with spies in their embassies as a secure location to receive documents/materiel and conduct debriefings.[41] U.S. signals intelligence (SIGINT) confirmed that the SMLM transmitted encrypted communications daily.[42]

The most significant indicator of the SMLM's true purpose, which was also conveniently assumed away, was the location of the SMLM compound. The delays in the two-year negotiations that should have provided the 66th CIC ample time to execute Project DART involved a Soviet demand that the compound remain in Frankfurt. By 1956, the USAREUR headquarters had relocated from Frankfurt to Heidelberg, so the SMLM compound should have logically moved to collocate with the U.S. command to which it was accredited as a liaison element. The Soviets adamantly insisted on remaining in Frankfurt, and USAREUR ultimately acquiesced because the Soviets tolerated the USMLM operating out of its robust West Berlin headquarters, and there were concerns that the Soviets might end the MLM agreement, which would end USMLM collection operations. Had USAREUR and the 66th CIC applied a strategic counterintelligence perspective, the Soviet position regarding the Frankfurt location would have been the reddest of red flags. What the U.S. leaders responsible for the MLM agreement failed to realize was that the KGB and GRU ran their residencies out of embassies and consulates in major cities, where they could clandestinely operate in the large and densely populated areas. Spymasters refer to this as *hiding in plain sight*. Frankfurt was West Germany's fourth-largest city, while Heidelberg was not among the 50 largest cities in West Germany.

A paradoxical footnote regarding the USAREUR decision to prioritize USMLM collection over a counterintelligence focus on the SMLM was that the value of USMLM collection was diminished by other Army counterintelligence shortfalls. A key principle of intelligence is that information collected on an adversary is only completely valuable as long as that adversary does not know the information has been collected/compromised. When the adversary is made aware that information has been collected/compromised, the information becomes less valuable; and, if the information is damaging to the adversary, it would likely be rendered of no value over time due to actions taken to mitigate the damage/risks associated with the compromised information.[43] Sardonically, all the intelligence that USMLM collected for at least the final two decades of the Cold War lost its value as it applied to this intelligence principle. In contrast to the over three-decade void of insider-type information regarding the SMLM during the same period, the Soviets (or their surrogates) had multiple sources who were known to have had access to all USMLM reporting, and are known to have compromised everything they had access to.[44] Although the known spies are recognized for significantly more damaging compromises than USMLM intelligence and collection activities, the fact remains that they provided comprehensive information applicable to USMLM for at least a 20-year period from 1969 to 1988. And these are just the known spies.[45] The irony here was that while USAREUR accepted a counterintelligence vulnerability in the SMLM in favor of USMLM HUMINT collection, it was the weaknesses in the Army counterintelligence program in West Germany that resulted in the devaluation of all USMLM collection activities.

THE DART LEGACY

When Project DART was initially conceived, the CIA had already demonstrated the ability to execute an exceedingly more complex technical intelligence operation. Rather than leveraging this known capability, the project languished in incompetence.

Had Project DART been a success, it could be assumed that the operation would have provided information to demonstrate that the SMLM was involved in clandestine HUMINT operations, and given USAREUR and the 66th CIC cause to appropriately address the true threat. Conversely, this one-time counterintelligence exploitation opportunity was lost, and Army counterintelligence was placed on the wrong trajectory for the next three decades.

Although Project DART was officially terminated in 1959, the apartment continued to be referred to as DART. The early compromise of the capability severely restricted its utility as a long-term counterintelligence enabler. DART was employed in support of various limited-duration operations over the years, but it was never again employed to systematically observe for anomalous activity at the SMLM compound. In fact, it was not until 1985, in the wake of the shooting of a USMLM member by a Soviet sentry in East Germany, that it was manned again on a 24/7 basis for 53 days to support overt surveillance operations canvassing SMLM vehicles leaving the compound.46 And while this was an important show of force operation, it did nothing to address the threat the SMLM posed as a clandestine HUMINT collection (or other active measures) platform.[47]

DART was finally returned to its landlord in October 1990 after the MLMs were disestablished on the day before German reunification. With the details now declassified, DART can be recognized as the longest-standing symbol of the failed counterintelligence effort to address the SMLM threat. Every month from May 1959 until October 1990, a 66th CIC Group/MI Brigade West German national employee would be given the DART rent money out of the Army Intelligence Contingency Fund, drive across the Main River to the Frankfurt apartment complex, and render payment, in cash, to the apartment landlord.[48] Every month for over 30 years, Army counterintelligence paid for an observation post that had been compromised within two months of operation, and regularly went years between operational usages.

Apparently, keeping DART on the books served to give some leaders the false impression that Army counterintelligence was actively addressing the SMLM issue.

NOTES

[1] Notably, Clyde Conrad, James Hall, and Albert Sombolay.

[2] The MLM agreement stated that the MLMs would have "complete freedom of travel wherever and whenever it will be desired over territory and roads in both zones, except places of disposition of military units, without escort or supervision." Extraterritoriality is a form of diplomatic immunity wherein foreign representations are exempted from the jurisdiction of local law of the hosting country; largely recognized as embassies, homes, offices, and vehicles being considered to be situated on the soil of the home country.

[3] Aden Magee, *The Cold War Wilderness of Mirrors: Counterintelligence and the U.S. and Soviet Military Liaison Mission 1947-1990* (Philadelphia: Casemate Publishers, 2021), 3-6.

[4] The North Atlantic Treaty Organization (NATO) was an intergovernmental military alliance among European and North American countries to constitute a system of collective defense whereby its independent member states agreed to mutual defense in response to an attack by any external party—notably a Soviet Bloc attack; the United States, UK, France, Belgium, Luxemburg, and the Netherlands were the original members, with Greece, Turkey, and Spain joining the alliance during the Cold War.

[5] James Gilbert, Jon Finnigan, and Ann Brey, *In the Shadow of the Sphinx: A History of Army Counterintelligence* (Fort Belvoir, VA: U.S. Army Intelligence and Security Command, 2005), 130.

[6] Ibid., 92-93.

[7] Whenever the United States took any actions to restrict the activities of the SMLM, the Soviets would react against USMLM in an escalatory manner, which would invariably restrict the USMLM's intelligence collection mission; the detention of USMLM vehicles was the most common form of retaliation, which was the capture by two or more vehicles operating in coordination to box in and immobilize a SMLM tour vehicle.

[8] Magee, *The Cold War Wilderness of Mirrors,* 24 & 104-105.

[9] The Komitet Gosudarstvennoi Bezopasnosti (KGB) was the Soviet Union's Committee of State that acted both abroad and within the Soviet Union to secure the nation through internal, foreign intelligence, counterintelligence, and secret police functions.

[10] Central Intelligence Agency, "About the CIA, The Berlin Tunnel," November 2012.

[11] Central Intelligence Agency, "About the CIA, The Berlin Tunnel," November 2012.

[12] U.S. Army Intelligence and Security Command, Freedom of Information/Privacy Office, Case #0402F-19 (Project DART), declassified and released 21 June 2019/redacted.

[13] Ibid.

[14] Ibid.

[15] Ibid.

[16] Ibid.

[17] Ibid.

[18] Ibid.

[19] Ibid.

[20] Ibid.

[21] Ibid.

[22] Ibid.

[23] Ibid.

[24] U.S. Army Intelligence and Security Command, Freedom of Information, Case #0402F-19 (Project DART).

[25] Ibid.

[26] Ibid. Operations security (OPSEC) is the process of identifying critical information/activities, determining vulnerabilities that might enable adversary intelligence to observe or collect critical information/activities, and implementing countermeasures to reduce or eliminate the risk of observation or collection by adversary intelligence.

[27] U.S. Army Intelligence and Security Command, Freedom of Information/Privacy Office.

[28] Ibid.

[29] Perhaps this resulted in a disregarded or at least a mishandled counterin-

telligence lead that also occurred in that critical year of the DART mishap. In 1959, the 66th CIC Group became frustrated with an unproductive double agent who was a member of a GRU network operating in West Germany and transferred the agent to the West German counterintelligence service (BfV) with the recommendation that the case be terminated and the network rolled up. However, the BfV saw an opportunity and tasked the agent to become more active and increase contact with his GRU case officer. Although the CIC had lost interest in the agent, the CIA remained involved as the U.S. coordinator due to the larger counterintelligence operation the double agent was a part of. Later that year, the double agent reported that his GRU case officer informed him that his dead drop was serviced by an SMLM and provided emergency communications instructions, which included a radio in an SMLM. This critical lead was lost or never considered credible. In either case, there is no conceivable reason the double agent would have fabricated the information. Sources: Central Intelligence Agency, "KGB Exploitation of Heinz Felfe: Successful Penetration of a Western Intelligence Service," March 1969, originally classified Secret; *National Counterintelligence and Security Center Counterintelligence Reader*, Volume 3: *Post-World War II to Closing the 20th Century*, p. 187.

[30] Richards J. Heuer, *Psychology of Intelligence Analysis* (Langley, VA: Central Intelligence Agency, 1999), 70.

[31] *See generally* Viktor Suvorov, *Inside Soviet Military Intelligence* (New York: Macmillan Publishing Co., 1984); Viktor Suvorov, *Inside the Aquarium: The Making of a Soviet Spy* (London: Hamish Hamilton, 1986); Klaus Behling, *Sione in Uniform: die Allijerten Militarmissionsen in Deutschland, Hohenheim*, (2004), 125-127; Christopher Andrew and Oleg Gordievsky, *KGB: The Inside Story of its Foreign Operations from Lenin to Gorbachev* (London: Hodder & Stoughton, 1990). The Russian military intelligence service was known as the Glavnoye Razvedyvatel'noye Upravlenie (GRU).

[32] The 66th CIC Group was redesignated as the 66th Military Intelligence (MI) Group, and then in 1986 as the 66th MI Brigade.

[33] Magee, *The Cold War Wilderness of Mirrors*, 271-276.

[34] *See generally* Stanislav Lunev and Ira Winkler, *Through the Eyes of the Enemy: Russia's Highest Ranking Military Defector Reveals Why Russia is More Dangerous Than Ever*. (Washington, DC: Regnery Publishing, 1998); Christopher Andrew and Vasili Mitrokhin, *The Sword and the Shield: The Mitrokhin Archive and the History of the KGB* (New York: Basic Books, 1999).

[35] A sleeper is an illegal agent in a foreign country who does not engage in intelligence activities until he or she is activated at a future time. A cache is a hiding place, especially one in the ground, for munitions, equipment, documents, or other items to be recovered when needed; derived from the French verb *cacher,* meaning "to hide."

[36] Spetsnaz: The Soviet's Sinister Strike Force Document Type: CREST Collection: General CIA Records Document Number (FOIA) /ESDN (CREST): CIA-RDP90-00965R000706940070-2 Release Decision: RIPPUB Original Classification: K Document Page Count: 3 Document Creation Date: December 22, 2016, Document Release Date: December 15, 2011, Sequence Number: 70 Case Number: Publication Date: April 1, 1986. The Soviets employed a similar strategy during the 1979 invasion of Afghanistan.

[37] &RYHU IRU DFWLRQ LQYROYHV DFWLQJ LQ D PDQQHU WKDW SURYLGHV D SODXVLEOH UHDVRQ IRU EHLQJ LQ D JLYHQ ORFDWLRQ RU RWKHUZLVH FDUU\LQJ RXW WKH DFWLRQ LV QRW WKH WUXH SXUSRVH

$ UHVLGHQF\ ZDV D .*% RU *58 LQWHOOLJHQFH DQG DFWLYH PHDVXUHV RIILFH OHJDO UHVLGHQFLHV DV WKH 60/0 EDVH RSHUDWHG

PHQWV VXFK DV 6RYLHW HPEDVVLHV DQG FRQVXODU

DWHG RXW RI HQWLWLHV WKDW ZHUH QRW VDQFWLR

D UH]LGHQWXUD $ GHDG GURS ZDV D PHWKRG

PDWHULDO WR RU IURP DQ DJHQW RU DVVHW ZKHUH LQIRUPDWLRQ LV OHIW WR EH SLF

XS REYLDWLQJ WKH QHHG IRU GLUHFW FRQWDFW EHWZHHQ DQ DJHQW DQG WKH DJHQ

KDQGOHU OHDYLQJ GRFXPHQWV RU PDWHULDO LQ D GHDG GURS RU UHWULHYLQJ WKH

FRQWHQWV RI D GHDG GURS DUH ERWK UHIHUUHG WR DV ³VHUYLFLQJ´ WKH GHDG GURS

7KH ORQH H[FHSWLRQ ZDV DQ LOO FRQFHLY

SODQW OLVWHQLQJ GHYLFHV LQ DQ 60/0 YHK

UHSDLUV

5HLQHU 3DXO)XOOH ZKR ZDV DUUHVWHG L

VS\LQJ IRU WKH (DVW *HUPDQ 6WDWH 6HFXU

KLV JXDUG GHWDLO DQG PDGH KLV ZD\ WR W

ZKHUH KH ZDV GULYHQ WR (DVW *HUPDQ\ KLG

LQ WKH WUXQN RI D 60/0 YHKLFOH 8OULFK +

War Story, Ed Digital, 2020.

[41] Confirming what should have been intuitively obvious for decades, GRU officer Vladimir Rezun defected to British intelligence and reported that the GRU referred to the SMLMs as residencies, which by definition meant they were sophisticated intelligence-collection platforms. He asserted that SMLMs made up the majority of the GRU residencies in West Germany, with the other two of their five residencies being collocated with the KGB residencies in the Bonn embassy and Cologne consulate. Rezun also reported that during his time as a GRU HUMINT officer stationed in the GRU residency operating out of the Soviet mission to the United Nations Office at Geneva from 1974 to 1978, he was made aware of two separate episodes in which a U.S. Army sergeant and later a U.S. Army major walked into an SMLM and volunteered to provide classified information/materiel for money. Rezun's visibility on these two episodes during his tenure in Switzerland would not suggest that these were the only two isolated cases of the SMLMs managing espionage-related activities over that four-year period, and certainly not over the decades-long period of SMLM operations.

[42] Magee, *The Cold War Wilderness of Mirrors,* 55.

[43] Spies are commonly given more lenient plea deals when they divulge the information that they had compromised to enable a comprehensive damage assessment.

[44] During this period, at the national level, U.S. counterintelligence suffered from policy and practices that disincentivized defections from agencies such as the KGB and GRU. As such, there was a void in information regarding Soviet intelligence collection efforts. When a toxic director of counterintelligence at the CIA was relieved after a two-decade reign, policies changed, and by the mid-1970s, defectors were providing information that led to many of the greatest U.S. counterintelligence successes in the 1980s and 1990s.

[45] George Trofimoff, James Hall, Zoltan Szabo, Clyde Conrad, Roderick Ramsey, Jeffrey Gregory, Jeffrey Rondeau, and Kelly Warren; all but Trofimoff and Hall were members of the Szabo/Conrad ring.

[46] Annual Historical Review, U.S. Army Intelligence and Security Command (INSCOM), FY 1985, p. 96 (110).

[47] $FWLYH PHDVXUHV ZDV D 6RYLHW WHUP GHV

FRYHUW RU GHFHSWLYH RSHUDWLRQV WR VX

SUDFWLFHV DFWLYH PHDVXUHV EXW LQ WKH

SUDFWLFHV DV ³PHDVXUHV RI VXSSRUW ´

7KH ,QWHOOLJHQFH &RQWLQJHQF\ )XQG ,&

VRXUFH IRU ³RII WKH ERRNV´ IXQGLQJ QHHGV

Aden Magee is a career intelligence and counterintelligence polymath. A public domain search provides a detailed reference for his recent body of work. He is a retired U.S. Army officer and a veteran of foreign wars. He has previously published on this topic.

