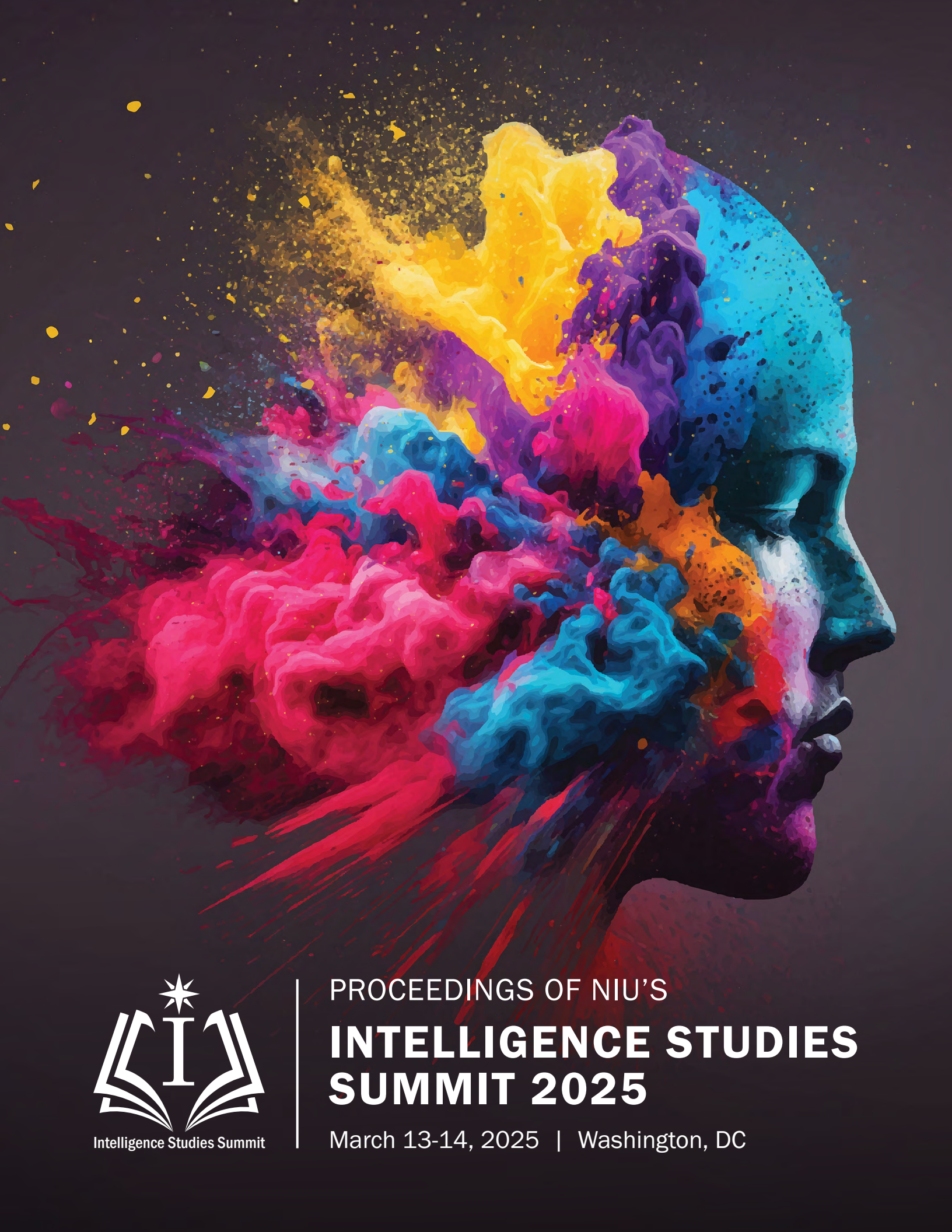


Intelligence Studies Summit

PROCEEDINGS OF NIU'S

INTELLIGENCE STUDIES SUMMIT 2025

March 13-14, 2025 | Washington, DC

PROCEEDINGS OF NIU'S

INTELLIGENCE STUDIES SUMMIT 2025

March 13-14, 2025

Intelligence Studies Summit

National Intelligence University
Washington, DC


Intelligence
Community
Campus
Bethesda

CONTENTS

◀ As the US Intelligence Community's university, NIU holds a unique position as the cornerstone of education, research, and innovation for developing and enriching the intelligence studies discipline now and into the future. NIU students are immersed in a classified learning environment that fosters the development of real-world solutions to national security challenges.

REFLECTIONS ON THE INTELLIGENCE STUDIES SUMMIT BY NIU PRESIDENT JOHN R. BALLARD, PH.D.

I was excited to join all of you as we explored some of the most important and forward-thinking topics in the field of intelligence. Together, we fulfilled an agenda that benefited all of us, with contributions covering a wide range of critical subjects.

Some of the key areas we discussed included the growing roles of technology, artificial intelligence, and cybersecurity, as well as international perspectives on intelligence, the intersection of culture and intelligence, and comparative approaches to teaching intelligence. We also focused on measuring the effectiveness of intelligence; and, of course, we reflected on the critical connection between intelligence and future warfighting. These topics sparked meaningful discussions that will certainly advance our discipline in productive and innovative ways.

Since assuming the role of President of the National Intelligence University, I have been privileged to travel and engage with leaders across the Federal Government about the future of intelligence. These conversations have been overwhelmingly positive, with many officials offering their support for initiatives, such as the Intelligence Studies Summit, and contributing valuable ideas they hope will shape our discussions going forward.

For instance, during a conversation in the Department of the Treasury, senior leaders expressed strong enthusiasm for our work. They highlighted the importance of economic and financial security and emphasized the value of integrating such topics into our efforts to educate the next generation of national security and intelligence professionals.

Another common theme has been improving information sharing across Federal, state, and local governments, as well as extending these efforts to private industry partners and our allies and friends around the world. As businesses continue to play a growing role in developing the hardware and software that supports the Intelligence Community (IC), enhancing collaboration and sharing across sectors is becoming ever more critical. So, there is strong support for efforts such as our Summit across the US Government.