Intelligence Studies: A Definitional Conundrum

by **Dr. William C. Spracher**

Over the years, the literature on intelligence has employed a wide variety of terms that have sometimes caused confusion and hair-splitting when it comes to explaining this critical emerging academic discipline. Some authors discuss "intelligence studies" without ever defining the term precisely. I offer a common-sense perspective that may help clear up the confusion. It is based on my doctoral dissertation completed 16 years ago, while new and enhanced intelligence studies programs were expanding across the nation, in large part due to the increased interest and concern in the wake of the failures that contributed to the 9/11 attacks. Many were aided by seed money from the federal government to help fix the problems, such as that provided through the Intelligence Community Centers for Academic Excellence (IC CAE) program established in 2005 and overseen by the fledgling Office of the Director of National Intelligence. The paper was titled "National Security Intelligence Professional Education: A Map of U.S. Civilian University Programs and Competencies."[1]

In that paper, I delineated national security intelligence as a category separate from law enforcement intelligence (which now includes homeland security intelligence) and competitive intelligence (which some equate to business intelligence, though there is some hair-splitting in this domain also). All three categories fall under the mission and focus of the International Association for Intelligence Education (IAFIE), founded in 2004 to promote intelligence education and training, a mission shared in part by the National Military Intelligence Foundation. In fact, in 2012, I organized and emceed a one-day symposium on "Intelligence Education and Training," held in Fairfax, VA, that was co-sponsored by the local DC chapters of IAFIE and then-NMIA (the Association was disestablished in 2017 and its missions assumed by NMIF). An edition of *AIJ* was published in 2013 (vol. 31, no. 2) which focused on that theme, incorporating much of the content from the symposium, including an introductory piece based on the keynote address by Dr. Mark Lowenthal, "Intelligence Education: *Quo Vadimus*?" An earlier edition predating my tenure as *AIJ* editor beginning in 2009 also highlighted the education and training theme.

The distinction between intelligence education and intelligence studies must be clarified, because these two terms seem to be used almost interchangeably in much of the literature. I view intelligence studies as a *subset* of intelligence education. College professors have been teaching about intelligence de facto for decades, but usually that has occurred more as an ancillary mission subsumed in programs belonging to the more traditional departments, such as political science, law schools, or popular interdisciplinary offerings like international relations, global studies, and security studies. The phenomenon of intelligence studies per se, taught by specialized departments or institutes and often leading to terminal degrees with the word "intelligence" in their titles (e.g., American Military University's Doctor of Strategic Intelligence), is fairly new.

Intelligence studies is a key component of intelligence education, and several higher education institutions in the United States have developed robust intelligence studies programs. Nevertheless, how these programs interact with other disciplines in producing a well-rounded graduate properly prepared for employment in the national security intelligence field is the province of intelligence education. There is more to educating an intelligence professional than merely subjecting him or her to an intense intelligence studies program (many of which focus almost exclusively on analysis). Developing an overall curriculum that gives the student all the tools he or she needs to become an intelligence "generalist" should be of concern to higher education administrators. Though a recognized "specialist," an analyst will be much better prepared for difficult on-the-job tasks if he/she has a thorough grounding in some subject other than just intelligence analysis, such as politics, economics, mathematics, literature, foreign languages, or computer science/cybersecurity.

In the early days of IAFIE, Dr. Lowenthal and one of the Association's founders, former FBI official Robert Heibel, often disagreed publicly about what the proper curriculum should be for producing a well-rounded intelligence professional. Heibel then headed Mercyhurst College's (now University) heralded intelligence analysis program and often boasted how many of its graduates were landing solid jobs in the IC. Lowenthal countered that, before learning how to do analysis, students needed to be schooled in a subject that merited being analyzed. In other words, he argued that students needed to learn about a discipline such as history, political science, physics, or engineering before tackling the processes for analyzing complicated issues within that discipline. This was not the only subject generating arguments among the IAFIE faithful. Others

included whether intelligence was a legitimate profession and whether intelligence studies was a valid academic discipline. Those discussions continue today. I interviewed Mark Lowenthal and Bob Heibel as subject matter experts for my dissertation and consider them as friends and highly accomplished intelligence scholars.

As a former intelligence officer, both in the Army and later as a civilian, I value intelligence education in general and intelligence studies as a critical component of it. Although I held a couple of positions in the military that had the word "analyst" in their job description, I have never been a full-time analyst. Therefore, I may not be speaking from a position of authority. However, as a longtime editor of an intelligence journal and a former professor at the National Intelligence University, I have an appreciation for the profession and the skills required to succeed in it. Let us stop quibbling about definitions and tackle the challenge of educating our future intelligence professionals, be they analysts, collectors, managers, instructors, or simply knowledgeable U.S. citizens concerned about national security.

NOTES

[1] George Washington University Graduate School of Education and Professional Development, August 31, 2009.

Dr. William C. Spracher is editor emeritus of the American Intelligence Journal *and a member of the NMIF board of directors. He is also vice president emeritus of the International Association for Intelligence Education and continues to serve on its board of directors. In addition, he is a member of the board of trustees of the Dwight D. Eisenhower Society and writes articles for its newsletter about Ike's leadership, including his deep understanding of and appreciation for intelligence and deception. A retired Army intelligence officer, in 2025 Bill was selected for the Military Intelligence Hall of Fame.*

2024 Night of Heroes

Foundation of Educational Skill Sets Needed for the 21st Century Military & Cognitive Competitiveness

by **James Carlini**

The next battle won't be fought on battlefields. It'll be waged in newsfeeds.

James Carlini, 2025[1]

This article discusses the need for a modernized educational framework for military personnel to address the evolving demands of 21st-century warfare, particularly in the cognitive and electronic domains. It emphasizes the necessity for a diverse and advanced skill set beyond traditional training methods. It also examines the emerging importance of Cognitive Competitiveness (CC) and Cognitive Warfare (CW) and addresses why we need an urgent shift in military training priorities. This article illustrates several important issues:

- **Cognitive skill sets are essential:** The military must prepare recruits with advanced cognitive skills to navigate the complexities of modern warfare, where the battlefield increasingly involves information and technology.

- **Obsolescence of traditional education:** Current educational methods in public schools do not equip recruits with the necessary skills for contemporary challenges in cyber and electronic warfare.

- **Need for FACT-based skills:** Early integration of FACT-based skills—Flexibility, Adaptability, Creativity, and Technology—into curricula is vital to prepare students for future military and civilian careers. These are beyond the STEM skills currently discussed in public education.

- **Shift from Industrial Age education:** The educational focus must transition from outdated Industrial Age methods to more relevant skill sets that reflect today's technological landscape.

- **Influence on public education is necessary:** The military should take a proactive role in shaping public school education to ensure that recruits possess the relevant skills needed in modern warfare.

- **Emerging technologies in warfare:** Future military operations will increasingly rely on advanced technologies, including AI and robotics, necessitating a workforce trained in these areas.

- **Cognitive Competitiveness and cognitive warfare are new frontiers:** Cognitive Competitiveness will be a requirement in a new AI-based economy and future. Cognitive warfare represents a significant threat, requiring military personnel to develop skills to counter misinformation and propaganda effectively.

- **Importance of early skill development:** Establishing educational programs in public schools focused on technology and cognitive skills at an early age can create a more capable military workforce, ready to tackle the complexities of modern combat. This could be a dual-purpose program enhancing skills for both military and industrial benefit.

This article underscores the significance of acquiring cognitive skills for modern electronic warfare, asserting that understanding and adapting to new technologies is crucial. The article highlights the obsolescence of traditional skills acquired in public schools by recruits, which do not align with the rigorous demands of today's emerging military fields, such as in cyber warfare and electronic warfare.

It advocates advanced training that extends beyond basic weapon handling to include managing and administering complex systems for counterintelligence and software development, necessitating a stronger foundational education. This "foundational education" should be developed over a long period. The skills needed go far beyond what was necessary 50 years ago and this article suggests that taking a more active role in influencing public school education at the middle school and secondary education level may prove to be beneficial.

The U.S. government must understand the level of education of its current military recruits. Many have

obsolete skill sets for emerging cyber technologies, and electronic and Cognitive Warfare. Few recruits have possession of the needed skills and expertise on their day of enlistment.

Instructors can teach a recruit how to fire a rifle or a mortar in a short period, but they need a much better secondary educational foundation across many cognitive and technical skill sets. New recruits must have foundational skills that can enable them operate to complex electronic weapons platforms; develop and analyze real-time software; administer complex technological systems for both intelligence gathering and counter-intelligence; and to initiate and counter cyberattacks.

Going a step further, in the area of Cognitive Warfare, we must military personnel who can see past disinformation and be cynical of the greater volume of propaganda coming out on social media platforms as well as opinion-bending information readily available and greatly seeded into those platforms as well as other forms of media today. Some of this could be accomplished using artificial intelligence (AI) applications, but we still need a seasoned cadre of people to develop, maintain, and augment these AI programs.

BEYOND STEM SKILLS TO MASTER TOMORROW'S WEAPONS PLATFORMS

In 21st-century warfare, the weapons used will range from traditional weapons platforms to electronic and cyber AI-enabled weapons as well as systems that use other emerging technologies. Will we be immersed in metaverse applications as well? This 3D virtual area is emerging in asymmetric warfare but has not yet gained significant traction.[2] Still, this new platform should be analyzed as to what military value it may have and the likely security vulnerabilities it creates in both traditional and electronic data gathering.[3]

We are no longer in the Industrial Age; the skill sets that were developed and taught in public schools focused on getting students a very basic foundation in skills needed for factory jobs. Students typically focused on the Three Rs: rote, repetition, and routine along with regimentation.[4] We are well beyond the Industrial Age. We need to ensure that new skills are taught to public school students at a much earlier age if we are to have a future pool of qualified recruits to draw from.

Many writers have argued that public school education must focus more on STEM-related topics, such as science, technology, engineering, and mathematics; nonetheless, we are even beyond that requirement now. Do we want military leaders to have some say in the curriculum used in public school education? This is a relatively new issue, but the investment of influence might be worthwhile as these new cognitive skills require time and effort to acquire.

The current approach to public schools is not working; we need a radical shift in what subjects and skill sets should be taught. Since the 2020 COVID pandemic, we have failed to bounce back to earlier scores in math, science, and reading comprehension.[5] In addition, we need to concentrate on skill sets like Cognitive Competitiveness, to function in a 21st century global environment. For example, in 2021, NATO hosted a conference that featured a panel on Cognitive Warfare; the panelists acknowledged that it was a new field that they did not know much about it and were looking for "experts in the field."[6]

We need a new approach. First, I argue that "there are no experts in this field as it is still emerging and very dynamic." The best one can now be is a good student, always learning. Now is the time to learn and develop a broad perspective—but not by proclaiming yourself an expert. Second, best practices change with the proverbial weather. What was important last year could be different and obsolete this year. The NATO leaders who are seeking: "experts" and "best practices" are looking for something that does not exist—not yet anyway. There is a lot to learn and what we should be looking for is people who are creative, innovative, and not locked into one perspective or one direction. Cognitive Warfare needs to be built on a foundation of strong Cognitive Competitiveness. That foundation should include people who have FACT-based skills. Third, we still need a framework to define the parameters and explicit specifications for Cognitive Warfare's concepts.[7]

NEW FACT-BASED SKILLS MUST BE INTEGRATED EARLY

New skill sets must be integrated into education at an early age. Skills to be successful today in complex technological fields include those that can be defined as FACT-based skills. FACT-based skills include Flexibility, Adaptability, Creativity, and Technology skills.[8] See Chart 1.

Many colleges and universities are not preparing students for today's multi-tasking, multi-disciplinary focus. In many cases, higher education has not really changed its formula for management and real estate education in 30+

Skill Set	Reason
Flexibility	Learning skills today does not set one up for a lifelong career. Lifelong continual learning and learning how to be flexible are critical.
Adaptability	Jobs are not "routine" anymore. Things change and the worker needs to adapt and assimilate to sometimes constantly changing conditions.
Creativity	How does one attack a problem? Solutions evolve as challenges change. Creative people are needed for innovation as well as defining alternatives for dynamically changing environments.
Technology	Every industry has been touched by computerization. Computer skills have become "basic skills" one must have in order to be viable in the workforce.

Chart 1 - Fact-Based Skill Sets[20]
(Keys to getting beyond Minimum-wage jobs)

years and yet the workplace, technology, infrastructure, and the global marketplace have changed substantially in 30 years across those fields.

We should also be looking at some of our adversaries as to what they are doing to develop key skills in this area. Complex systems require complex skill sets to manage and operate them to their maximum potential. SILO degrees (focusing on a single area or disciple) must be replaced by multi-disciplinary degrees covering two to four areas. See Chart 2**.**

Fifty years ago, many students graduated from college with a degree with a single focus, a single discipline (like accounting, biology, or mathematics). For the most part, they still do. Today, however, most projects and complex jobs require a more broad-based approach and understanding across several disciplines. A background in multi-disciplinary areas is preferred. Most universities have not changed their degree program curricula in fifty years. Talk to most universities about Cognitive Competitiveness in various environments across many disciplines and they would be overwhelmed.

Chart 2:
Traditional Skills vs. New Multi-Disciplinary Skills[9]

Traditional Skill (Single Skill, in four persons)

Real Estate	Infrastructure	Technology	Buildings/Facilities

Multi-Disciplinary Skills (In One Person)

Real Estate
Infrastructure
Technology
Buildings/ Facilities

Today's public school students should focus on acquiring **FACT**-based skill sets. This is what is needed by young adults in order to compete successfully in today's and tomorrow's job markets. The military must compete with that job market if it is to recruit skilled individuals.

Weapons platforms as well as other military techniques and requirements are not getting simpler; they are getting more complex. They are also getting more technology-based, in both traditional as well as electronic warfare, which requires more than a basic understanding of technology. The jobs of today, as well as tomorrow, must be filled with people who possess a whole new set of flexible, adaptable, and creative skills using technologies, to be successful and forge real career paths.[10] Industrial-age educational approaches and solutions must be abandoned. Not every job will be automated. Skilled workers at every level will still be needed.

Military leaders should consider whether they should influence what is included in the 21st century public school curriculum; this could be a very important military investment to ensuring a strong generation of ready-to-serve warriors who understand the new nuances of the 21st century battlefield. This battlefield will be more

technology-driven in the traditional sense as well as in the new dimension of electronic cyberwarfare which is expanding geometrically on an annual basis.

ADDING A NEW INSTITUTE FOR LEARNING IN PUBLIC SCHOOLS

Just as the ROTC program in secondary schools has been a good feeder system for future military recruits, it might be time to re-evaluate that mission and develop a new endeavor to create some type of new Learning Institute? The Institute's role in developing foundational and critical skills at an early age for all these emerging areas like drones, robotics, AI, and other electronic surveillance careers would be an asset to education. Students would acquire and master skills in these new areas through participation within the Institute.

The idea of having a course of study or a series of courses in some type of institute promoting these new emerging technologies could be a new area to become involved in at the secondary school, or even the middle school level. This approach would begin to develop students with skills which could translate into good careers both in the military and corporate sectors.

A restaurant server in Wisconsin told me about her sixth-grade daughter involved in a robotics class at school. She said she was learning a lot and developing a robot to compete at state-level. This type of technical education being initiated at that level is what the military needs to actively promote across the country with some type of focus on gaining skills in these emerging technologies. Otherwise, where are you going to get recruits who can quickly assimilate and be productive in electronic warfare, including Cognitive Warfare?

Just think of the level of expertise someone who was involved in a program like this since middle school would walk in with at the age of eighteen. It is the equivalent of getting a musician into a military band. You expect them to come in with a certain level of awareness, proficiency and expertise, but that takes time. That proficiency does not come overnight, let alone in eight weeks. It is a long process.

Someone who has developed skills since the fifth grade will be more proficient and have a broader set of skills than someone who started in high school. Developing a solid foundation in some of these new and emerging electronic technologies cannot be started in the first year of enlistment. It's too late. If a foundation of skills were introduced at a middle school level and then enhanced by state and regional competitions at both middle school and high school levels, we could develop team dynamics, as well as showcase ideas and innovations, and the military would be a huge beneficiary. Much more advanced and classified expertise could be immediately added to a person's expertise at an early age. See Chart 3.

Something like this must be initiated quickly because our traditional public school teaching is now missing the mark. So many high school graduates are not walking out with basic mathematics and reading skills at the high school level, let alone the basic FACT-based skills mentioned above. (The same applies to STEM-related skills)

We cannot apply 20th century skill sets to solve 21st century challenges. Acquiring new skill sets for personnel is just as important as acquiring new weapons platforms and new supporting technologies. Just as hardware becomes obsolete, so do the skill sets of leaders and technical personnel. The skills must be renewed and updated to remain cutting-edge.

Chart 3:
Supplemental Institute for Acquiring Technology Skills

Grade	Course Levels	General Skills Addressed
Middle School	Introductory Overview (Drones, Robotics, or AI)	Basic skill sets; learning definitions, basic concepts, and basic applications. Small group projects.
High School	Intermediate/ Advanced (Select One or Two Specialties to Pursue)	Working on prototypes or working models. Doing more competitive activities. Working individually and in small groups.
College	Advanced II (Focus on one Specialty)	Working on more hands-on projects and creative innovation within the discipline. Actually developing tools and perfecting their use.

In business, whoever has the best-trained workforce is the toughest competitor. In warfare, whoever has the best-trained military is the toughest competitor and most likely, the ultimate victor.[11]

PREPARING FOR COGNITIVE WARFARE

New cognitive skill sets are also needed long before getting to a military age. Should the military be more supportive of public school initiatives? It could not hurt, especially if the Department of Education gets unraveled. The Department of Defense should be able to address some of the gaps by demanding the addition of critical curricula to ensure the development of a qualified group of individuals for future recruitment requirements.

If the next battlefield is the brain, what are we doing with our future generations to prepare them for this type of warfare and to be able to adequately defend themselves from this new, emerging form of electronic warfare?

Cognitive Warfare is already being used to shift our focus to destabilize our democracy. A current example is TikTok which is very questionable application as to its advantages compared to the information-gathering aspects it possesses for the Chinese Government. Other initiatives are being developed by Russia as well as Israel.

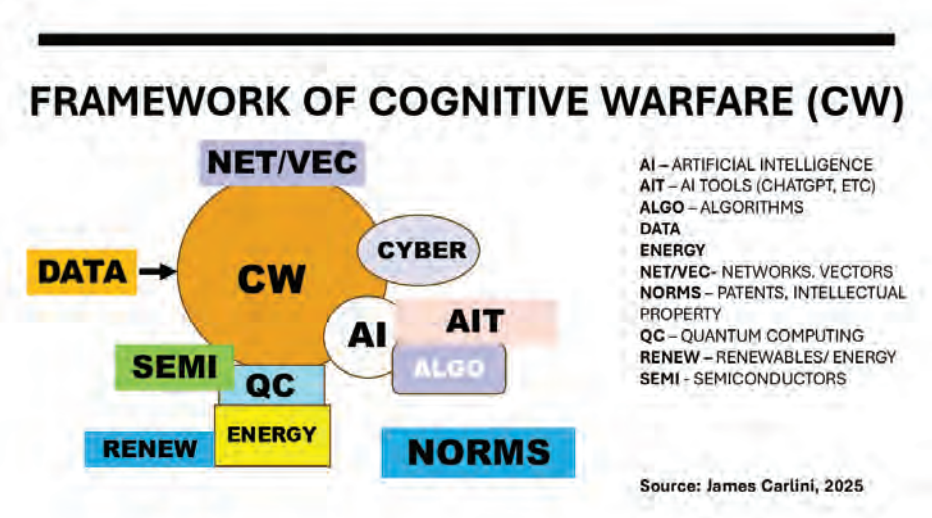
> "Influencing and manipulating public opinion are full-fledged modes of action for powers aiming to destabilize our democracies."
>
> General Eric Autellet, the French Armed Forces Deputy Chief of Defense

A whole new area of electronic warfare is emerging. Cognitive Warfare (CW) is becoming a new tool for our major adversaries, like China and Russia, as well as other state acotrs like North Korea and Israel. It is also starting to be used by non-state terrorist groups as well who have no formal ties to a single sovereignty. Some of these non-state groups are also "for hire" and will contract out to various governments and agencies to perform various attacks.

Cognitive Warfare is a concept that is still evolving and crystallizing. It can be defined as: *"*The weaponization of public opinion by an external entity, for the purpose of influencing public and governmental policy, and destabilizing public institutions."[12] Chart 4 provides a visualization of the various components making up elements of a total CW framework. The CW Framework depicts all the working elements needed to build a CW Platform. From using the latest in AI and AI Tools (AIT) to establishing a sophisticated platform of quantum computing (QC) power and networks (NET/VEC), it is designed to take in data (DATA) and perform its magic in destabilizing beliefs and "winning the hearts and minds of the opposition."

Cognitive Warfare involves the use of key components of software, hardware, and other infrastructure that are combined to provide a new electronic weapons platform. If we look at the types of software CW will be using, we can see that their demand for power and processing will be huge. Faster and more complex semiconductors (SEMI) used in graphic processing chips, AI, and quantum computing (QC), will have a heavy demand for power and energy (ENERGY) as well as backup energy which could be delivered by types of renewable

Chart 4
CW Framework

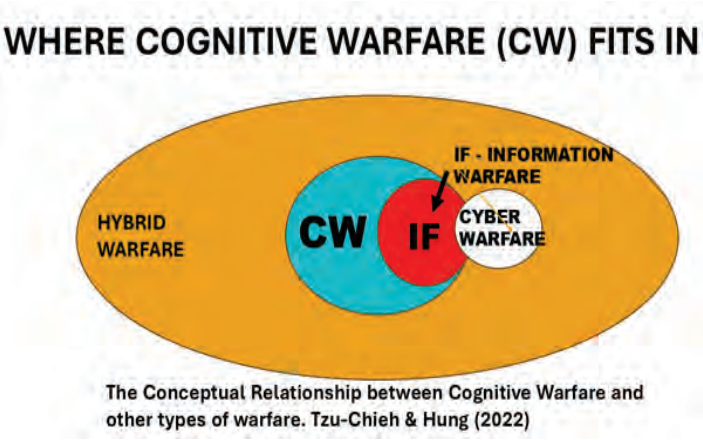


energy (RENEW). This emerging platform is focused on providing a sophisticated vehicle for attacking the mind of individuals as well as groups to break down beliefs, norms, and ideologies replacing them with new ideas.

The conceptual relationship between CW and other types of Asymmetric Warfare is depicted by the illustration created by Tzi-Chieh and Hung in 2022. It defines how CW brings together the components of hybrid warfare. See Chart 5. We must first identify a cyber threat as a form of as a Cognitive Warfare (CW) action; we can focus on creating an effective counterattack . The longer the lie or misinformation is left unchallenged, the harder it will be to counter and defeat it as it begins to become adopted and "accepted" by those who are vulnerable**.** See Chart 6.

Proportionality is a strategy for failure.[13] If three attacks are volleyed, you do not respond with three or even six counterattacks. You counter with a barrage of one hundred or one thousand) You want to squelch the misinformation as quickly as possible and squelch the source(s). On the other hand, when it comes to responding to misinformation or disinformation targeted to the mind, the responses must be quick to "counter the "spin, before it gets in." The faster someone reads a counter to the propaganda, the more likely they will discount it. The more it lingers without strong response, the more "accepted validity" will start to occur.

Chart 5
Tzi-Chieh & Hung (2022) CW in Hybrid Warfare



Does Cognitive Warfare impact the quality of Open Source Intelligence (OSINT)? The short answer to that question is yes. Many adversaries and allies have an interest in the emerging field of Cognitive Warfare (CW). According to Majors Andrew MacDonald and Ryan Ratcliffe, writing for the U.S. Naval Institute in its flagship Proceedings, "The United States is falling behind in confronting national security challenges at the intersection of technology and cognition. To catch up and address this emerging threat, the United States should develop and implement a concept that treats the cognitive dimension as offensive and defensive maneuver space."[14] Chart 7 illustrates the diversity of targeted individuals and groups across many different areas.

Chart 6
CW Attack and Counterattack Cycle

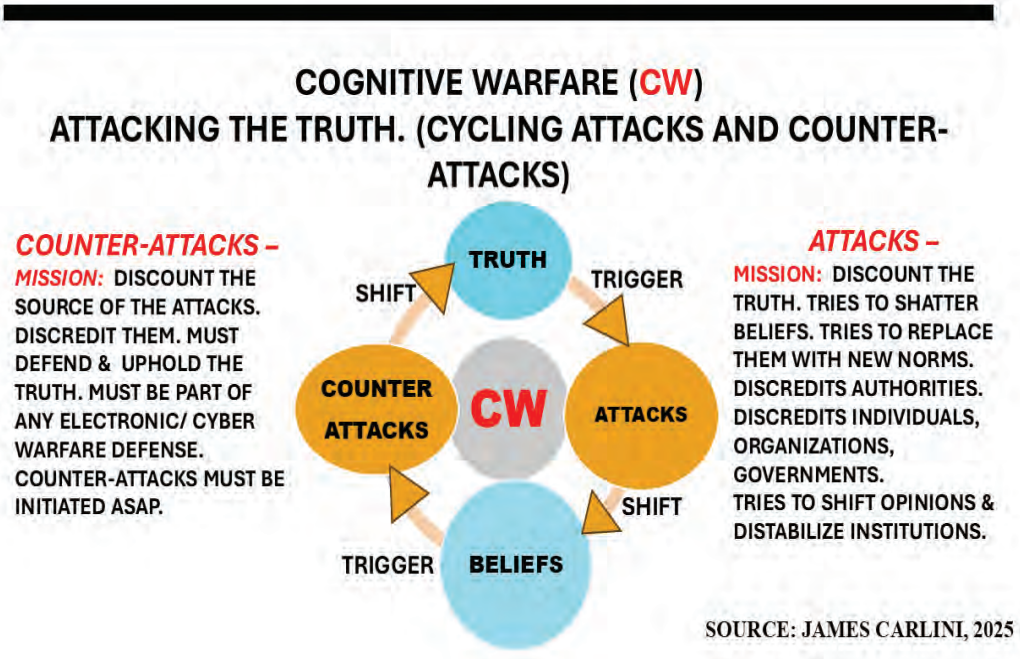


Chart 7
Examples of Cognitive Warfare Targets – Offense

Individual (Single, Or Multiple)	Group	Ideology/Ideologies
Billionaire/ Poor Person	Class (Poor, Rich)	Wealth, Capitalism, Classism
Celebrity (Actor, Radio, TV)	Media (Radio, TV, and Hollywood)	Various
CEO	Specific Company	Capitalism
CEO	Industry Sector (e.g., Energy, Automobile, Banks)	Capitalism, Environmentalism
Doctor(s)	Healthcare	Various
General, Admiral	Military	Various
Gun Owner	NRA	Conservatism
Newsperson(s)	Media	Various
Personality (Influencer)	Media, Social Media	Various
Politician(s)	Political Party/ Specific Country	Various (Capitalism, Communism. Socialism, Libertarianism)
Professor(s)	Academia	Various
Religious Figure(S) (Pope, Mullah)	Specific Religion	Various Religious Ideologies
School(s)	Academia	Various (Liberalism and Conservatism)
Sports Figure(s)	Team, Sport	Various
Taxpayer(s)	Citizens	Various
Women	Women	Feminism

Source: James Carlini, 2025

OSINT is defined as "the intelligence discipline that pertains to intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely matter to an appropriate audience to address a specific intelligence and information requirement."[15]

When it comes to disinformation from Cognitive Warfare initiatives, what is spread out to various social media platforms and other publicly accessible media, becomes questionable and would impact the quality of information collected by any type of OSINT application.

This new twist must be accounted for when we look at the accuracy and reliability of what is collected through the means of OSINT. We need to have people who are able to analyze the validity of data collected to extract only that information that is accurate and not massaged or manipulated to distort the truth.

THE IMPACT OF COGNITIVE WARFARE INTO THE FUTURE

In general, people are becoming more aware that "Cognitive Competitiveness" skills have important civilian applications across many industries. In fact, in military applications, this could also be a more effective means of defeating an enemy than traditional warfare. So, if the human brain is the new battlefield of the 2lst century, we must do everything we can to prepare the next generation to build a foundation of cognitive skill sets to ensure a fair playing field, both in military and civilian economic universes.

This is an area that the United States needs to get a better grasp of as more and more countries look at this as a new type of weapons platform that does not cost as much as a nuclear submarine or aircraft carrier but still can do a lot of damage in the area of Asymmetric Warfare within the electronic warfare area as well as on social media platforms.

We already see many arguments as someone puts up a meme that supports one political view or tears it down—and often with great intensity. This is why many countries with various political ideologies across the world are rethinking their "freedom of speech" across many social media platforms. Clearly, social media platforms have devolved into arenas of misinformation, hostility, and performative outrage.[16] And this problem is on the rise across many platforms from TikTok, to Facebook, and to Linked In.

Creating "cognitive confusion" to discredit institutions and unseat political individuals as well as parties can be a very effective weapon which we are just starting to see some of its abilities. TikTok is a good example, but what is the next TikTok and who will be using it to change behavior and influence beliefs?

All these arguments in heated discussions lead to a new weapon that is gaining traction with many countries and non-state terrorist groups. Indeed, as Chief Ten Bears commented to Josey Wales, "Your words have iron."[17] Words can "have iron" in them as more countries begin to use and defend against this new form of asymmetric warfare.

An example of verbal warfare between two people (or maybe one is a Bot?) might be when someone overstates their qualifications. That person might have two years of real work experience, but they claim to be experts. That person might want to discount the other person's experience immediately. That person might have worked on some small systems like wiring up a local area network for a coffee shop, but they build up their shallow expertise as if they have greater expertise and experience. Such a person confuses "tinkering" with mastery. A quick response to discount all they have claimed would be, "Just because you play with small Lionel trains in your basement, does not give you the skill sets to be the chief infrastructure engineer for the Burlington Northern."[18]

The putdowns go back and forth increasing in intensity sometimes. Other times, they give up. The absurdity of it often makes one wonder: Are we even debating a human or just arguing with a bot?

If we look at that argument and automate it with a slant on "Cognitive Warfare", we might increase the debate as well as the intensity in the character assassination. CW is a methodical effort to manipulate perceptions, sow distrust, destroy credibility, introduce new norms, and attempt to destroy unity. Foreign adversaries are already exploring its effectiveness and employing it. Their goal is to target Western societies via social media as well as more traditional media to destabilize nations, political parties, political leaders, classes (rich vs. poor), communities and fracture consensus.

Out of all these militaries listed below, who has any fraction of a force dedicated to Cognitive Warfare? Russia? The United Kingdom? The United States? See Chart 8.

Based on the invitation of NATO several years ago for anyone with any expertise to join their Mad Scientist Open Innovation initiative which the US ARMY was working on, it is not a huge universe of skilled people.[19] At this point, I would say the difference between an "Expert" and a novice is maybe one or two years of experience. No one has 20 years, everything is too new, and more importantly, still evolving.

Most countries are lucky if they have a well-equipped standing army ready for traditional warfare. When it comes to electronic warfare as well as Cognitive Warfare, most are sadly lacking. If they are sadly lacking, in this type of warfare, it would parallel the Polish coming out with a horse-mounted cavalry, to defend against an armored column of Blitzkrieg, if they were bombarded with a huge disinformation attack on any Social Media platform.

The United States, if it is to remain a superpower, must invest in building up people with these skill sets immediately and a person cannot be well-trained in any basic training program. Think proficiency of a musician walking into a military band. They just don't walk in and grab and instrument and play. Years of training, performances and application were added to them long before walking in. We need to start thinking the same way if we are to recruit productive people from day one within the emerging area of Cognitive Warfare.

Taking a bold initiative today to begin to equip students with Cognitive Competitiveness skills now in the public-school institution, will guarantee a solid universe of

Chart 8 - Traditional Military Strengths[21]

Country	Active Military Personnel	NATO Member
Russia	1,500,000	✗
U.S.	1,328,000	✓
Ukraine	880,000	✗
Turkey	355,200	✓
Poland	202,100	✓
France	200,000	✓
UK	184,860	✓
Germany	181,600	✓
Italy	165,500	✓
Greece	142,700	✓
Spain	133,282	✓
Romania	81,300	✓
Canada	68,000	✓
Hungary	41,600	✓
Netherlands	41,380	✓
Bulgaria	37,000	✓
Czechia	28,000	✓

candidates to recruit for these new Cognitive Warfare initiatives later. Developing some type of program to augment what they are learning from a basic curriculum is imperative. If you fail to act now, be ready to submit to adversaries who already see the impact this area can have on total government and economies.

Based on these numbers, NATO has a combined 3.44 million active military personnel, 2.11 million not including the United States.