This Summit was a unique and valuable opportunity for us to join together, share ideas, and collaborate in shaping the future of the intelligence profession. By continuing to work together, we can ensure the IC can and will deliver objective, unbiased, and expertly crafted intelligence products that sustain the safety and security of our nation.

Thank you once again for your participation and ideas. I look forward to ongoing engagement with all of you, and to strengthening our network of advocates, as we move forward to advance the study of this vital discipline.

Warm regards,

John R. Ballard, Ph.D.
President

NIU convened its first Intelligence Studies Summit (ISS) in Washington, DC, during March 2025. The ISS aimed to provide a collegial forum for academics and intelligence practitioners to share their research and discuss the intelligence studies discipline and intelligence education.

SUMMIT PANELS AND PRESENTATION ABSTRACTS

PLENARY PANEL: THE CONCEPT AND FUTURE OF INTELLIGENCE STUDIES

The Idea of "Intelligence Studies" in a University

Michael Ard, Ph.D., Johns Hopkins University

Intelligence Studies depends on other disciplines—including history and philosophy, centered on ethics—and needs to focus on core competencies, including writing and research. The roughly 100 Intelligence Studies programs within universities around the United States strive to serve the goal of making the profession better, much like journalism schools. These unclassified Intelligence Studies programs face the challenge of remaining current—including shifts from terrorism to great power competition to homeland security—and of integrating private sector intelligence and artificial intelligence (AI), as well as defending against adversary use of AI.

The Future of Intelligence Studies

Stephen Marrin, Ph.D., James Madison University

Intelligence Studies—that is, developing knowledge of intelligence—is inherently multidisciplinary. The field has changed substantially since Sherman Kent called for an intelligence literature, spurring the creation of several Intelligence Studies journals and making it all the more important to conduct literature reviews to build on prior scholarship. These developments also show the need to internationalize Intelligence Studies and tap the global pool of ideas.

The Future of Intelligence Studies

Michael Goodman, Ph.D., King's College London

Intelligence professionals face a stream of iterative challenges, for which the field of Intelligence Studies should help them prepare. First among these is: How do we define the threat? In addition, hybrid and gray zone conflicts increasingly require us to redefine "war" and "peace," as well as the array of suitable responses and redlines to draw. Does the Intelligence Community (IC) have the correct balance between analysis and collection? The United States and the United Kingdom focus on the short-term—the "tyranny of the tactical"—while our adversaries bring a longer-term perspective. In this environment, how might the IC increase its appetite for risk and develop alternative approaches to tackling threats?

PLENARY PANEL: ORGANIZATIONAL ROLES AND PERSPECTIVES ON INTELLIGENCE STUDIES

Andrew Macpherson, Ph.D., American Political Science Association
Everette Jordan, Association of Former Intelligence Officers
Katherine Pherson, International Association for Intelligence Education
Russ Porter, International Association of Law Enforcement Intelligence Analysts
Melissa Graves, Ph.D., International Studies Association
Christopher Bailey, LLM, SJD, Intelligence Studies Consortium
Spencer French, Society for intelligence History

Striving to foster collaboration among intelligence practitioners and scholars who engage with intelligence-related issues, these organizations also provide expert perspective on the IC's work to media outlets, promote undergraduate and graduate research relevant to intelligence practitioners, and share insights from different academic disciplines and the private sector to improve analytic standards and tradecraft within the IC. They also convene scholars who approach the study of intelligence through a variety of disciplinary perspectives—including science and technology, history, political science, and anthropology—to share knowledge and provide the IC with the broader context it needs to develop improved organizational practices and to refine processes, such as the formulation of collection authorities, in response to the challenges posed by emerging technologies or new forms of media. In addition, these organizations foster scholarship on aspects of the intelligence profession, such as law enforcement, that are sometimes overlooked in academic scholarship on the intelligence profession.

ANALYTIC METHODS AND CULTURES

Do Memory Techniques Have a Place in the Intelligence Analyst's Toolkit?

Cody Herr, US Army

An experiment to test the effect of memory training on intelligence analysis indicates memory training can boost the recall of key details from intelligence reporting. This suggests a link exists between memory optimization and analytic performance. The results infer that a modest IC investment in memory training would better support policymaking.

Preliminary Assessment of Israel's Intelligence Failure: Strategic Surprise and Deception on October 7th

Julia Shufro, The Fletcher School, Tufts University

Fostering a culture of continuous critical review and scenario testing can help IC analysts avoid blind spots and anticipate unconventional threats to national security. Using Israel's intelligence failure of October 7, 2023 as a case study, this paper explores how devil's advocacy—a key tool to address cognitive bias—can guard against strategic surprise. It finds that a failure to imagine enabled Hamas to pull off a deadly

strategic surprise. The attacks are a reminder that humility is imperative for proper preparation and human intelligence is essential to understanding intent.

The Intelligence Community and the Academy: The Imperative of Mutual Learning in an Era of Great Power Rivalry

Daniel Tobin, National Intelligence University

By sharing their intellectual traditions, academia and the IC can build a common road to rigor and relevance. Academia must adopt the IC's redefinition of research from theory building to descriptive inquiry as a foundation for accumulating knowledge about specific countries and regions. The IC must learn from academia that its ultimate product is increasing sense-making capability. Its key task is asking the right questions and then discriminating among competing interpretive frameworks.

Helping Intelligence Analysts Gain Insight

Adrian Wolfberg, Ph.D., Case Western University

A qualitative, interview-based study on how insight emerges identified a four-phase process: 1) a triggering phase of unpredictability, problem finding, and conflicting representations; 2) an emergence phase of internalized tension, priming, and dwell time; 3) an insight phase; and 4) a post-insight phase of resistance, mitigation, and solutions. This process produces four insight archetypes: understanding novel problems; communicating complexity effectively; achieving greater awareness through self-reflection; and navigating organizational politics and agendas.