NOTES

[1] James Carlini, "Social Media Platform Politics," March 31, 2025, https://intpolicydigest.org/the-platform/social-media-platform-politics/
[2] James Carlini, "Weaponizing Metaverse for Asymmetric Warfare," *American Intelligence Journal*, vol. 40, no. l (2023): 32.
[3] James Carlini, "Developing Skills for Open-Source Intelligence Operations," *American Intelligence Journal*, vol 39, No. l (2022): 35.
[4] James Carlini, "Why Johnny Isn't Ready to Take on Today's Jobs: The Need for FACT-Based Skill Sets," George Mason University, Center for Infrastructure Protection & Homeland Security, 2015, https://cip.gmu.edu/2015/11/12/why-johnny-isnt-ready-to-take-on-todays-jobs-the-need-for-fact-based-skill-sets/
[5] Ray Dominaco, "The Nation's Report Card Should Trigger Alarm Bells," February 17, 2025, https://www.city-journal.org/article/national-assessment-of-educational-progress-results-student-reading-scores.
[6] The NATO Innovation Online Conference, November 9, 2021, https://www.youtube.com/watch?v=xrnjcCgO19I
[7] Jake Bebber, "China is waging cognitive warfare. Fighting back starts by defining it," March 19, 2025, https://www.defenseone.com/ideas/2025/03/china-waging-cognitive-warfare-fighting-back-starts-defining-it/403886/?oref=d1-category-lander-river.
[8] James Carlini, "Why Johnny Isn't Ready to Take on Today's Jobs: The Need for FACT-Based Skill Sets," George Mason University, Center for Infrastructure Protection & Homeland Security, 2015, https://cip.gmu.edu/2015/11/12/why-johnny-isnt-ready-to-take-on-todays-jobs-the-need-for-fact-based-skill-sets/
[9] James Carlini, *Location Location Connectivity* (self-published, 2014).
[10] James Carlini, "From Our Partners – Why Johnny Isn't Ready to Take on Today's Jobs: The Need for FACT-Based Skill Sets," Center for Infrastructure Protection & Homeland Security, George Mason University, 2015, https://cip.gmu.edu/2015/11/12/why-johnny-isnt-ready-to-take-on-todays-jobs-the-need-for-fact-based-skill-sets/
[11] James Carlini, "The Application of Artificial Intelligence to Asymmetric Warfare: Not a Silver Bullet," *American Intelligence Journal*, vol. 37, no. 2 (2020): 32.
[12] Cognitive Warfare: The Forgotten War with Tanguy Struye de Swielande 2024 https://www.youtube.com/watch?v=dMSDL02yDag
[13] James Carlini, "Asymmetric Warfare Just Around the Corner: Domestic Terrorism," *American Intelligence Journal*, vol 41, no. 1 (2024): 88.
[14] Majors Andrew MacDonald and Ryan Ratcliffe, "Cognitive Warfare: Maneuvering in the Human Dimension," *Proceedings*, April 2023, vol. 149/4/1, 442. https://www.usni.org/magazines/proceedings/2023/april/cognitive-warfare-maneuvering-human-dimension.
[15] U.S. Army, *Open-Source Intelligence*, Army Techniques Publication No. 2-29 (Washington, DC: Department of the Army, 2012), 1-1.
[16] James Carlini, "Social Media Platform Politics," March 31, 2025, https://intpolicydigest.org/the-platform/social-media-platform-politics/.
[17] "The Outlaw Josey Wales" Scene where Josey Wales meets Ten Bears," Movie, 1976, https://www.youtube.com/watch?v=eyPZFi2b380.
[18] James Carlini, "Social Media Platform Politics," March 31, 2025, https://intpolicydigest.org/the-platform/social-media-platform-politics/.
[19] The NATO Innovation Online Conference, November 9, 2021, https://www.youtube.com/watch?v=xrnjcCgO19I; see also Cognitive Warfare Concept (NATO) Video (2024), https://www.youtube.com/watch?v=lnP8w2bpixo
[20] James Carlini, *Location Location Connectivity* (self-published, 2014).
[21] The data used are 2024 NATO estimates sourced from Statista and United24.

James Carlini is a visionary and strategist for mission-critical networks, technology, and intelligent infrastructure. He has been president of his own consulting and research firm since 1986. Jim has written frequently for the American Intelligence Journal. He served in the Air National Guard and the U.S. Army Reserve from 1972 to 1985.

BRIDGING THEORY AND PRACTICE IN OSINT: A COMPARATIVE BOOK REVIEW FOR INTELLIGENCE EDUCATION AND PROFESSIONAL DEVELOPMENT

Reviewed by Jessica Stutzman

Michael Bazzell's and Jason Edison's *OSINT Techniques: Resources for Uncovering Online Information*
and
Rae Baker's *Deep Dive: Exploring the Real-World Value of Open Source Intelligence*.

The Intelligence Community (IC) faces surging volumes of publicly accessible information, increasing the need for robust training and professional development in Open-Source Intelligence (OSINT). As digital platforms proliferate and adversaries refine their tactics, OSINT practitioners must be capable of gathering, scrutinizing, and interpreting online information with speed and precision. In recent years, some of the most innovative OSINT techniques have emerged not from government experimentation but from private-sector breakthroughs, revealing a rich exchange of ideas that benefits both realms. Industries ranging from cybersecurity to corporate due diligence have pioneered flexible, tech-savvy methods that can elevate the IC's own OSINT practices.

A comparative review of Rae Baker's *Deep Dive* (2023)1 and Michael Bazzell's *OSINT Techniques* (11th ed, 2024)[2] demonstrates how private-sector expertise can sharpen government intelligence tradecraft, bridging traditional methodologies with cutting-edge developments. Their distinct backgrounds, achievements, and perspectives highlight how OSINT can unite conceptual depth and real-world tactics—an approach poised to benefit the entire IC. Understanding the authors themselves, as well as the pedagogical and operational philosophies informing their work, offers further insight into why these texts deserve attention from practitioners seeking to stay ahead in an increasingly complex digital landscape.

BACKGROUND AND AUTHOR PERSPECTIVES

Rae Baker draws from extensive experience in cybersecurity, digital investigations, and intelligence analysis, combining experience from private and government-adjacent roles. Her work underscores the "human side" of intelligence by addressing analytical bias, burnout, and the cognitive foundations of effective OSINT. Earning certifications such as Associate of ISC2 (CISSP), SANS GOSI, and AWS Solutions Architect, as well as top placements in Trace Labs OSINT Capture the Flag competitions, she demonstrates both technical and conceptual mastery. Baker's focus on reflective, ethics-conscious tradecraft holds particular value for IC professionals looking to build resilient, critically minded analysts through long-term development programs.

Michael Bazzell is renowned for his expertise in tactical OSINT and operational privacy. He spent over two decades in cyber investigations, much of it with the FBI. After transitioning to the private sector, he established the IntelTechniques platform and developed a suite of OSINT tools, virtual labs, and training modules. Known for highly pragmatic, case-driven instruction, Bazzell emphasizes investigator security and real-world demands—an approach that aligns well with agencies seeking rapid onboarding and immediate tactical proficiency. His breadth of experience in both federal and private arenas makes him a leading authority on streamlined investigative workflows and effective online methodologies.

Although these two authors emerge from distinct professional backgrounds, their works share a common impetus: equipping OSINT practitioners with reliable, effective approaches to digital investigations. Baker's conceptual lens centers on the interplay between the intelligence cycle and critical thinking, while Bazzell's more tactical orientation speaks to immediate investigative needs and real-time operational concerns. Examining each book's structure and pedagogical style reveals why both are indispensable, depending on a reader's goals, organizational setting, and readiness to embrace OSINT's evolving demands.

RAE BAKER'S *DEEP DIVE*

Rae Baker's *Deep Dive* (2023) emphasizes a rigorous theoretical framework for OSINT, urging OSINT practitioners to approach open-source research as part of a broader intelligence discipline rather than a mere collection of tools and websites. She underscores that every OSINT inquiry must serve a specific investigative aim, which strengthens critical thinking and ensures high ethical standards.

Baker organizes *Deep Dive* into three distinct sections: foundational theory, domain-specific applications, and forward-looking guidance. In Part I, she lays out the conceptual bedrock for effective OSINT, placing it firmly within the intelligence cycle and drawing attention to human-centric factors such as bias, burnout, and mental resilience. Part II maps these theoretical principles to diverse "touchpoints," including social media analysis, business intelligence, and transportation tracking. Each chapter acts as a standalone module, complete with terminology, methodologies, and case-based scenarios, making the text exceptionally adaptable to structured courses or agency-level curricula. These discrete modules allow readers to focus on areas most relevant to their investigative context, strengthening both conceptual grounding and practical application. The final portion of the book shifts the focus to emerging investigative frontiers, ensuring the material stays relevant as technology and threat landscapes evolve.

From an educational standpoint, this modular design aligns with the professional training goals of the IC. Rather than settling for superficial tool demonstrations, instructors can adopt *Deep Dive*'s step-by-step chapters to define specific learning outcomes, such as social media exploitation or business reconnaissance, and embed both conceptual frameworks and real-life examples. This approach encourages learners to develop not only procedural knowledge but also a deeper understanding of OSINT's strategic implications.

A central strength of *Deep Dive* lies in Baker's commitment to critical thinking over rote tool usage. Citing frameworks like David T. Moore's adaptation of the Paul-Elder model3, she consistently pushes readers to question assumptions and clarify investigative objectives. This mindset is particularly beneficial in fast-evolving digital environments, where platform updates or emerging technologies can quickly render static techniques obsolete. By reinforcing the "why" behind each step of the intelligence cycle, Baker ensures that analysts maintain a degree of methodological rigor and adaptability.

Baker highlights ethical considerations, including mental health, privacy rights, and checking personal biases. This focus stands out in a field often dominated by purely tactical guides. She positions OSINT as an inherently human-driven process that demands cognitive awareness and a commitment to objectivity. Although *Deep Dive* covers domains ranging from subject identification to business intelligence, it never loses sight of shaping analysts who understand the ethical and intellectual imperatives of OSINT.

Because *Deep Dive* covers a broad spectrum of intelligence workflows and advanced topics, including cryptocurrency, non-fungible tokens (NFTs), and geospatial tracking, some readers may initially feel overwhelmed. Those new to OSINT or lacking a basic grounding in intelligence methodologies might want more explicit, step-by-step instructions. However, Baker's relatively tool-agnostic approach ultimately fosters a more enduring skill set, focusing on overarching principles and readiness for continuous change. She lays the groundwork for adaptability across changing platforms and organizational standards by encouraging analysts to focus on overarching principles rather than technical knowledge.

From a professional development standpoint, this breadth can be a significant advantage. *Deep Dive* cultivates foundational adaptability, which the IC increasingly values as it faces evolving challenges. Agencies committed to building practitioners who thrive beyond initial training will find that Baker's strategic emphasis and ethical depth create an intellectual framework for sustainable growth. For entry-level and intermediate practitioners, *Deep Dive* serves as a robust roadmap when paired with hands-on labs, mentorship, or supplementary technical references. This conceptual grounding sets the stage for more tactical approaches, such as those found in Michael Bazzell's latest publication.

MICHAEL BAZZELL'S *OSINT TECHNIQUES* (11TH EDITION)

Michael Bazzell's *OSINT Techniques* (11th ed.) maintains a thoroughly tactical orientation, continually updating its content to keep pace with changing online environments and investigative needs. Building on the four-part structure introduced in earlier editions, this release broadens its scope to address emerging cyber threats such as ransomware data dumps and stealer logs, reflecting the evolving nature of open-source research.

At the heart of *OSINT Techniques* lies a clear commitment to practical, step-by-step instruction. *Section I: OSINT Preparation* helps readers establish a secure investigative environment by covering operational security (OPSEC) concepts. Early chapters focus on optimizing computer setups, isolating investigative activities within dedicated virtual machines (VMs), and employing browser configurations that safeguard the user's identity. Here, Bazzell underscores that even the most skilled analyst remains vulnerable without appropriate OPSEC: any slip-up can compromise ongoing investigations or expose personal data.

Section II: OSINT Resources & Techniques forms the central backbone of the text. Drawing on over two decades of online investigative work, much of it with the FBI's Cyber Crimes Task Force, Bazzell details a range of methods for collecting and analyzing information on email addresses, usernames, social networks, domain names, and more. Each chapter is organized into a lab-like module replete with annotated screenshots,

flowcharts, and, in some cases, free, customizable scripts that automate repetitive tasks. For instance, readers can access "custom search tools" from the IntelTechniques website to perform simultaneous queries across multiple sites or quickly pivot between different data sources. This arrangement makes the book particularly valuable for high-tempo agencies, private-sector threat intelligence teams, and independent investigators seeking immediate operational results.

In addition to social media exploitation and online communities, *Section II* also dives into lesser-known resources—like historical archives, advanced search operators, and people search engines—to help analysts identify obscure connections. Bazzell consistently revisits the importance of verifying each lead and warns of the ephemeral nature of online platforms: a website or social media profile might vanish or relocate overnight. The book remains a living roadmap rather than a static reference manual by emphasizing agility and a willingness to pivot when a given site or tool becomes obsolete.

Section III: Leaks, Breaches, Logs, & Ransomware is a standout addition in the 11th edition, expanding on what was once a single chapter about data breaches in previous versions. Bazzell offers in-depth tutorials for searching stealer logs, navigating major breach repositories, and handling ethically charged or legally problematic sets of compromised data. He highlights real-world scenarios where ransomware groups post sensitive information to hidden onion sites, cautioning practitioners to remain fully aware of both the legal ramifications and personal security risks of investigating such data troves. The text guides readers through advanced tactics for harvesting insights from stolen records by providing specific command-line examples and offering program recommendations, while grounding efforts in operational security best practices.

Section IV: OSINT Methodology then ties everything together into a repeatable workflow. Readers learn to merge technical expertise with structured notetaking, link analysis, and professional case reporting techniques. Bazzell offers practical suggestions such as using a digital "scratch page" or employing visual mapping tools for link analysis to keep investigations organized and transparent. He also addresses policy and ethics, advocating that each agency or organization develop guidelines (which should be reviewed by legal counsel) to govern the acquisition, storage, and use of sensitive information discovered online.

One defining characteristic of *OSINT Techniques* is its explicit assumption that readers possess at least a moderate level of technical literacy. Chapters on Linux-based VMs, command-line tools, and custom scripts can overwhelm those who are new to computer forensics or come from a purely theoretical intelligence background. Without some foundational knowledge, new analysts risk treating the text as a "checklist" of tactics, lacking deeper insight into why certain methods work in specific contexts. Bazzell acknowledges this gap by advising readers to skip overly technical sections and revisit them later; however, agencies adopting this book for training should consider supplementing it with mentorship or entry-level labs that reinforce the strategic rationale behind each tool.

Still, for law enforcement groups, government agencies, and corporate security teams well-versed in information technology, *OSINT Techniques* stands out as a gold-standard manual. Readers benefit not only from Bazzell's wealth of real-world investigative examples—spanning missing persons, online child solicitation, cyber intrusions, and terrorism cases—but also from the companion IntelTechniques website, which offers frequent updates and corrections as internet platforms evolve. The result is a text that encourages continuous learning and adaptation, aligning perfectly with the high-velocity demands of modern intelligence work.

Bazzell's pragmatic, case-driven style resonates with trainers who orient new analysts to their duties quickly and reliably. His hands-on focus, fortified by custom scripts and detailed flowcharts, ensures that *OSINT Techniques* functions as a living, dynamic toolkit rather than a static resource. His methodology complements Rae Baker's conceptual emphasis, creating a holistic OSINT ecosystem when applied together.

CONTRASTING METHODOLOGIES FOR HOLISTIC OSINT MASTERY

Deep Dive and *OSINT Techniques* offer complementary approaches that, when combined, yield a more comprehensive range of investigative skills. *Deep Dive* highlights conceptual elements of OSINT and urges analysts to develop critical thinking, ethical judgment, and resilience. Baker introduces perspectives on mental health, cognitive biases, and structured analysis, all of which help practitioners adapt to shifting technologies and mission priorities. Her emphasis on understanding the "why" behind each procedure, along with a modular format aligned with structured training, sets a solid foundation for long-term professional growth. However, *Deep Dive* occasionally lacks granular instructions for beginners, and its scope may overwhelm readers without mentorship or lab-based exercises.

OSINT Techniques pursues a practical, tool-focused strategy that delivers step-by-step tutorials, annotated screenshots, and customizable scripts. Bazzell covers a wide spectrum of topics, including virtual machine setup and advanced search operators, offering immediate operational benefits for agencies handling high-velocity investigations. This approach demands basic technical fluency and sometimes prompts new analysts to rely too

heavily on scripts. Despite that limitation, the text acts as an indispensable field manual for investigators with solid OPSEC experience, and frequent IntelTechniques updates keep the content current.

A fundamental distinction emerges in how each author balances methodology and technology. Baker encourages readers to question assumptions and refine investigative objectives before selecting tools, while Bazzell provides a ready-made catalog of technical resources that he continually updates. An IC training pipeline that merges these strategies can produce analysts who blend reflective, ethical reasoning with proficient real-world execution. Students reinforce their sense of purpose and analytical discipline under Baker's framework, then advance to Bazzell's detailed, operationally driven tutorials.

This dual strategy prevents practitioners from adopting an overly academic mindset or relying too heavily on automation. Baker's conceptual depth offers the foundational knowledge and intellectual infrastructure necessary for long-term flexibility, while Bazzell's extensive resource pool allows analysts to address evolving platforms, data sources, and threats rapidly. Together, these methodologies address the full scope of today's intelligence challenges, equipping OSINT practitioners to excel at both strategic assessment and on-the-ground investigation.

TARGET AUDIENCES AND RECOMMENDATIONS

Deep Dive provides analytical depth for academic institutions, government agencies, and private-sector organizations seeking to nurture a deeply rooted analytical mindset. Instructors, policy-oriented analysts, and practitioners will appreciate Baker's emphasis on ethics, bias mitigation, and personal resilience, which resonates with the complex human factors at play in intelligence work. Although newcomers to OSINT may need additional guidance, the book's modular chapters and extensive coverage of multiple OSINT domains make it an exceptional choice for holistic training programs.

OSINT Techniques provides tactical proficiency (a hands-on approach) that benefits self-driven practitioners, technical professionals, and high-velocity operational units. Readers looking for clear, step-by-step instructions and immediate applicability will benefit most, especially those in law enforcement, the IC, or cyber threat intelligence aiming to shorten the onboarding process for new investigators. Given its emphasis on scripts, virtual labs, and platform-specific tactics, the text remains unsurpassed in tactical and technical depth. However, it assumes a certain level of IT proficiency, which may present challenges for those without the necessary technical background.

Both *Deep Dive* and *OSINT Techniques* lend themselves to IC certification tracks and structured continuing education programs. Baker's modules can serve as a conceptual foundation for advanced analyst certifications, while Bazzell's systematic exercises provide tangible checkpoints for skill validation. Together, they enable teams to measure progress in a testable, objective format and align their training pathways with the growing demands of modern OSINT.

INTEGRATING BOTH WORKS FOR COMPREHENSIVE OSINT DEVELOPMENT

A possible drawback in relying on either book in isolation is the risk of imbalance. Practitioners who dive into purely strategic analysis without hands-on fluency may develop an overly theoretical mindset, while a tool-centric approach can drift into a "checklist" mentality that ignores deeper ethical and methodological considerations. Because open-source data is becoming more pervasive, and adversaries increasingly adept at deception or denial strategies, OSINT professionals ultimately need both conceptual mastery and tactical skill.

Despite each text's inherent value, they function most effectively when integrated into a comprehensive OSINT development strategy. Baker's method-centric perspective illuminates the conceptual "why," ensuring that investigators remain adaptable, ethically grounded, and critically engaged. Bazzell's highly practical focus on the "how" streamlines investigative tasks, equipping analysts to respond swiftly to leads or data exposures. By combining these two approaches, organizations can produce analysts who not only master scripts and platforms but also understand the broader implications of their findings.

In the IC, law enforcement, cybersecurity, and private investigations realms, where mission requirements and resource constraints vary widely, this complementary integration proves particularly relevant. Agencies that rely exclusively on Baker's conceptual frameworks without practical experience in tool usage may encounter difficulties in day-to-day investigative workflows. Conversely, programs that fixate on Bazzell's recommended scripts and specialized platforms could neglect the ethical, methodological, and human dimensions Baker elucidates. Balancing these viewpoints helps forge a new generation of OSINT professionals prepared to face the uncertain and rapidly shifting demands of digital intelligence.

BUILDING THE NEXT GENERATION OF OSINT PROFESSIONALS

Ultimately, *Deep Dive* and *OSINT Techniques* function as complementary resources that together offer a comprehensive foundation for OSINT professionals. Baker focuses on conceptual and ethical frameworks, shaping strategic, adaptable OSINT practitioners; Bazzell concentrates on practical, evolving tool-

sets for real-time digital investigations. Whether you are an educator or an operational leader, these books do more than provide insight—they outline a clear path to cultivating a workforce that is resilient, forward-thinking, and ready to navigate an increasingly complex intelligence environment.

Positioning these works at the core of OSINT education helps the IC develop a new generation of practitioners who excel in strategic thinking and precise execution. In practical terms, this entails building training and recertification programs centered on ethical awareness, analytical rigor, and actionable investigative skills—traits that keep intelligence professionals effective in a fast-evolving digital landscape. By integrating the strengths of each author's approach, the IC lays the groundwork for an adaptive, future-ready intelligence workforce capable of meeting the demands of modern OSINT. When instructors and operational leaders integrate these methods cohesively, they create a robust framework that addresses the full lifecycle of digital investigations.

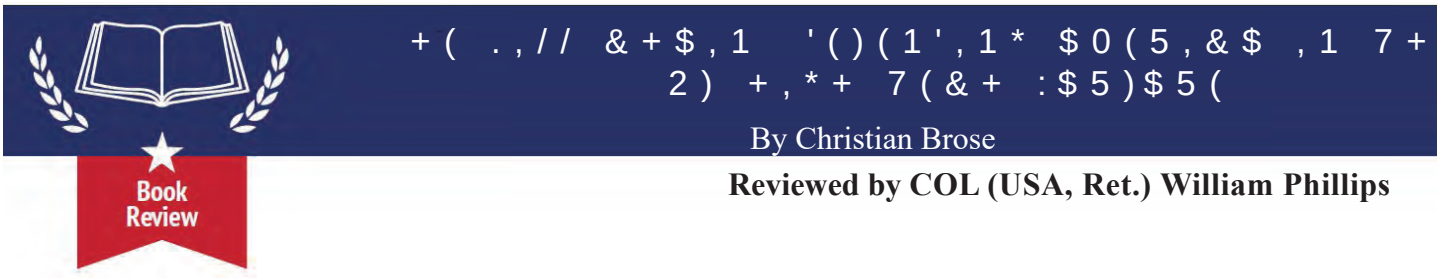
NOTES

[1] Rae Baker, *Deep Dive: Exploring the Real-World Value of Open Source Intelligence* (Indianapolis: John Wiley and Sons, 2023).

[2] Michael Bazzell and Jason Edison, *OSINT Techniques: Resources for Uncovering Online Information* (self-published, 2024).

[3] D.T. Moore, *Critical Thinking and Intelligence Analysis* (Washington, DC: Joint Military Intelligence College, 2006), 27-76.

Jessica Stutzman is an Open-Source Intelligence (OSINT) practitioner and doctoral student at American Military University, specializing in strategic intelligence. She brings over 15 years of experience supporting the U.S. Intelligence Community as a contractor and consultant, contributing to national security missions through advanced OSINT capabilities. Her work spans both domestic and international arenas, including consultative roles with United Nations entities and various U.S. government agencies.



+(.,// &+$,1 '()(1',1* $0(5,&$,1 7+2) +,*+ 7(&+ :$5)$5(

By Christian Brose

Reviewed by COL (USA, Ret.) William Phillips

In today's competitive strategic and operational environments, replete with new and disruptive technologies, budget constraints, and the significant rise of China as a threat to U.S. international interests, *Kill Chain* is essential reading for U.S. military strategists and national security practitioners.[1] Accordingly, the United States must understand the current and future environments and challenges and be agile to adapt to them. Alternatively, consider the chances of winning a war against China by employing Cold War-era engagement methodologies and technological processes amid an information revolution that facilitates better and faster decision-making.

In *Kill Chain*, Christian Brose, former Staff Director of the Senate Armed Services Committee and Senior Policy Advisor to Senator John McCain (R-AZ), masterfully discusses the concept of "kill chain," which he believes, when properly implemented, will enable U.S. victory in a war against China, a peer competitor. According to Brose, "The kill chain is a process that occurs on the battlefield or wherever militaries compete. It involves three steps: The first is gaining an understanding of what is happening. The second is deciding what to do. And the third is taking action that creates an effect to achieve an objective."[2] He suggests that "although the effect may involve killing, more often the result is all kinds of non-violent and non-lethal actions that are essential to prevailing in war or military contests short of war."[3] Brose explains, "Focusing on the kill chain can help us avoid the common error of mistaking means for ends, the tool we use for the outcomes we seek when we think about technology."[4] Cautiously, he reminds readers that the government cannot afford to keep making this same mistake decade after decade. In this context, Brose articulates a motive for availing the book. He writes *Kill Chain* to help "make better sense of highly complex military and technological changes and how to navigate them successfully."[5]

Brose uses twelve chapters to enlighten readers about the changes and challenges in warfighting methodologies from the Cold War to the present. While expanding on the "kill chain" concept to help win in war, he emphasizes the need for innovation, adaptability, and the use of new technologies to assist warfighters in making better, faster decisions, thereby enabling operational success. The historical facts, firsthand experiences, observations, and warnings are insightful and should be considered by government decision-makers and military strategists.

In the first two chapters, Brose discusses the necessity of rethinking previous perspectives on force posture and the application of the military instrument of national power to address current realities concerning great power competition. His observations are salient, merit thoughtful consideration, and seek to inspire a desire for change. Specifically, he emphasizes the United States' fixation on operating under Cold War-era assumptions and methodologies. For example, during the Gulf War, the conflict in the Balkans, and the fight against al-Qaeda in Iraq, the United States relied on its superior technology and fought on its own terms from sanctuaries that our opponents could not reach.[6] Although victorious in those endeavors, he cautions the overly zealous and the militarily pompous that "winning had less to do with any decisive transformation in how the United States built battle networks and closed kill chains, and far more to do with the fact that our opponents were just not that capable."[7] Fundamentally, Brose suggests that these victories reinforced America's sense of dominance as well as its traditional assumptions about how to wage war.[8]

Unfortunately, these successes clouded the complacent minds of policymakers. As Brose states, "there was still no pressing need for change. Washington was as confident as ever in our dominance—overly so, in fact—and in the legacy military tools and ideas that delivered it. We kept buying many of the same kinds of military platforms and planning to use them in many of the same ways we had since the Gulf War."[9] After noting the problem of the government spending large amounts of money to sustain older methodologies that did not enhance or improve kill chains, Brose explains, "our kill chains struggle to confront dynamic threats, such as moving targets or multiple dilemmas at once. The primary reason for this is that the U.S. military understands the world, makes decisions, and takes actions but was not built to change."[10]

Brose implies that the United States' adherence to Cold War assumptions and methodologies hindered its ability to respond swiftly to the Russian invasion of Ukraine and the annexation of Crimea, as well as China's military buildup in the South China Sea. After outlining the events that unfolded in 2014, Brose notes a distinctive shift in the attitudes of government leaders. In the book, he writes, "It was not until the ambushes of 2014, first by Russia and then by China, that things began to change. Washington leaders were abruptly seized by what many of them began to refer to as the re-emergence of great power competition. And they started to think about how to respond …. And ways the United States could harness the most cutting-edge technologies, such as artificial intelligence, to leap ahead of its strategic competitors."[11] Seemingly, the "metathesiophobia," the fear of change, of the complacent, was met with a much-needed dose of necessity. But unsurprisingly, Brose's historical observations support the notion that bureaucracies are naturally conservative and resist change until it is prioritized.

Relatedly, Brose discusses the military-industrial complex and the commercial technology revolution in chapters three and four. He emphasizes the government's need to maintain a robust relationship with the military-industrial complex to leverage new and emerging technologies that could help ensure the military's competitive advantage against evolving threats. In doing so, Brose highlights the early contributions of the military-industrial complex to the development of advanced weapons such as the Minuteman missile, the atomic bomb, nuclear-powered submarines, and the SR-71 Blackbird. According to him, "The military-industrial complex grew up in response to incentives that Washington created."[12] He goes on to describe the motivations of engineers to solve the challenging problems posed by the Cold War while acknowledging that their work could also lead to personal wealth and increased safety for America.[13]

Brose then strikes a delicate balance in discussing the need for the government, notably the late Secretary of Defense Robert McNamara and Congress, to institute policies, regulations, and budgetary constraints to better account for government expenditure and manage procurement processes, despite the risk of discouraging government contractors from developing breakthrough technologies.[14] Interestingly, Brose implies that government bureaucracy affected innovation and the creative spirit of engineers working for well-compensated government contractors. However, he does not adequately explain or address the reasons behind the government's imposition of regulations to manage expenditures and processes. There is a subtle implication in the text that the government was stifling intellectual free-spiritedness and hindering progress.

Still, Brose reminds readers that Silicon Valley thrived and produced consumer products independent of the government—"commercial markets for the software, services, and consumer electronics that Silicon Valley was building quickly dwarfed the buying power of the Pentagon."[15] Brose also states, "the technology provided by those companies to commercial clients connected everything and everyone put better information in more

people's hands, and enabled them to make better, faster decisions about life and work."[16] He calls it a commercial technology revolution.[17] Brose notes, "The information revolution also created the conditions for an explosion in artificial intelligence and machine learning, which is the ability of machines to understand and learn from information independently of human commands."[18] He says, "There is simply nothing like this happening in the Department of Defense .... Most of the Department of Defense is ill-equipped to take advantage of machine learning in part because of how it deals with its own data."[19]

In the next few chapters, Brose addresses the concepts of change and innovation, as well as lethal autonomous weapons (intelligent machines of war). He rhetorically asks, "Can militaries innovate and change in the absence of war?"[20] In response, he states, "Military innovation and adaption are made more difficult because the nature of any bureaucracy is to resist change, not promote it."[21] "It is extremely difficult for militaries to innovate and change in the absence of war, but not impossible."[22] "It is only when civilian and military mavericks are aligned in favor of disrupting the status quo that real innovation becomes possible in the absence of war."[23] As a critique, the author rightly expresses that more enlightened mavericks are needed to advocate for change in the posture and readiness of the military but does not thoroughly address the political nature of Congress and the Senate Armed Services Committee that confront well-intentioned change agents. This may be important because war is an extension of politics.

In the last three chapters, Brose broaches the subjects of strategy, bureaucracy, and winning a war in the future. After making it clear to readers in previous chapters that China is a peer competitor to the United States, he opines that the government needs to shift its national strategy to include the defense and protection of the U.S. Homeland as a strategic focus area. Although the Department of Homeland Security is tasked with safeguarding the Homeland, Brose's assertion appears to be a reconsideration that should encompass combatant commands, government departments, and agencies. He states, "A new defense strategy must start by rethinking America's goals."[24] He also notes, "The thought of the US military fighting to defend its homeland is a foreign concept for most Americans and our military. It is seen as something that the United States forces others to do but does not have to do itself."[25] Brose implies that this refocus differs from the current Department of Defense's top priority of Homeland Defense, which includes "limited missile defense, support to domestic law enforcement, and confronting US enemies from our shores."[26] Brose states, "The United States is headed into a future that will be unsettling as it is unfamiliar, but we do not need to fear … the main question is not whether the US military should change but whether we can change and change fast enough."[27]

In a broad-veiled warning, which suggests that complacency could be catastrophic, Brose reminds readers of two important concerns: China's ascendancy and the need for a different kind of military. In *Kill Chain*, he says, "Denying China's military dominance is a clear definition of the US military's most pressing problem."[28] He further adds, "Changing how and for what the United States would fight in the future is necessary but not sufficient. We also need to change what our military fights with. The United States needs to build a different kind of military."[29] Reflectively, Brose believes that refocused national strategies are warranted and that incorporating new information technologies into an adaptable military force will enhance the strength, adaptability, and flexibility of the military instrument of national power and the viability of the kill chain to protect U.S. interests and defend the homeland.

In summary, Christian Brose's *Kill Chain* reminds readers that China is not just a peer competitor to the United States; the growing strength of its economy will also make its military a formidable challenge to the U.S. military and the broader military instrument of national power. Nevertheless, he implies that one should never disregard the ingenuity of those in Silicon Valley and those supporting the military-industrial complex in finding solutions to U.S. defense-related technology problems. However, these solutions must be recognized, championed, and implemented.

More broadly, Brose suggests that concentrated efforts, such as changing aspects of our national strategies, reevaluating the design of our military—including future procurement—and refocusing on the basics, like the military's strategic and operational kill zone, are essential. Implementing these actions will make the United States more competitive against rising threats to U.S. international interests and the homeland during this era of great power competition, potentially allowing for victory in a war against China. *Kill Chain* is an easy read and is recommended for national security professionals.
Editor's Note: Although this book was published five years ago, the topic remains significant and relevant to current U.S.-China relations and engagements, as well as the renewed focus on U.S. military readiness. Notably, China is identified as a pacing threat in the current

U.S. *National Security Strategy*; however, defense planners should consider peer-level military capabilities when gathering intelligence, developing strategies, and positioning forces to execute theater-level plans, especially in the Indo-Pacific region. The importance of this book is further underscored by the need to integrate artificial intelligence and disruptive technologies for enhanced lethality, while also making targeted defense budget cuts. Additionally, sources suggest that Xi of China has ordered his military to prepare for a potential invasion of Taiwan by 2027. Hopefully, we will not witness a repetition of events akin to those of 2014.