Innovators, Inflators, and Gisters: A Structural Theory of Intelligence Analysis

Adam Wunische, Ph.D., The George Washington University

Intelligence agencies expend significant resources to train analysts, facilitate discussions, and negotiate disagreements to produce rigorous, logical, and objective analysis. These are neither necessary nor sufficient for producing sound analysis, which arises, instead, from structural conditions that promote rigorous quantitative measurement, objectivity in the face of political pressure, and logical methods that are reproducible and defensible. Analysts and managers must identify the forces shaping their team's culture and adjust practices to maximize its strengths and minimize its weaknesses.

AI AND INTELLIGENCE

Enhancing Scenario Planning Through Human-AI Integration: A Framework for Strategic Intelligence and Foresight

David Kamien, Mind-Alliance Systems, LLC, and Sheila Ronis, Ph.D., University Group Partners, LLC

A new framework for integrating artificial intelligence with human expertise in strategic intelligence foresight showcases the transformative potential of artificial intelligence in intelligence studies. This presentation

proposes a systematic approach to optimizing human-AI collaboration in intelligence analysis that draws from lessons learned from intelligence failures, emerging AI capabilities, and insights from a workshop of former National Intelligence Council leaders and senior IC analysts (www.intelforesight.com), which provided crucial perspectives on implementing AI-enhanced foresight systems while maintaining essential human judgment in strategic intelligence.

Applying Artificial Intelligence for Strategic Warning

Nandita Balakrishnan, Ph.D., Special Competitive Studies Project

The IC's human-led approach to intelligence analysis can be time-intensive and susceptible to bias. This presentation examines how artificial intelligence (AI) and intelligent automation can improve strategic warnings, particularly on China, Iran, North Korea, and Russia. It explores optimal use cases for policymakers, identifies an ideal dataset and model, outlines technical challenges to be overcome, and assesses the costs/benefits of an in-house government capability, procuring an existing industry tool, or staying with the current human-led approach. Finally, it recommends how the IC can quickly and safely integrate AI systems into its strategic warning process.

Accounting for Unexplainable AI in the Intelligence Community

Jason King, Georgetown University

This research develops a generalized framework to address the problem of unexplainability in artificial intelligence that blends user-centric analysis, sociotechnical systems design theory, user needs, and the sliding scale of autonomy against supervision. The framework was used to evaluate the efficacy of artificial intelligence in the US defense, intelligence, law enforcement, and national security agencies. The framework moderately succeeded in identifying user profiles, training data, and some courses of action that either enhanced AI explainability or reduced its need. However, the subjective application of these concepts, especially user needs as explainability goals, and a lack of data on AI models and organizational structure hindered a conclusive application of the framework.

AI and Sensemaking: Why the Knowledge Ecosystem Is More Important

Thomas Pike, Ph.D., National Intelligence University

Today's knowledge ecosystem democratizes artificial intelligence (AI) access and customization. Individuals, with minimal training, can apply AI models to their data to generate novel insights; then a decentralized global network dedicated to problem-solving continuously updates and refines them. This presentation delves into the open source ecosystem, elucidating why this global problem-solving network approach surpasses all others in encoding knowledge and why its methodology bears mathematical resemblance to the workings of deep learning and large language models (subsets of AI). It offers insight into how the IC should reevaluate its acquisition of AI-related technology, the technology literacy of its workforce, and its policy environment.

Deploying Secret Agents for Decision Advantage: The Problem of Accountability

Richard Searle, DBA, Fortanix, Inc.

In great power competition, artificial intelligence (AI) systems create decision advantage. Their natural language processing capabilities can synthesize an overwhelming volume and variety of information. This autonomous agentic capability is vital to achieving a speed of relevance for multidomain operations characterized by confrontation between adversarial AI systems. However, the need for accountability for the quality of intelligence puts humans at the center of the mission given the ambiguity inherent in intelligence tasks, the opacity in the logic of autonomous AI agents, and the potential delegation of responsibility within human-machine interactions. This presentation assesses increasing agentic autonomy in intelligence operations and urges the IC to focus on the importance of accountability in implementing AI systems supporting national security.

TECHNOLOGY IN INTELLIGENCE AND INTELLIGENCE EDUCATION

The Evolving Nature of Emerging Technologies, and Implications for the National Security Arena

Brian Holmes, Ph.D., National Intelligence Council, Office of the Director of National Intelligence

Awareness of emerging technology and its threats and opportunities is growing in both the government and academic realms, with increasing references to scientific and technical intelligence (S&TI) in national security policy documents and law. Technology creates threats beyond weapons, such as foreign adversaries running the cyber environment in which US companies operate. Understanding technology trends, threats, tools, and how to use technology will be part of the future of intelligence analysis because technology is central to geopolitical competition and the economy. Emphasizing the human element, a good S&TI professional needs to be familiar with the technology itself, legal elements, and all facets of economics, politics, and foreign relations in a global context, while also providing deep knowledge in one area. Academic institutions will play a key role in exposing students to these tools and thinking through what skills students need to be good S&TI professionals.

A Brave New World: The Technological Transformation of Conflict and Intelligence

Wesley Moy, Ph.D., Johns Hopkins University

Drones have transformed the conduct of the Russia-Ukraine war, and newer technologies, such as artificial intelligence and quantum computing, will redefine conflict even further—requiring a parallel transformation in intelligence activities. Emerging technologies hold the potential to solve, or at least mitigate, some of the IC's vexing problems—including processing vast quantities of data, maintaining connectivity and communications in remote areas, and acquiring new sources of data. The closed nature of many of its systems has slowed the IC's adoption of new technologies, leaving some IC entities unable

to support advanced systems and making it difficult to compete with the private sector for talented technology personnel.

INTELLIGENCE BEYOND GOVERNMENTS

National Intelligence: Present and Future Challenges for Enterprises in the Era of Rising Technology

Manuel Balcázar, DPA, Center for Studies on Security, Intelligence, and Governance (CESIG), Technological Institute of Mexico (ITAM)

Greater global uncertainty will challenge budget-strapped intelligence services already juggling intensifying traditional threats and new emerging risks. Add to that organized crime, which—in various forms—threatens governments and corporations alike. A strategic alliance among the intelligence agencies of democratic governments and an emerging crop of legitimate private sector intelligence entities could mitigate these adverse trends by protecting core activities and addressing emerging threats, such as cyberthreats, money laundering, electronic illegal markets, and both virtual and physical terrorism. Such joint efforts could enhance intelligence capabilities within major corporations, promote an intelligence-oriented culture, and strengthen partnerships with businesses to navigate 21st century uncertainties more effectively.

Network-Centric Professional Development: Intelligence Associations in the Global Century

James Ellsworth, Ph.D., University of New Mexico

This session revisits the author's 2006 paper in the *American Intelligence Journal* that outlines a strategy to professionalize the intelligence workforce by leveraging not-for-profit intelligence professional associations as a multiplier for official US Government intelligence education and training. Professionalization remains an important vehicle for safeguarding technical competence and ethical practice in times when funding and/or political constraints might threaten the maintenance of standards crucial to the defense of both the security of the nation and the liberties of its people.

Bridging the Divide: Integrating Corporate Geopolitical and Strategic Intelligence Programs into National Security and Intelligence Studies

Angela Miller Lewis, Ph.D., Georgetown University

Private sector intelligence teams have robust capabilities that can offer valuable insights to government agencies. This presentation proposes integrating corporate intelligence practices into academic curricula and national security operations, advocating for a more collaborative and holistic approach to intelligence gathering. It explores how corporate intelligence teams—with their access to on-the-ground intelligence in conflict zones, commercial threats, and regional instability—can provide critical insights to national security agencies and vice versa. Drawing on case studies of major global events, the presentation highlights the potential for public-private partnerships in intelligence sharing to enhance national security.

MEASURING INTELLIGENCE EFFECTIVENESS

Does Intelligence Pay? Assessing Information Advantages in Declassified Intelligence Briefings

Austin Carson, Ph.D., University of Chicago

To assess whether intelligence reporting provides novel and more useful information than mainstream news reports, we compared 5,000 President's Daily Briefs (PDB) to 370,000 foreign affairs articles in the *New York Times* to assess each source's relative success in anticipating coups. The PDB was substantially more likely to discuss domestic tension and relevant political actors in countries that experience an attempted political coup, mentioning the country multiple months before a coup attempt; the *Times* only two days before the event. The PDB's informational advantage is not uniform. It provides better early warnings when the coup attempts are harder to observe and when the country is embroiled in a civil war, but its advantage falls in countries where the *Times* has a foreign bureau. This novel methodology for measuring private information offers a rare test of the value-added of massive investments in intelligence bureaucracies made by modern states.

Usefulness and Accuracy in the President's Daily Brief

Thomas Dolan, Ph.D., University of Central Florida

This paper investigates when estimates in the President's Daily Brief (PDB) are more likely to be accurate and useful. Using declassified PDBs from 1960 to 1980 and stated probability, subject, region, and time horizon variables, we assess when estimates are more likely to be accurate and useful—operationalized as similar information appearing in the *New York Times* within a week of PDB publication. Results suggest: (1) current intelligence estimates are more likely to be correct than future estimates; (2) most also appear in the *Times*; (3) estimates involving military issues and other countries' domestic politics are less likely to be correct than estimates about other topics; and (4) the stated probability of a future event occurring was statistically unrelated to its actual probability of occurring.

INTELLIGENCE AS KNOWLEDGE PRODUCTION

Definitions of Intelligence: Public, Academic, and Institutional Perspectives in Türkiye

Yenal Göksun, National Intelligence Academy, Turkey

How intelligence is defined varies across countries, services, and cultures—offering clues about how it is practiced. But definitions can also vary within the same culture. This presentation examines institutional, academic, and public perspectives on the concept of intelligence in Türkiye and the interactions among these perspectives to identify commonalities/differences and the dynamics behind them. The institutional perspective—obtained through institutional definitions, activity reports, and other official sources—examines the culture of the intelligence service. Under the academic perspective, the literature on intelligence studies in Türkiye unveils differing approaches to the concept. Last, media representations and public discourses determine the public's approach to intelligence, which is significant because of its impact on intelligence ethics and oversight.

Philosophy and Intelligence Studies: Giving Intelligence Studies a Theoretical Foundation

MAJ Joshua Roling, Ph.D., Joint Task Force-North

Among the discoveries that led to quantum mechanics, German physicist Werner Heisenberg brought to light a paradox: the more one knows about the position of an electron, the more uncertain the observer is about its momentum, and vice versa. His "uncertainty principle" compelled a rethinking of not only its scientific, but also its philosophical implications. This suggests intelligence studies—now centered on tradecraft, IC history, and national security policy—should focus on methods of questioning—enriching curricula with philosophical works that consider what it means to question, to observe, and to know. Current intelligence studies address the practical application of intelligence but lack the theoretical foundation to enable students to question assumptions they may consider immutable.

The Intelligence Community Is Broken: A Roadmap To Achieve Real Analytical Reform

Kathleen Vogel, Arizona State University

Many studies call attention to US intelligence failures and the need for intelligence reform, but proposed solutions are largely organizational, technological, or outsourcing fixes that do not get at the root of these analytic failures. Despite the billions invested, reforms implemented after 9-11 and the 2003 Iraq War have failed to create the robust research capability needed for knowledge-generation within the IC because it has not given priority to developing, maintaining, and improving its strategic research capabilities. We will examine the roots of the problem and propose a way to rebuild the IC's strategic research capability.

INTELLIGENCE STUDIES AS A PROFESSIONAL AND ACADEMIC DISCIPLINE

Making the Case for Intelligence Studies as an Academic Discipline: Praxis, Discipline, and the Challenge of Collective Efficacy

Stacey Pollard, Ph.D., Director, Ann Caracristi Institute for Intelligence Research, National Intelligence University

Intelligence studies faces a persistent puzzle: despite its growing institutional presence and relevance to international security, the field has yet to be recognized as a distinct academic discipline. Intelligence studies meets core disciplinary criteria in ontology, epistemology, and institutional support, but falls short in methodology, with limited application of systematic empirical research. Employment of a dialectical framework, highlighting the dynamic interplay between praxis and discipline, shows that this methodological weakness stems both from its practitioner-driven origins and from a lack of collective efficacy among scholars, which has hindered consensus on shared standards and cumulative knowledge-building. Intelligence studies must strengthen its methodological foundations and develop greater scholarly cohesion to mature into a robust academic discipline.