NOTES

[1] Christian Brose, The Kill Chain: Defending America in the Future of High-Tech Warfare (Philadelphia, PA: Grand Central Publishing, 2020).

[2] Ibid., xviii.
[3] Ibid., xvii-xviii.
[4] Ibid., xxviii.
[5] Ibid., xxviii.
[6] Ibid., 7.
[7] Ibid.
[8] Ibid.
[9] Ibid., 12.
[10] Ibid., 20.
[11] Ibid., 39.
[12] Ibid., 44.
[13] Ibid.
[14] Ibid., 45.
[15] Ibid., 53.
[16] Ibid., 54.
[17] Ibid.
[18] Ibid., 61.
[19] Ibid., 63.
[20] Ibid., 78.
[21] Ibid.
[22] Ibid.
[23] Ibid.
[24] Ibid., 188.
[25] Ibid., 191.
[26] Ibid.
[27] Ibid., 205.
[28] Ibid.
[29] Ibid., 198.

Reviewed by COL (USA, Ret) William Phillips, an assistant professor of joint, interagency, and multinational operations at the Army Command and General Staff College. COL (Ret) Phillips is a former strategist and plans chief for a combatant command. He holds multiple defense-related degrees, including a Master of Strategic Intelligence from the National Intelligence University and a doctorate from Georgetown University.

BOOK AND DAGGER: HOW SCHOLARS AND LIBRARIANS BECAME THE UNLIKELY SPIES OF WORLD WAR II

By Elsye Graham

Reviewed by Dr. J. Rocco Blais

Book Review

THE SPY WHO CAME IN

After reading *Book and Dagger: How Scholars and Librarians Became the Unlikely Spies of World War 2*, there is a new appreciation for the innovation of those professors and book collectors who became intelligence agents and fought to keep America safe during the Cold War. The author, Elyse Graham, is a notable historian and American writer, with degrees from Massachusetts Institute of Technology as well as Princeton and Yale University. Currently, she is a professor at Stony Brook University teaching poetry, argumentation, data humanities, and linguistics; her works have been favorably reviewed in the *New York Times* and *Time* magazine.

The extraordinary achievements that were documented, but not open to the public until recently, are due to safeguarding our secrets for the greater cause of our national security interests. "Espionage is more an art than a science. The key to espionage is the successful recruitment of spies. It is not easy, hence the small number of successful headhunters in the Clandestine Service of my day at the CIA."[1] The untold story of academics who became Office of Strategic Services (OSS) agents, as well as invented modern-day spy craft, and helped turn the tide of the war reveals the undeniable power of humanities in changing the world. The internal calling for a select few with gifted minds from campus to be trusted and take part in the shadow war of espionage has become history's greatest clandestine mystery.

When you receive a knock at the door by a silver-haired gentleman in a blue twill suit, you best answer; you can run, but you can't hide, or you may only be able to hide for a little while. One story recounted in the book was from Wallace Phillips (United States Navy), who reported directly to Major General William Donovan, the memoir had the scene as follows:

> First, he swore me to utter secrecy, then he told me more about myself than I had dreamed anyone else could know. He asked me if I wanted to serve my country. I told him that I was already in the Massachusetts State Guard at Sudbury, but that was not enough. He then informed me that I had been chosen to be the Lawrence of Morocco. [2]

TOO CLEVER TO BE TRAPPED BY A WOMAN?

One could live without fearing one's neighbors; no spies were allowed to operate in Stockholm, by government decree.[3] At this time, Sweden was a neutral country and thriving with men and women being notably clothed, stores stocked well, Stockholm streets busy and dramatically different than most of Europe being under military occupation. Poland and France had very few men as they were shipped off to Germany; whereas the women were known as '*widows*,' not knowing if the men would come back or not. What went on in the camps during 1942 – 1943, not many outsiders knew as Hitler's playbook was kept a secret. Outside of Europe, there were passages leaked and the press called it the 'Jewish problem' and it was becoming quite clear by what that meant. However, the Nazi's kept the many camp activities hidden even from many who worked nearby. This begs the crucial questions, "*How can that be? How is that so?*" With at least 1.1 million Jewish people dying in Auschwitz, Sweden tilted its neutrality in Germany's favor.

An American medieval scholar named Dr. Adele Kibre from August 1942 until the end of World War II lived in Stockholm, Sweden as an OSS agent. Dr. Kibre put her PhD in medieval studies as well as her master's degree in Latin to work as a scholar, micro-photographer, and documentation researcher. During those days in Stockholm, there were joint operation projects between British and American intelligence agencies with ordinary-looking people who lurked in the streets near diplomatic districts. Many secret police that were not very good at maintaining a low and clandestine profile were rampant. The OSS cautioned its agents not to meet sources at hotels they were staying at, as surely they were infested with spies pretending to be hotel staffers and quite possibly Swedish counterespionage

agents. Having foreign intelligence officers who lived at the hotel were most likely involved in the game, bugging rooms, ink blotting the registry, and collecting wastebaskets from rooms. Your next-door hotel guest or lunch table constituent could be eavesdropping on you with or without you knowing. So what could you do without giving yourself away? "Adele Kibre – a hard-nosed literary detective, a brunette from a Hollywood where blondes have all the fun, a woman serious about being taken seriously – was strangely well positioned to pull off a charm offensive on these particular targets."[4]

THE DIRTIEST WORK THAT CAN POSSIBLY BE IMAGINED

It is sometimes said that espionage is the second-oldest profession, the oldest, of course, being prostitution. Sometimes one profession helps the other."[5] You may never know who you are talking with, working for, or meet at King's Crown Hotel in New York City. Janet Coatesworth was a freelance writer and stenographer on 2 August 1939. On one particular occasion a physicist asked Janet if he could go to her hotel room and type a letter for her, which was a common profession during that time because women knew how to type, and men did not. This dapper gentleman dressed oddly and pacing frantically began to elaborate aloud about drafting this letter to F.D. Roosevelt, United States President, White House. Janet captured his warning to include extremely powerful bombs that could destroy an entire port and also the surrounding territory. Once she was done typing the physicist said, please add the signature line 'Yours truly, Albert Einstein.' Janet thought for sure this gentleman had a few screws lose, was deranged, and self-deluding phony. "Janet Coatesworth didn't know it, but her letter changed the course of the war."[6] Though World War II ended with the use of atomic bombs, the general public did not know about atomic energy and nuclear fusion, but President Roosevelt knew because men within the scientific community often built trust to safeguard these secrets. Sometimes, doing the dirty work at the very bottom, having power from below; the power of the pen or in this case, the power of a stenographer, is the perfect cryptographic tool.

SPIES, LIES AND A PLOT THAT NEVER DIES

The American military would capture a new city from the Nazi's and as they fled, those German soldiers would do their best to destroy the tidal wave of documents, but they were unsuccessful. The archives left behind were so vast that intelligence services couldn't keep up as there was too much information to be analyzed. In the summer of 1944, a Library of Congress research analyst reading through the items sent by the Interdepartmental Committee for the Acquisition of Foreign Publications (ICAFP) kept the documents flowing from London to Washington, D.C. However, they needed many more staffers to get through the eighty-five thousand issues. The Nazi's had realized that art had high value, masterpieces were worth lots of money, sending silver for submarines, melting bronze statues for bullets, and would burn or sell off the greatest artworks throughout Europe. By the fall of 1944, the OSS created a special intelligence outfit of historians rightfully named the Art Looting Investigation Unit. The Art Unit, which worked for the OSS was a group of women and men who was led by the Allied military command to protect important art, documents, monuments, and anything deemed necessary to securely archive."[7]

In conclusion, this book has many vignettes that capture highly encouraged readers; professors, historians, analysts, intelligence professionals, librarians, and academics alike. Many advocate that World War II was the physicist's war. In actuality, there were a lot of moving parts many done in secrecy that transformed how the war was fought and ultimately how it ended. The Second World War was a turning point in human history – it should also be known as the historian's war, the spy's war, the artist's war. Quite possibly the scholar's war. "The bomb may have ended the war, but the research and analysis performed by the people described in this book won it. So spectacular were their contributions that they changed the future of intelligence."[8]

Office of Strategic Services (OSS) Memorial Wall. 9

NOTES

[1] Barry Michael Broman, Indochina Hand: Tales of a CIA Case Officer (Haverton, PA: Casemate Publishers, 2024), 213.

[2] Elyse Graham, Book and Dagger: How Scholars and Librarians Became the Unlikely Spies of World War II (New York: Harper Collins Publishers, 2024), 9.

[3] Graham, Book and Dagger, 79.

[4] Ibid., 98.

[5] Ibid., 79.

[6] Ibid., 140.

[7] Ibid., 249.

[8] Ibid., p. 279.

[9] The Office of Strategic Services (OSS) Memorial. The dedication of the Major General William J. Donovan statue, CIA Headquarters, 28 October 1988. Retrieved from http://www.ossh.com/cia/intelligence/oss_memorial.shtml.

Dr. J. Rocco Blais is the Assistant Dean of the School of Science and Technology Intelligence and Associate Professor at the National Intelligence University (NIU) in Bethesda, Maryland. Dr. Blais has taught cyber intelligence, data science, national security and policy, science and technology, intelligence collection, and thesis methodology design since December 2016.

THE INTOKU CODE: DELTA FORCE'S INTELLIGENCE OFFICER—DOING GOOD IN SECRET

By Wade Ishimoto

Reviewed by LTC Kevin Petit (USA, Ret)

Wade Ishimoto, the legendary Delta intelligence officer, authored a 294-page book about Vietnam, Desert One, and half century old special operations exploits. Do we need more books like this? This review argues the world needs this one. "Ish," as his comrades call him, is a giant in the special operations community. His memoir is a mandatory read for Special Operations Forces (SOF) veterans, history buffs, strategists, and scholars. *The Intoku Code: Delta Force's Intelligence Officer – Doing Good in Secret* is a compelling exploration of leadership, ethics, and humility.[1] Ishimoto presents a philosophy rooted in the Japanese concept of *Intoku.* This idea emphasizes doing good without seeking recognition. The book weaves personal anecdotes, historical references, and practical insights. It offers readers a roadmap for leading with selfless integrity. The author's extensive background in military and intelligence services makes this a gem.

Wade Ishimoto was born in Hawaii shortly before the 1941 attack on Pearl Harbor. Post World War II cultural and societal challenges shaped his early life. He enlisted in the U.S. Army in 1961. Throughout his service, Ishimoto served as a Military Policeman, counterintelligence agent, human intelligence case officer, and spent fourteen years in Special Forces. His significant assignments, all superbly detailed, included some gems. He served in Vietnam as a Project Gamma Operations Sergeant. This operation sought Vietcong operatives in Cambodia. He became embroiled in the 1969 Green Beret Murder case. This involved the "mole-hunting" and the subsequent extra-judicial killings of informants allegedly on behalf of the Central Intelligence Agency (CIA). He served as an instructor at the Special Forces School and was a founding member of Delta Force. He also led a roadblock team during the 1980 EAGLE CLAW American hostages rescue attempt. After retiring, Ishimoto continued to contribute to national security. Notably, he took part in investigations into the 1993 Branch Davidian standoff and the 1996 Khobar Towers bombing. Wade Ishimoto's career is unequalled.

The book has four features: *Intoku*, adaptability, leadership, and historical insight. The first theme is *Intoku* Code. It is the book's central idea. This Japanese philosophy translates into doing good deeds without seeking recognition. This principle guided Ishimoto's actions throughout his life. The code emphasizes humility and selflessness. He prioritizes service, responsibility, and moral courage. *Intoku* is the standard against which Ishimoto measures all leaders. He is refreshingly candid about those that do—and do not—demonstrate this virtue. The book presents as having been written for this purpose, rather than out of any fierce inner impulse to reminisce or grandstand. The core idea of positive leadership and rejecting credit claiming is not novel. It is, however, extraordinarily rare in modern times.

The second theme is adaptability. The story journeys from the complexities of military operations to racial prejudices. It is a story of resilience, tenacity, and growth. Ishimoto grows and achieves under austere, dangerous, and politically sensitive environments. Whether through stubbornness, loyalty, or luck, he thrives and endures.

The third theme is leadership and mentorship in Ishimoto's life. He attributes much of his success to the guidance he received. In turn, he mentors others by fostering a learning, supportive culture. Ishimoto journeyed from Army private through sergeant major while holding a reserve officer's commission. This gives him a unique leadership advantage on both officer and enlisted perspectives. He gained this view while serving in top tier units, in peace and war. Ishimoto relays these virtues through personal experiences, providing readers with a primary source account of critical events. These include Delta formation and EAGLE CLAW details. These narratives provide perspectives on U.S. military history and the special operations intricacies. This work's chief contribution may be in its corroborative detail. The operation descriptions are plainly articulated, detailed, and original. Readers will feel the Vietnam jungle heat. They will feel fatigue from the long-range patrol operations. The prose captures the hardship and disappointment on the Iranian refueling site, Desert One.

Herein lies the work's value: it is a historical work, articulated in plain prose, by an on-scene operator. He compliments the EAGLE CLAW chapters with 44 glossy, engaging photos. These pictures compliment his accessible and engaging writing style. There is an EAGLE CLAW story about the two troopers on a Ranger-bike, pulling perimeter guard around the Iranian Desert One refueling site. Initially, a civilian tour bus breached the perimeter. Next, a 30,000-gallon fuel truck also penetrated the American hide-site before a Ranger shot it with a shoulder-fired weapon. These vignettes are part of official history and lore. The Delta commander Army Colonel Charlie Beckwith and the mission commander, Air Force Colonel James Kyle, relay the tale in their respective memoirs. This history is now part of the Ranger Regiment's orientation and indoctrination program. Yet 45 years later, we learn that Wade Ishimoto was in that buddy-team.

Former Secretary of State Dean Acheson wrote his memoir in 1961 titled, *Present at the Creation*. This connoted his presence and assistance in building the post World War II, U.S.-led global order. Likewise, Ishimoto was "present at the creation" of the nation's first counterterrorism force. His account of 1st Special Forces Operational Detachment - Delta is magnificent. He dispassionately details the challenges, personalities, friction, and politics. His account surpasses Beckwith's' 1983 account in *Delta Force* because he settles no political feuds nor splays justifying anger.

Ishimoto's historical vignettes are golden. It is easy to forget the 1970s featured international kidnappings and plane hijackings. Ishimoto recounts the August 1978 Chicago's O'Hare airport hijacking. On site, he advised the authorities. The Serbian national hijackers flew the plane to Ireland before being apprehended. Four months later, Delta also advised on the December 1978 Marion, Illinois hijacking. The Federal Bureau of Investigation (FBI) Special Weapons and Tactics (SWAT) tam resolved that crisis. In February 1979, an Afghan rebel faction kidnapped U.S. Ambassador Adolph "Spike" Dubbs. The communist Afghan government botched the rescue attempt, and the rebels assassinated Dubbs before Delta deployed. The same day, Iranian militants seized a portion of the U.S. embassy compound in Tehran. Militants held several hostages before releasing them a few days later. Delta requested to investigate and provide site exploitation. The State Department agreed, but European Command denied it. This would prove calamitous. Nine months later, Iranian revolutionaries seized 52 American hostages in the same compound. Delta lost its chance to have an on-site recon of the future rescue mission.

Regrettably, the book contains flaws. First, it is not a scholarly account. It does not pretend to be one—which is good because it does not deliver sophisticated theory. Readers expecting deep intellectual lessons will have to draw them out independently. Second, some readers might find detailed military jargon and operational descriptions challenging to follow. Third, in one sense it is a "who's who" in the national security power circles. But in another sense, it drops many names, some recognizable, and some obscure. This part reads more like homage to old friends and mentors than a leadership guide. It is not ostentatious name-dropping, but it is unnecessary. Last, readers interested in the "birth of Delta" account--perhaps its best feature—must wade in 127 pages to get a mere 68 on the topic. The story could have profited from more development.