Capturing and Sharing First-Hand Accounts for Improving Intelligence Performance

Peter Usowski, Center for the Study of Intelligence (Ret.)

This presentation focuses on the efforts made inside and outside the CIA to capture and share the experience and expertise of current and former intelligence leaders and practitioners. These first-hand accounts have served as important sources for the study of intelligence and the ongoing education of intelligence professionals.

INTELLIGENCE STUDIES AND THE CYBER DOMAIN

Updating Digital Literacy: Achieving Curricular Upgrades To Elevate Technology and Cybersecurity Education for Homeland Security Intelligence Students and Professionals

Michelle Black, Ph.D., University of Nebraska at Omaha

An in-depth analysis of education and training in the technology and cybersecurity fields within Department of Homeland Security (DHS) found that few analysts are taking advantage of free courses offered by government agencies. This presentation offers actionable recommendations to alleviate technological issues that deter usage and provides an updated curriculum roadmap for DHS to ensure digital literacy for its students and professionals to maintain a competitive workforce that is adept at identifying new and existing threats to the homeland.

Exploring the Evolution of Cyber Intelligence (CyINT): A Disciplinary Debate and Practical Implications for Intelligence Professionals

James Austin and Yongkuk Cho, NATO Cooperative Cyber Defence Centre of Excellence

This presentation examines the redevelopment of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) Cyber Threat Intelligence (CTI) course into a cyber for intelligence professionals course. Recommendations are included on effective methodological approaches to imparting CyINT knowledge to the broader Intelligence Community.

EDUCATING FUTURE INTELLIGENCE PROFESSIONALS

The Rise of Intelligence Studies in the South: Lessons from The Citadel, the Military College of South Carolina

Frank Emerson, JD, and Muhammad Fraser-Rahim, Ph.D., The Citadel

In 2017, The Citadel, the military college of South Carolina, created a Department of Intelligence and Security Studies to create a next-generation workforce with expertise and skills in the intelligence domain. Students gain knowledge in tradecraft and the intelligence profession in preparation for careers in

intelligence or graduate studies in security-affiliated fields. This presentation provides insights into the program's conception, academic focus, experiential learning, and future that have given rise to an intelligence Mecca emerging out of the American South.

Centers in Intelligence Education: A Comparative Perspective

Jonathan Smith, Ph.D., Coastal Carolina University

Using a comparative case study approach, this research explores the development and operation of intelligence education centers (and comparable institutional structures) across the Anglosphere. The intent is to explore the degree of similarity in motives for creating and operating such programs and what country-specific factors might explain variations between the cases.

INTERNATIONAL PERSPECTIVES AND PARTNERSHIPS

Reconsidering Intelligence Studies Research and Education Among the Five Eyes

John Blaxland, Ph.D., Australian National University

As in the United States, the intelligence discipline in the fellow Five Eyes partners—Australia, Canada, New Zealand, and the United Kingdom—has been transforming. This presentation examines the important and complementary role these close partners have played—from the Second World War to the present—with an eye toward what the future may hold. It draws on the presenter's experience as a military intelligence officer, his teaching ("Honeypots and Overcoats" on Five Eyes intelligence) and his extensive scholarship.

Building the Intelligence Community: National Intelligence Academy

Talha Köse, Ph.D., National Intelligence Academy, Turkey

Türkiye's recent creation of a National Intelligence Academy is indicative of Ankara's commitment to engage in theoretical debates and contribute to scientific advancements in the intelligence domain. This presentation discusses the role of the Academy in building a Turkish intelligence community and the creation of mechanisms to foster interdisciplinary collaboration among academics, experts, students, and others engaged in intelligence-related work. By integrating these various stakeholders, the National Intelligence Academy aims to function as a dynamic hub for the exchange of ideas, methodologies, and innovations.

Intelligence Education in Transition: A Comparative Study of Iraq, Egypt, and Morocco

Muhanad Seloom, Ph.D., Doha Institute for Graduate Studies

This presentation explores how Egypt, Iraq, and Morocco are modernizing their intelligence training to address contemporary security challenges and how international partnerships, especially with the United

States, have shaped intelligence education in these countries. It considers the challenges of incorporating technological advancements and ethical concerns into the curriculum. It argues that intelligence education reform is crucial for enhancing operational effectiveness, promoting accountability and transparency, and contributing to the broader global intelligence architecture.

A Deeper Shade of Red

Robert Levine, Ph.D., Johns Hopkins University

US civilians and officers acting as foreign national or military leaders in war games often make decisions that are hard to distinguish as "foreign." How can we better prepare officers and civilians for playing these roles? This presentation explores four rings of information that would help. The outermost requires learning the ideology, history, and contours of a country's society to offer perspective. Next is specialization—studying a culture from within a discipline, such as politics, economics, or military, where immersion can yield profound insights—followed by a focus on the nuts and bolts of how the foreign organization operates. The innermost ring requires a mirror—how might what are we are doing be seen and interpreted by foreign entities.

History and Culture in Intelligence Analysis

Ioannis Kotoulas, Ph.D., University of Athens, Greece

Combining intelligence analysis with history deepens policy proposals and strategic thinking. Both intelligence analysts and historians rely on fragmentary data to weave a coherent story and need historical and cultural knowledge to understand a country or region to make informed predictions. Ukraine provides a case study on the importance of knowing history and culture when crafting intelligence analyses. Understanding the war requires knowing its geopolitical and historical context, the entangled symbiosis of Russians and Ukrainians, and the erroneous perceptions of Russian revisionism that underpinned the decision to invade and the expectation of easy victory. The positivist contribution of intelligence analysis can reduce the danger of essentialism inherent in historical perspectives.

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

Anthony Ioannidis, Ph.D., and Anastasios-Nikolaos Kanellopoulos
Athens University of Economics and Business, Greece

Rooting intelligence studies in business administration and cutting-edge technologies would prepare students for specialized tactical and strategic intelligence roles while fostering innovation in global security. Business administration prioritizes strategic planning, organizational leadership, and operational efficiency. Artificial intelligence, big data analytics, and cybersecurity give students market-relevant expertise that would ensure intelligence studies stay competitive. Converting the National Intelligence University into a mega-university would expand its ability to provide experiential learning and real-world

problem-solving opportunities in a classified environment. Collaborating with private enterprises, public institutions, and international allies would create a pipeline of highly skilled professionals able to address emerging security challenges.

INTELLIGENCE AND FUTURE WARFARE

How Much Intelligence Is Enough to Support Large-Scale Combat Operations?

Elizabeth Coble, US Army Command and General Staff College

In the wake of the Global War on Terrorism, the US military is refocusing on large-scale combat operations. How should the Intelligence Community respond? What doctrine, organizational, process, and policy changes need to occur? Should the United States strengthen intelligence-sharing agreements beyond the Five Eyes or bilateral alliances? Two case studies assess these questions. The first looks at Britain's 21st Army Group in August/September 1944 to assess if it had a clear enough picture of German military capabilities to continue operations? The second looks at multinational intelligence operations in 2006 to support the Republic of Korea/US Combined Forces Command. Was the intelligence enough? Does the type of intelligence influence leaders' trust in the reporting? How do classification and dissemination procedures affect what is made available to senior leaders?

War Without Fear: Transforming Intelligence and Strategy in the Era of Lethal Autonomous Weapons

LTC Mark Askew, US Army, Futures Command, and Antonio Salinas
Georgetown University and National Intelligence University

The proliferation of lethal autonomous weapon platforms will transform the character of warfare. Autonomous systems' lack of fear fundamentally alters our calculus of offense, defense, and strategic risk. Lethal autonomous weapons can execute operations without hesitation, enabling bold offensive strategies and unyielding defensive postures previously limited by human vulnerabilities. Adversaries may believe they must counter with equally aggressive tactics. The emergence of a new era defined by systems that operate without fear will force us to reassess how we teach intelligence studies and perform assessments. Intelligence professionals must master the traditional understanding of fear and human behavior in conflict to be able to evaluate the implications of fearless warfare tools.

FUTURE OF INTELLIGENCE STUDIES: SELECT PAPER

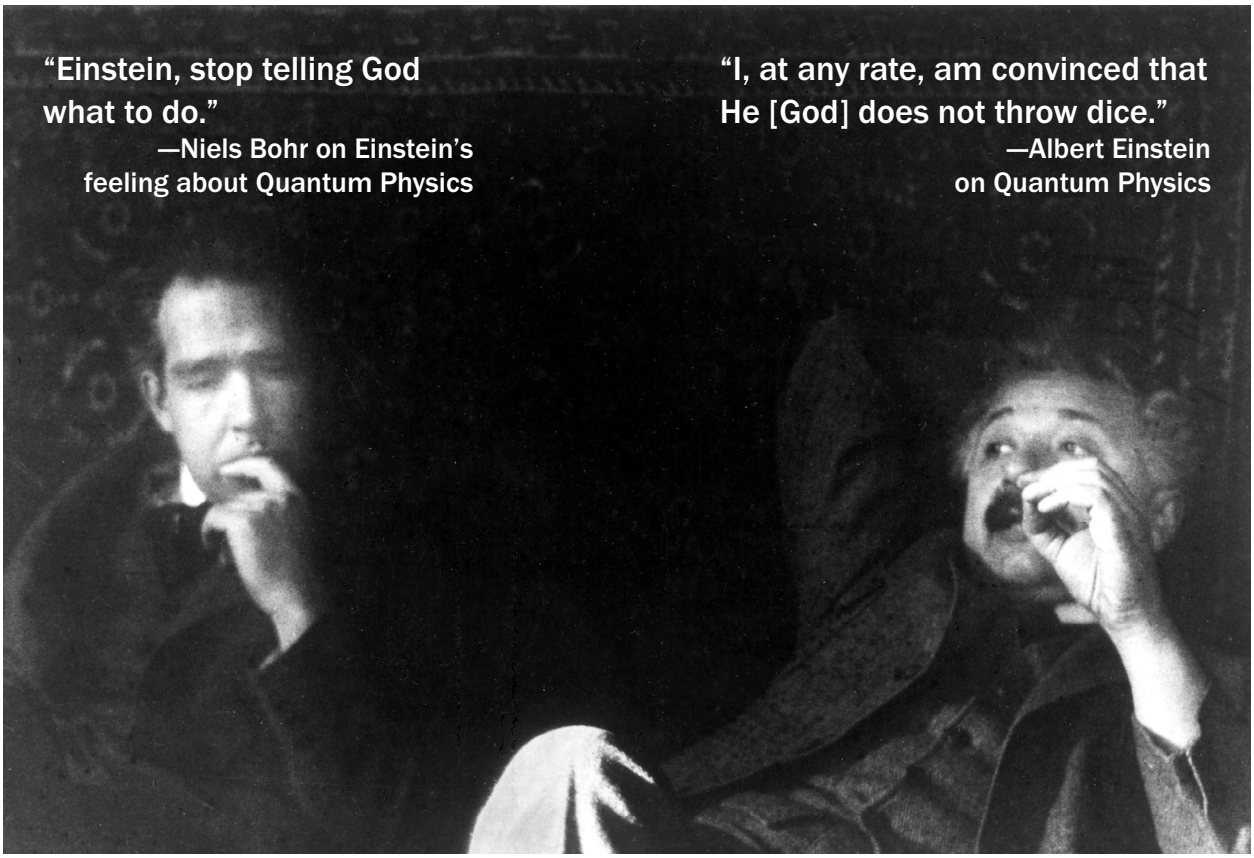
STOP TELLING GOD WHAT TO DO: Enriching Intelligence Studies with Philosophy Curriculum