History buffs will love it for its added details on important historical events. Special operations veterans will revere it as an honest, detailed account from one of the SOF plank-holders. Leadership and management aficionados will appreciate *The Intoku Code* as it

challenges the prevailing leadership notions. It eschews the corner office, rank, or titles as power manifestations. Instead, Ishimoto advocates for a leadership style that inspires trust and fosters meaningful change. His reflections on teamwork and decision-making, particularly in military and intelligence operations, provide poignant lessons for professionals.

To sum, *The Intoku Code* is an insightful and inspiring read. It ventures beyond military achievements and lauds esteemable values and principles. His emphasis on "doing good in secret" serves as a character lesson. Read it for the invitation to embrace humility, self-discipline, and service to others as the true markers of success.

NOTES

1 Wade Ishimoto, The Intoku Code: Delta Force's Intelligence Officer – Doing Good in Secret (Havertown PA: Casemate publishers, 2024).

Dr. Kevin Petit is a faculty member at the National Intelligence University and serves as the Strategic Intelligence and Special Operations (SISO) concentration director. He is a retired Army officer with over four years in Iraq and Afghanistan theaters. He holds a Ph.D. in international relations from George Washington University.

CAUGHT IN THE CROSSFIRE: THE INSIDE STORY OF PAKISTAN'S SECRET SERVICES

By Naseem Akhtar Khan

Reviewed by MSgt Logan Fountaine

Conventional wisdom suggests that democratic nation-states are stable, have strong governance, and are unlikely to backslide. This notion, however, is wrong.

This essay argues Naseem Akhtar Khan's *Caught in the Crossfire: The Inside Story of Pakistan's Secret Services* is worth reading for democratic backsliding aficionados.1 While the book lacks novel revelations, it offers meaningful insight for intelligence professionals and military strategists examining the intersection of globalization, counterintelligence, and leadership in South Asia. Khan offers a unique perspective on international partnerships and adversaries, the effects of the political elite on governance, and solutions to the emerging security challenges in the region. He critically disputes the "democratic, strong stable state" assumption. He explores Pakistan's geopolitical and security challenges by narrating his experiences, including his service in the Pakistan Army and the Pakistan Inter-Services Intelligence (ISI). Khan argues that foreign allies and enemies exploit Pakistan's geostrategic location, leading to weak governance and further internal divisions and alienation between the government and its people. A divided relationship between the government and its citizens undermines the principles of democracy and hinders societal achievements. He distinctively interrelates his memoirs and Pakistan's history as evidence for his concepts and how the dynamics of Pakistan's international relationships affected the region's security. This review argues that the book is flawed but has exceptional features.

Khan's unique background and experience as a military member and security professional provided him with credibility for his authentic insights. He collectively served in the Pakistan Army as an artillery officer and in the ISI as a counterintelligence professional for approximately 40 years. Khan held numerous high-level assignments, including commanding the ISI detachments in Rawalpindi and Islamabad, being the sector commander of Punjab Province, and eventually becoming the Deputy Director General of security and counterintelligence. He also served as a diplomat for the Ministry of Foreign Affairs in Dubai for approximately three years while in the military, and post-retirement, established a private security company with an international presence. Throughout his service, he had a role during the Russian invasion of Afghanistan, the Afghan civil war, and the United States' involvement in Afghanistan after the September 11, 2001, terrorist attacks. Khan highly values his education and has attended some of Pakistan's most prestigious military schools, such as the Command and Staff College in

Quetta. His experiences provided several strengths to his book.

Khan used his distinguished upbringing and career to strengthen his argument countering the international community's misrepresentation of Pakistan's security narrative. He used personal experience in counterintelligence operations to emphasize adversaries exploiting Pakistan's internal vulnerabilities. One example was Khan's arrest of a spy network of Pakistani scientists and engineers working on behalf of a foreign intelligence entity to sabotage Pakistan's nuclear program. He also identified high-profile politicians working for Pakistan's adversaries to undermine democracy and prioritize personal ambitions. Khan uses examples of India's disinformation and influence operations in Pakistan and the United States to clarify the interference of democratic states.

However, Khan also illuminates Pakistan's government as a culprit in further dividing the government from its citizens with "deep-rooted corruption" throughout Pakistan's social structure. He witnessed numerous incidents, which strengthened the book and his argument. Another significant strength of his book was his suggestions to Pakistan and the international community on reforming existing processes to mitigate national security threats. Through his anecdotes, he challenged the international community to understand Pakistan's history and how it remains an ally to the West, but not without undue struggle caused by the U.S.-sponsored regional decisions. He also challenged Pakistan to align its governance with its national ideology, fix its poor governance and economic erosion, and address complex internal and external security issues, which create a fragile state.

Although Khan's personal experiences provided credibility to his arguments, the book had several weaknesses. One of his weaknesses is the potential biases throughout the memoir. The book comprises the author's opinions and experiences, offering distinctive insights into Pakistan's security issues. However, it does not include external sources that could provide a more comprehensive perspective. One bold claim was how the U.S. withdrawal from Afghanistan "shattered the existing world order," and compared the U.S. presence in Afghanistan to the historical British occupation.

Part four, excluding the conclusion section, weakens the book's overall impact by shifting from Khan's operational insights as an ISI officer to less compelling reflections on his post-retirement career in private security. Part four attempts to emphasize the importance of international relationships and evolving security trends, such as process modernization and threat management. Despite the attempt, it detracts from the book's narrative by shifting to an unrelated topic. The lessons learned section included leadership and personal recommendations, such as recognizing mistakes, accepting responsibility, and self-belief. Though these were positive messages and aligned with some of the concepts discussed throughout the book, they are out of place for the book's final part.

In sum, Khan's work is an excellent book for those interested in the upbringing of Pakistan soldiers and the security situation from an insider's perspective. The book has its strengths and weaknesses, but overall, it is a unique memoir-style work that clarifies misconceptions from the international community on what has contributed to Pakistan's continuous democratic backsliding. The author sometimes weakens his overall message through a style shaped by personal perspective and narrative choices. However, it remains captivating in the intricacies and struggle of a fragile democratic state, further exacerbated by foreign adversaries exploiting existing internal security issues and dissidence between the government and its citizens.

NOTES

[1] Naseem Akhtar Khan, Caught in the Crossfire: The Inside Story of Pakistan's Secret Services (Philadelphia: Pen and Sword Books, 2024).

Master Sergeant Logan Fountaine is a Special Agent with the Department of the Air Force's Office of Special Investigations (OSI). He recently graduated from the National Intelligence University with a Master of Science of Strategic Intelligence degree.

BRIXMIS AND THE SECRET COLD WAR: INTELLIGENCE COLLECTION OPERATIONS BEHIND ENEMY LINES IN EAST GERMANY

By Andrew Long

Reviewed by Dr. Christopher E. Bailey

Book Review

Andrew Long, a Cold War historian and an accomplished historian, offers a fascinating book on an important military intelligence collection asset that operated in East Germany from 1946 to 1990. BRIXMIS (formally known as the British Commander-in-Chief's Mission to the Commander-in-Chief, Group of Soviet Forces of Occupation in Germany) was one of six allied military liaison missions established after the war ended in occupied Germany under separate bilateral military agreements. The United States, Great Britain, and France established liaison missions in 1946-47 in Potsdam; each had an official liaison mission and "touring" privileges throughout occupied East Germany, allowing the teams to observe Soviet and East German military activities on the ground. In turn, the Soviet Commander-in-Chief established three separate military liaison missions in occupied West Germany (one each in the British, American, and French zones of occupation). In short, the Western military liaison missions based in Potsdam had a unique opportunity to collect important information about the Soviet Army's home station facilities, order of battle, unit equipment, field training sites and activities, general combat readiness, and much more. In other words, the allied missions were positioned to collect valuable information on what specifically the West needed to know about Soviet/East German combat readiness and, during periods of increased tension, whether cross-border hostilities were imminent.

There are several earlier works in this niche field of intelligence studies, including published books, articles, theses, monographs, and news articles. Some American readers will be familiar with the Potsdam-based U.S. Military Liaison Mission (USMLM) and the March 1985 killing of U.S. Army officer Major Arthur Nicholson while he was trying to collect information about the Soviet Army's new and formidable T-80 tank near Ludwigslust-Techentin in the northeast corner of the former East Germany. For example, there are several good books about the Potsdam-based USMLM[1] and its Frankfurt-based Soviet counterpart (the SMLM).[2] There is also one book (in French) about the French Military Liaison Mission (MMFL)[3] that—like the BRIXMIS—was based in Potsdam. This leads to an important question: what has been previously published on BRIXMIS, and what does Andrew Long add to this body of literature?

There are two good, previously published books on BRIXMIS. In 1996, Tony Geraghty offered the first published work on BRIXMIS.[4] Geraghty, an accomplished author with access to important primary source material and BRIXMIS veterans, provides an excellent history from 1946-90. He places BRIXMIS in the context of the postwar political rivalry and the East-West military confrontation in Germany. BRIXMIS was always a small unit, never with more than 31 soldiers on tour ("pass") in the East, although the unit was staffed with highly qualified intelligence collectors and linguists. Thus, while the teams were unarmed, a qualified linguist with a knowledge of Russian or colloquial German, or a capable driver, might get his team out of a difficult situation. Geraghty provides a fascinating perspective on the 1953 East German uprising over economic grievances, how British traitor George Blake (then serving in the Berlin Secret Intelligence Service/SIS station one floor down from the BRIXMIS offices) likely compromised mission activities, how the British managed to access an advanced Soviet fighter (the 1966 Firebar affair) that had crashed in the British sector (in the Havel), and how a BRIXMIS tour managed to access a T-64 tank. No doubt, Geraghty shows that BRIXMIS was a premier intelligence activity that found things that would have otherwise been difficult to collect through clandestine, attaché, signals intelligence, or imagery assets. In some cases, BRIXMIS demonstrated that otherwise reliable signals intelligence was just wrong. In other words, BRIXMIS could track many indicators of hostilities much more effectively than other collection assets. I did appreciate his appendix I ("The BRIXMIS 'Trophy Cupboard' of Intelligence Scoops").

In 1997, Steve Gibson, a former British tour officer, authored an account of his first-person experiences in 1989-90; Gibson provides readers with the detailed experiences of a British officer in the year before and after the end of the Cold War.[5] He takes the reader through the BRIXMIS selection process and introduces the reader to the touring experience with all of its opportunities and challenges. Like Geraghty and Long, Gibson narrates the experiences of Soviet/East German vehicle chases and detentions, replete with vehicle ramming and

shootings. He tells the reader about his experiences on a "Tommy" (Operation Tomahawk, the late-night visits to garbage dumps in search of intelligence prizes), trying to photograph a moving Soviet kit train with a highly sought army-level command and control vehicle, and collecting on new equipment (often involving a judgment call on the possible gain v. risk at guarded sites). Gibson also relates the last BRIXMIS mission before the Wall came down, as well as the difficult and uncertain period before BRIXMIS closed its doors after German reunification in October 1990. Clearly, BRIXMIS performed an important final role as a verification and confidence-building tool during the Soviet withdrawal.

Andrew Long is an accomplished military historian who has published five prior books on the Cold War. Long used diverse resources in writing *BRIXMIS and the Secret Cold War.* He mined a range of prior materials, published and unpublished, conducted archival research in the United Kingdom and Germany, and interviewed many BRIXMIS veterans. The result is a richly detailed book that covers the mission itself and how it evolved in the British/allied intelligence enterprise; how the unit trained, equipped, supported, and deployed its personnel; how its teams conducted reconnaissance activities (euphemistically called "touring"); what it had for the "tools of the trade" (e.g., the maps, vehicles, cameras, and other equipment); and how the teams fought (and sometimes overcame) their Soviet/East German opponents who sought to interfere with their tours and make their lives more difficult. All of this is illustrated with interesting stories that resulted in important intelligence "scoops." Long leaves the reader with no doubt about the value added by BRIXMIS in preparing the West for a war in Central Europe that (thankfully) never came.

Andrew Long expanded on the earlier works, providing the reader with a comprehensive account that builds on the earlier works. Unlike earlier authors, he is somewhat less focused on great collection stories; he offers an analytic work that examines a range of important issues, while using interesting historical events to illustrate important points. He offers useful information on official liaison activities, including interpreter support at formal meetings, social events, and the Spandau Prison, which was located in the British sector. Critically, Long provides an unmatched examination of how BRIXMIS operated inside the British intelligence enterprise. His book provides the usual photographs, maps, and charts, along with a detailed glossary and appendices for the 1946 Robertson-Malinin agreement that chartered the BRIXMIS, a listing of BRIXMIS chiefs and deputies, and detailed information on different touring vehicles, equipment, and the Chipmunk aircraft used for local reconnaissance flights in the Berlin Control Zone.[6] Long's bibliography and index have greater detail than that offered by Geraghty or Gibson.

The BRIXMIS mission conducted three-man vehicle patrols throughout East Germany. Typically, tour activities were planned based upon operational taskings from the British Army of the Rhine or London, as a follow-up to earlier patrols, from a cueing by other national collection assets (e.g., a signals intercept), or recent events. A tour might last from a single day in the local area (Potsdam) or a multi-day trip to a distant corner of East Germany. The touring teams often had to evade Soviet KGB/GRU teams, East German security forces (e.g., the Stasi or local police), and Soviet/East German soldiers. Some areas of East Germany were marked as Permanently Restricted Areas (PRAs) or Temporary Restricted Areas (TRAs) that would be out-of-bounds to mission tours. Understandably, such restricted areas had important installations or training areas or training areas in use; such signage typically also heightened a tour officer's interest in that area. The teams were equipped with touring kit that included annotated maps, multiple cameras with specialized lenses, infrared scopes, camping equipment, food, and extra food—but neither weapons nor radios.

The BRIXMIS teams learned, over time, the need for close, tri-mission coordination involving the American and French military liaison teams to enhance collection coverage and avoid any undue Soviet/East German attention that might result from overworking a location/area. The BRIXMIS teams helped map East Germany, charted 95 percent of the Soviet order of battle in East Germany, photographed equipment and aircraft at sensitive locations (sometimes by climbing on top of equipment at guarded sites); emplaced unattended ground acoustic sensors that could collect on passing vehicle traffic; collected refuse at military garbage dumps (Soviet soldiers typically lacked toilet paper and might use any handy substitute); and stole ammunition samples, documents, and even equipment. In many cases, BRIXMIS provided key insights into new Soviet equipment, order of battle, the transfer of equipment to the East German Army, and tactics. Some of the mission's greatest feats involved photographs of the interior of a T-64 tank and its fire control system, the recovery of documents detailing the new T-80 tank, a section of explosive reactive armor from a T-80, confirmation of new combat vehicles and aircraft, and even an anti-tank missile. All of this was invaluable for military planners, intelligence analysts, and the UK-based technical experts who would have been involved in the design/fielding of new equipment that could counter or defeat Warsaw Pact forces.

I strongly recommend Andrew Long's book. *BRIXMIS and the Secret Cold War* is a fine contribution to this niche corner of Cold War history. BRIXMIS provided British forces with a unique service that could not have been matched by any other single Cold War collection asset in search of ground truth.

NOTES

[1] See, for example, John A. Fahey, *Licensed to Spy: With the Top Secret Military Liaison Mission in East Germany* (Annapolis, MD:

U.S. Naval Institute Press, 2002) (a first-person account of a naval officer in the early Cold War period); James R. Holbrook, *Potsdam Mission: Memoir of a U.S. Army Intelligence Officer in Communist East Germany* (Bloomington, IN, Authorhouse, 2013) (the author shares his experiences as Soviet/Russian specialist and his own intelligence collection experiences in East Germany).

[2] Aden Magee, *The Cold War Wilderness of Mirrors: Counterintelligence and the U.S. and Soviet Military Liaison Missions, 1947-1990* (Haverton, PA: Casemate USA, 2021).

[3] Patrick Manificat, *Au Coeur de la Guerre Froide - La Mission Militaire de Potsdam 1947-1989* (Paris: Histoire & Collections, 2015) (available only in French).

[4] Tony Geraghty, *BRIXMIS: The Untold Exploits of Britain's Most Daring Cold War Spy Mission* (London: HarperCollins, 1996).

[5] Steve Gibson, *BRIXMIS: The Last Cold War Mission* (Gloucestershire, UK: The History Press, 1997).