Joshua Roling

In 1926, Albert Einstein had a problem. A year earlier, a young physicist named Werner Heisenberg threatened the assumptions on which the aging scientist understood the universe. Working day and night, Heisenberg discovered the foundational roots of what we now call quantum mechanics, which unveiled a curious paradox: the more one knows about the position of an electron, the more uncertain the observer is about its momentum. Conversely, the more certain one is about the electron's momentum, the less sure the observer is about its position. Later termed the *uncertainty principle* (1927), Heisenberg's discovery compelled his contemporaries to consider not only the scientific but also the philosophical implications of his work. As he aged, Einstein increasingly refused to rethink the conceptual grounding of science, admonishing the new physicists that "God does not play dice with the universe." Willing to abandon long-held assumptions, physicists of the new school broke with their venerated predecessor. Niels Bohr, mentor and collaborator of Heisenberg, retorted that Einstein ought to "stop telling God what to do."[1]

Bohr's reproof was not so much a criticism of Einstein's faith as it was a reproach of his unwillingness to engage in the conceptual underpinning of science. Einstein implied that there are immutable assumptions that governed the universe, which like God are infallible, infinite, unquestionable. Heisenberg, on the other hand, seemed willing to jettison any assumption. The son of a professor of Greek philology and avid reader of Plato in his youth, Heisenberg understood the symbiotic relationship between conceptual and empirical thinking, leading him to declare in his 1958 book, *Physics and Philosophy,* that "what we observe is not nature itself, but nature exposed to our method of questioning."[2]

This paper proposes that intelligence studies ought to focus more on the methods of questioning that make possible our observations of nature. To do so, I propose enriching the curriculum of intelligence studies with philosophical works that consider, at the atomic level of conceptual thinking, what it means to question, to observe, and to know. In its current form, intelligence studies focuses primarily on intelligence tradecraft, history of the Intelligence Community (IC), and national security policy. While these valuable areas focus on the practical application of intelligence, they lack the theoretical foundation to enable students to question assumptions they may consider immutable about their profession. Just as



Source: Publicly available image of Niels Bohr and Albert Einstein, https://commons.wikimedia.org/wiki/File:Niels_Bohr_Albert_Einstein3_by_Ehrenfest.jpg.

Heisenberg imbued physics with philosophy to make his discoveries possible, I propose that intelligence studies adopts the works of philosophy to grant students the ability to understand the conceptual underpinning of empirical experience and observation.

To explain how philosophy will enrich both the study and application of intelligence, I must enter the dangerous territory of defining it. Rather than attempt to encapsulate every characteristic of intelligence, I shall propose what I consider one reasonable definition. Fundamentally, the act of intelligence is an effort to know and understand objective reality through subjective observation to enhance national security. Every collection discipline attempts to understand reality and then to communicate that understanding to someone for a decision or action. Yet we all know how difficult that can be. We have so many collection disciplines, and we demand that one corroborate another, because we recognize that every means of collection mediates the observer's understanding of reality, offering a necessarily incomplete and sometimes misleading perception.

Questions concerning the mediation of experience and objectivity raise important epistemological questions which, luckily for students of intelligence, have been debated for millennia. Philosophers of

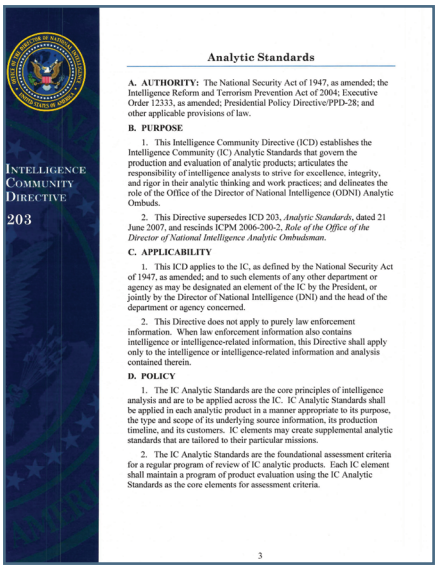
epistemology concern themselves with what it means to know and the methods with which we obtain knowledge. For instance, Plato tells us of men chained within a cave since their birth, heads bound to look only straight in front of them. Unbeknown to the bound men, others behind them make shapes behind a lit fire, casting shadows before the prisoners' eyes. The bound men believe these shadows to be reality, since they know of nothing else. One day, a prisoner escapes the cave, goes outside, and discovers the objective truth of the world. Returning to the cave to inform his fellow prisoners, the bound men think the enlightened subject has gone mad and cast him from their community. From this analogy we discover important variables to Plato's investigation of reality and observation. The escapee discovers the truth not through his senses, which introduce miscalculation and manipulation. Instead, he discovers the truth through a quest for enlightenment and, in Plato's telling, a closeness to God. Plato's conception of objective truth is therefore the product of one's personal rationality, education, and spiritual enlightenment.[3]

Plato's analogy precedes the thinker most responsible for the Western conception of objectivity and truth: René Descartes. Descartes presents a provocative thought experiment chiefly concerned with the question: how do I know that I exist? Extending that question further, he asks: how do I know anything exists? Descartes suggests a trinity in which humankind can observe and attain knowledge of the world: the self, God, and the external world. Commonly termed the "Cartesian Split," Descartes formalized the conceptual foundation of modern science, epistemology, and intelligence: the division between the subjective self and an external, objectified reality that exists independently of our observations.[4]

Empiristic philosophers challenged Descartes' neat division between the self and objectified reality. John Locke, George Berkeley, and David Hume argued that knowledge of objective reality accrued primarily through personal experience, either in the form of a subjective sensation or reflection.[5] When we observe the world, according to the empiricists, we do not observe reality in the way it *actually exists,* but rather the way in which the senses of our mind understand it. A radical skeptic, Hume suggested that human perception is limited by the fleeting nature of the subjective self and its passions. Our conception of reason and rationality is therefore a fiction of the mind, leading Hume to proclaim that "reason is, and ought only to be, a slave of the passions."[6]