[6] The Berlin Control Zone was a four-power organization that owed its existence to a 1945 agreement on the rules of flight in the city, rather than the 1946 bilateral agreement that established the BRIXMIS. Nonetheless, after the 1953 East German uprising, the BRIXMIS chief noted a need for an airborne reconnaissance capability, and the mission acquired a single-engine two-seat trainer (Chipmunk aircraft) that performed low-altitude photographic missions (sometimes as low as 300 or 500 feet). Long provides much more information on the Chipmunk flights than either Geraghty or Gibson. See Andrew Long, *BRIXMIS and the Secret Cold War: Intelligence Collection Operations Behind Enemy Lines in East Germany* (Philadelphia: Pen & Sword, 2024), 107-118.

Dr. Christopher E. Bailey is a professor at the National Intelligence University in Bethesda, Maryland, specializing in national security law, international law, and professional ethics. Dr. Bailey is licensed to practice law in California and the District of Columbia. He has an LLM degree in National Security & U.S. Foreign Relations Law, as well as an SJD degree in International and Comparative Law, from the George Washington University School of Law.

Book Review

TRAITOR'S ODYSSEY: THE UNTOLD STORY OF MARTHA DODD AND A STRANGE SAGA OF SOVIET ESPIONAGE

By Brendan McNally

Reviewed by Mr. Daniel Brezin

There are countless books available on Nazi Germany and Soviet espionage, but Mr. Brendan McNally uncovers an odd corner of this strange and secretive world in his new book, *Traitor's Odyssey*. McNally retells the story of a very eccentric woman—Martha Dodd, daughter of William Dodd who was the American ambassador to Nazi Germany in the 1930s. While calling Martha's journey an odyssey might be a stretch, McNally relentlessly leads the reader through her wild days in Berlin to her final years in Prague.

At this point, one who is familiar with the topic might ask, wasn't a similar story already told in Erik Larson's 2011 book *In the Garden of Beasts*?[1] The answer is partially, yes. Whereas Larson's book focuses mostly on the family's time in Berlin, McNally continues the story of Martha's bizarre life up to her death in Prague. A reader who is interested in the history of U.S. diplomacy with Nazi Germany should read both books, but McNally expands on Martha's time spent dabbling in espionage.

Mr. McNally is uniquely positioned to capture the raw culture and grit of life in former Soviet bloc countries. As a journalist and author who has written about defense, security, and intelligence issues, he also lived in the Czech Republic for many years. This allowed him to integrate firsthand knowledge of the culture into his writing on Martha's escapades around the region. The reader is immersed in the social scene as Martha attempts to promote herself as an American spy for the Soviets.

Unfortunately, despite her best efforts, Martha was not much of a spy. Nor was she a very good communist. In fact, there was little interesting about her character other than her alleged willingness to have sex with just about any man she met, except Hitler. This storyline was a distraction from what a reader might have hoped to be a deep dive into Cold War espionage tradecraft, and what little bit existed was largely speculative. McNally had to use the term "presumably"—frequently—to fill in the blanks. There were also many odd exclamations and crass vernacular sprinkled in that did not fit with the rest of the story.

How useful was Martha as a spy? For her Berlin years, there was a lack of substantial evidence that she provided any useful intelligence to the Soviet Union. Regardless, the NKVD kept their man on her (literally) because she was the American ambassador's daughter. Years later when she was living back in the United States, the Vassiliev KGB archives noted in 1948 that an agent relationship should not

be established with her due to her talkative and reckless behavior.[2] She was too open about her support of communism and relentlessly volunteered herself to work as a spy for the Soviets. Nonetheless, the KGB kept in contact with her, and she was able to broker introductions of KGB agents to important social circles in the United States. Meanwhile, her NKVD lover and handler from Berlin suffered a typical tragic Russian ending.

As Martha and her husband ultimately came under the scrutiny of the Federal Bureau of Investigation, they did what any good aspiring communist would do and fled with their millions of dollars to Mexico. With no access to any intelligence, the Soviets had little use for her.

Regardless, while living in exile and fearing extradition back to the United States, the Soviet Union granted them asylum and safe passage to Prague where they could live out the communist dream—a dreary existence even with their money. In an anticlimactic conclusion, the U.S. Attorney's office dropped all charges except for a significant fine for failing to appear in court.

NOTES

[1] Erik Larson, *In the Garden of Beasts: Love, Terror, and an American Family in Hitler's Berlin* (Crown Publishing, 2011).

[2] Alexander Vassiliev, Alexander Vassiliev Papers, manuscript/mixed material, https://lccn.loc.gov/mm2009085460, 77.

Mr. Daniel Brezin, a graduate student at National Intelligence University's School of Science and Technology in Bethesda, Maryland. Mr. Brezin recently spent three years on assignment as a diplomatic technology officer with the State Department at the U.S. Embassy in Berlin.

CHIP WAR: THE FIGHT FOR THE WORLD'S MOST CRITICAL TECHNOLOGY

By Christopher Miller

Reviewed by Jai K. Singh

Chip War is a thought-provoking and insightful book that offers a detailed evolution of the computer chip, tracing its development from the 1930s to the present-day production of artificial intelligence (AI) chips. Chris Miller's extensive research on computer chips approached from the technical and national interest perspectives, beautifully marries these viewpoints and illustrates how they are intertwined. With a bachelor's degree from Harvard University, as well as a master's degree and doctorate in history from Yale University, Dr. Miller certainly has the credentials to provide a thorough historical context for chips and their connection to national security interests in the key countries that have been striving for dominance in the chip industry.

I was motivated to read *Chip War* because the subject matter intrigued me, especially given the recent exponential growth in the AI chip market. It was an eye-opener to realize how our daily lives are so intertwined with chips; not a second goes by without their presence, whether in our Wi-Fi, mobile phones, cars, trains, kitchens, or computers. The list is virtually endless.

I enjoyed the exploration of chip evolution. Coming from an engineering background, I appreciated the detailed descriptions of the internal architecture of chips and the various solutions discovered to improve their design continuously. Reading about the technical aspects was nostalgic and fun, taking me back to my engineering classes. It was fascinating to observe how a country's economy can be tied to chip production and how this aligns with U.S. national interests. The book emphasizes the urgent need for innovation because the nations that control the chip market will undoubtedly become global superpowers. This should serve as a wake-up call for the United States to invest heavily in the next generation of chips if it wants to maintain its status as a global leader.

Chris Miller also underscores the connections to national security and intelligence by dedicating multiple chapters to this topic, stressing how vital it was for the U.S. government to support the chip industry during the early years of integrated circuit research and manufacturing, which contributed to winning the Cold War. He argues that it is essential for the U.S. government to assist American chip companies again to prevent adversaries like

China and Russia from gaining a significant lead in this industry through firms like Huawei, which is becoming a behemoth in both manufacturing and research. Companies like Taiwan Semiconductor Manufacturing Company (TSMC) are increasingly dependent on Huawei's business, raising the risk of China potentially manipulating these chips for intelligence gathering—an alarming national security risk for the United States and its allies. At this juncture, chips are truly like the crude oil of the 1980s, a significant point highlighted by Miller.

Intelligence practitioners should read this book to understand the critical need for the United States to maintain its lead in this industry. It exemplifies the role integrated circuits played in keeping the United States ahead of countries like China and Russia, as well as their links to Japan and Taiwan. I highly recommend this book, as it not only provides significant historical context for the progress made by the United States since World War II but also offers insights into how national intelligence and security are tied to the necessity for the United States to continue leading in the chip industry.

Jai K. Singh, IT Program Manager at the Office of Director of National Intelligence (ODNI), at the National Counterintelligence and Security Center; he has over 20 years of experience in managing IT projects in various industries.

CO-INTELLIGENCE: LIVING AND WORKING WITH AI

By Ethan Mollick

Reviewed by Saleela Khanum Salahuddin

Wharton Professor Ethan Mollick published *Co-Intelligence: Living and Working with AI* in April 2024, just as the discussions about integrating artificial intelligence (AI) across the intelligence community (IC) were formalizing on the policy front, which continues into the present to advance the U.S. government's national security mis sion by harnessing cutting-edge AI technologies.[1] As the AI Policy and Governance Lead for the Office of the Director of National Intelligence, I work with the Chief AI Officers across the IC on developing approaches and methodologies to accelerate AI adoption across the IC.

The framework that *Co–Intelligence* presents is worth consideration as these developments are underway.

Let's first define AI. Carnegie Mellon has said, "AI refers to the ability of machines and computers to perform tasks that would normally require human intelligence. These tasks include things like recognizing patterns and making predictions. Ultimately, that's not magic; it's math."[2] As a matter of statutory definition, according to 15 U.S. Code § 9401, AI is defined as "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments." The notes in 10 U.S. Code § 2358 further define artificial intelligence as:

1. Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.
2. An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action.
3. An artificial system designed to think or act like a human, including cognitive architectures and neural networks.
4. A set of techniques, including machine learning, that is designed to approximate a

cognitive task.

5. An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting.[3]

With this AI definition in mind, Mollick presents his framework via "Four Rules of Co-Intelligence,"[4] outlined below. These four rules are valuable for Intelligence Community (IC) AI policymakers, practitioners, and the IC workforce to apply when leveraging AI to benefit analytic tradecraft applications and day-to-day work operations. It is through greater engagement and experimentation with AI tools in the IC mission, as informed by this framework, among others, that the U.S. government's national security apparatus will be able to deploy AI capabilities at mission speed.

Principle 1: Always Invite AI to the Table: "You should try inviting AI to help you in everything you do, barring legal or ethical barriers."[5] Mollick's main premise is that AI, as a quasi-sentient form of machine-based intelligence, is a tool that can augment human thinking and output and increase productivity if used responsibly and ethically. But for AI tooling to have this valuable impact for society and the economy, it must be brought to the table—i.e., used in everyday personal and working life. Mollick uses the analogies of AI as a co-worker, teacher, expert, and companion to bring this point home.[6] Inviting AI to the table by using it is essential because only those users who understand the limitations and abilities of AI will be able to innovate in the best way.

Principle 2: Be the Human in the Loop. "For now, AI works best with human help, and you want to be that helpful human."[7] AI needs to be used and not just admired as exquisite technology. It is only through the active daily use and application of AI as an intelligent software system that we can ensure that AI receives 'reinforcement learning from human feedback' to reduce bias and error in outputs while increasing the volume of productivity.[8] At a micro-level, this means that a lone human user of AI as a tool—such as an IC analyst hard-pressed for time and working to support a warfighter or operational demands—needs to ensure they cross-check AI-derived outputs against their own subject matter expertise and critical thinking to ensure that final outcomes are well-informed and accurate, rather than wholesale accept AI-derived outputs.

On a macro-level, human engagement "requires a broad societal response with coordination among companies, governments, researchers, and civil society. Companies must make principles like transparency, accountability, and human oversight central to their technology. Researchers need support and incentives to prioritize beneficial AI alongside raw capability gains. And governments need to enact sensible regulations to ensure public interest prevails over a profit motive."[9] The human in the loop principle is central to responsible and ethical AI use to generate ideas while simultaneously applying human thinking and creativity to filter, sort, and then refine the optimal output.

Principle 3: Treat AI like a Person (but tell it what kind of person it is). "AI systems don't have a consciousness, emotions, a sense of self, or physical sensations . . . [but] working with AI is easiest if you think of it like an alien person rather than a human-built machine."[10] Mollick advises that the easiest way to do this is to provide contexts and constraints in feeding prompts to AI tooling to help create an AI "persona" that produces outputs valuable to a human user who then edits and provides further guidance to the machine for improved outputs, enabling taking advantage of AI as a "form of collaborative co-intelligence."[11] The implications of this principle for the IC and the United States' national security use and application of AI are profound. If, as noted by Massachusetts Institute of Technology professor John Horton,[12] AI does not have an independent morality but is instead interpreting the moral instructions of the inputs it receives, it is important that AI models are trained based on policy and governance rules guided by a value set anchored in American democratic principles. When considering the adversarial and economic threat posed to the United States by AI global competitors such as China, whose stated goal of world dominance in AI by 2027 seems frightening when placed next to their highly criticized track record on privacy and civil liberties,[13] the criticality of this principle becomes clear. For American world leadership in AI to be truly realized, AI must be treated like a person, but one informed by American democratic guidelines and guardrails.

Principle 4: Assume this is the worst AI you will ever use. "As AI becomes increasingly capable of performing tasks once thought to be exclusively human, we'll need to grapple with the awe and excitement of living with increasingly powerful alien co-intelligences . . . you can view AI's limitations as transient, and remaining open to new developments will help you to adapt to change, embrace new technologies, and remain

competitive[.]"[14] The U.S.-based tech sector giant, Microsoft, acknowledges that even the most cutting-edge AI tools face barriers to widespread adoption, due in part to concerns around bias, accountability, and property rights, among other factors.[15] Even so, there are trusted ways to secure AI outputs and mitigate these concerns, namely by adhering to risk management frameworks, such as the one outlined by the National Institute of Standards and Technology.[16] With regards to the IC and its adoption of AI, efforts to deploy AI safely and securely will be possible so long as risk management frameworks are in place that support innovation and engagement. And given the importance of the risk management frameworks in governing how AI will be deployed domestically and globally, it is once again critical that those risk management frameworks be informed by American democratic principles.

It is fair to question whether we should heed Mollick's guidance, when there are so many voices in academia aiming to shape future AI adoption. Beyond his credentials and reputation in the technical and policy AI communities, Mollick has a unique ability to make complex technical subject matter and its potential societal application relatable and easily understood. Mollick specializes in entrepreneurship and innovation and has dedicated his research to real world applications of emerging technology, with his scholarship featured in *Forbes*, *The New York Times*, and *The Wall Street Journal*.[17] Mollick's framework is compelling and persuasive even without these academic and mainstream credentials. Even as AI advancements continue at ever-increasing speeds—"advanced reasoning and knowledge application in complex scenarios" is beginning to be seen in near doctoral-level AI outputs[18] – the Four Rules of Co-Intelligence will remain both easy to understand and important to consider because "[t]oday's decisions about how AI reflects human values and enhances human potential will reverberate for generations."[19] These values, particularly for the IC, should be developed to ensure that America and its allies lead the world in democratically-guided AI innovation, policy, and governance.

NOTES

[1] Ethan Mollick, *Co-Intelligence: Living and Working with AI* (New York: Portfolio, 2024).

[2] Jennifer Monahan, Artificial Intelligence Explained, Carnegie Mellon University Heinz College, https://www.heinz.cmu.edu/media/2023/July/artificial-intelligence-explained (July 2023).

3 For more information on AI research see the National Institute of Standards and Technology (NIST) overview on artificial intelligence (https://www.nist.gov/artificial-intelligence) and the National Artificial Intelligence Initiative (https://www.ai.gov/).

4 Mollick, Co-Intelligence, 46-62.

[5] Ibid., 47.

[6] Ibid., xx.

[7] Ibid., 52.

[8] Ibid., 13-14, 37-38.

[9] Ibid., 44-45.

[10] Ibid., 56-57.

[11] Ibid., 60.

[12] John Horton, Large Language Models as Simulated Economic Agents: What Can We Learn from Homo Silicus?, https://john-jo-seph-horton.com/papers/llm_ask.pdf (March 22, 2023) (advancing the thesis that newly-developed large language models — because of how they are trained and designed—are implicit computational models of humans).

[13] Gyana Swain, *ComputerWorld, China Unveils Ambitious Three-Year Plan To Dominate AI and Computing Standards,* https://www.computerworld.com/article/2132168/china-unveils-ambitious-three-year-plan-to-dominate-ai-and-computing-standards.html (May 30, 2024).

[14] Mollick, *Co-Intelligence,* 62.

[15] Megan Crouse, TechRepublic, *Generative AI in Security: Risks and Mitigation Strategies,* https://www.techrepublic.com/article/micro-soft-generative-ai-security-risk-reduction-isc2/ (Oct.15, 2024).

[16] National Institute of Standards and Technology AI Risk Management Framework, https://www.nist.gov/itl/ai-risk-management-framework.

[17] Mollick also authors the widely read tech blog One Useful Thing, https://www.oneusefulthing.org/.

[18] Samantha Dunn, CNN, *OpenAI's GPT-5: Set to Achieve Ph.D.-Level Intelligence by 2026, Says CTO Mira Murati,* https://www.ccn.com/news/technology/openais-gpt-5phd-level-intelligence-2026-cto- mira-murtati/ (June 21, 2024).

[19] Mollick, *Co-Intelligence,* 45.

Saleela Khanum Salahuddin is the Artificial Intelligence Policy and Governance Lead, Office of the Director of National Intelligence, Office of Science and Technology.