Awakened and alarmed by the empiricist's skepticism, Immanuel Kant produced a new epistemological framework within his seminal work, *Critique of Pure Reason.* In this book, Kant suggests that humanity can indeed observe reality because there exists innate knowledge that he calls *a priori* knowledge. Refuting Hume and the empiricists, Kant argues that an observer possesses both empirical knowledge gained from senses and *a priori* knowledge innately programmed into the human psyche. Moreover, the observer can take empirical knowledge and deduce patterns through logic, overlaying analytical capability to bridge the divide between empirical and *a priori* understanding.[7]

The philosophical implications of these works address the core concerns of intelligence studies and tradecraft, illuminated most directly within Intelligence Community Directives (ICD). For instance, ICD 203 outlines analytical standards meant to generate "excellence, integrity, and rigor" of IC analysis. ICD 203 implicitly endorses Descartes' Cartesian partition by demanding that analysts produce



INTELLIGENCE COMMUNITY DIRECTIVE 203

Analytic Standards

A. AUTHORITY: The National Security Act of 1947, as amended; the Intelligence Reform and Terrorism Prevention Act of 2004; Executive Order 12333, as amended; Presidential Policy Directive/PPD-28; and other applicable provisions of law.

B. PURPOSE

1. This Intelligence Community Directive (ICD) establishes the Intelligence Community (IC) Analytic Standards that govern the production and evaluation of analytic products; articulates the responsibility of intelligence analysts to strive for excellence, integrity, and rigor in their analytic thinking and work practices; and delineates the role of the Office of the Director of National Intelligence (ODNI) Analytic Ombuds.

2. This Directive supersedes ICD 203, *Analytic Standards*, dated 21 June 2007, and rescinds ICPM 2006-200-2, *Role of the Office of the Director of National Intelligence Analytic Ombudsman*.

C. APPLICABILITY

1. This ICD applies to the IC, as defined by the National Security Act of 1947, as amended; and to such elements of any other department or agency as may be designated an element of the IC by the President, or jointly by the Director of National Intelligence (DNI) and the head of the department or agency concerned.

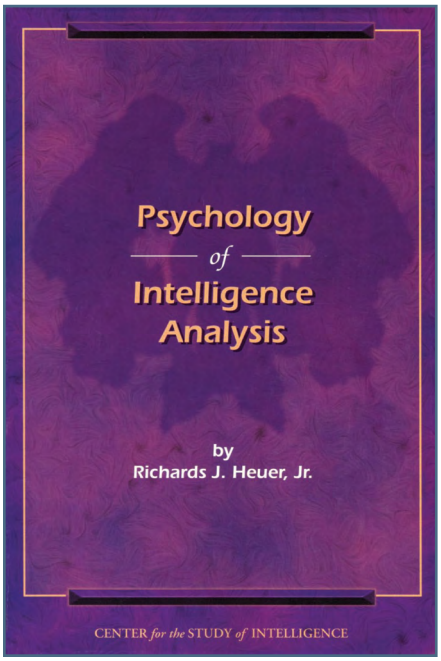
2. This Directive does not apply to purely law enforcement information. When law enforcement information also contains intelligence or intelligence-related information, this Directive shall apply only to the intelligence or intelligence-related information and analysis contained therein.

D. POLICY

1. The IC Analytic Standards are the core principles of intelligence analysis and are to be applied across the IC. IC Analytic Standards shall be applied in each analytic product in a manner appropriate to its purpose, the type and scope of its underlying source information, its production timeline, and its customers. IC elements may create supplemental analytic standards that are tailored to their particular missions.

2. The IC Analytic Standards are the foundational assessment criteria for a regular program of review of IC analytic products. Each IC element shall maintain a program of product evaluation using the IC Analytic Standards as the core elements for assessment criteria.

3



"objective" analysis—sanctioning Descartes' understanding of a self capable of observing an objectified reality. The ingredients of objectivity are the observer's awareness of her assumptions and biases, alongside reasoning techniques designed to mitigate the influence of impertinent assumptions.[8]

While guidelines are effective in governing behavior, they lack the conceptual grounding to enable creative and investigative thought. By studying guidelines without their philosophical grounding, students are at risk of, to paraphrase a line from Frank Herbert's *Dune,* knowing something by heart without knowing the heart of it.[9] Students of intelligence know what to do and how to behave but do not investigate why, at the theoretical level, ICD 203's guidelines are so crucial. The inclusion of philosophical grounding would enable students to interrogate the so-called *a priori* assumptions that undergird the IC's current prescription of safeguards and analytical techniques. As both Einstein and Heisenberg show us in the world of physics, breakthroughs in the techniques within certain disciplines require a conceptual rather than empirical revolution. To have such a revolution, one must examine assumptions rather than accept them as immutable facts. Reading and discussing foundational works of philosophy enable such an examination to occur, leading to the possibility of conceptual breakthroughs in the future.

Scholars of intelligence studies often attempt to encapsulate what characteristics define an academic discipline, and to answer the question if intelligence studies exists as a true one. Each discipline, however, evolves and contributes to others, eventually increasing our awareness across multiple fields of natural science. For instance, physics required chemistry to understand quantum mechanics. Biology required history to discover the theory of evolution. Richards Heuer's *Psychology of Intelligence Analysis* brought to bear the mature field of psychology to the more nascent discipline of intelligence analysis. Heuer's publication demonstrated how foundational knowledge of one field can lead to conceptual breakthroughs of another. This study recommends that developers of intelligence curriculum employ the foundations of philosophy to enrich the conceptual possibilities of intelligence studies. Students deserve an education in which they can examine the assumptions which guide their profession. This examination makes visible and mutable assumptions that they may have considered infallible, infinite, and unquestionable, so that students of intelligence can follow the advice of Niels Bohr and "stop telling God what to do."

MAJ Joshua Roling is an active-duty strategic intelligence officer in the Army. He began his Army career as Long-Range Surveillance Detachment Leader and Executive Officer with C/52nd Long Range Surveillance (LRS) Company at Joint Base Lewis-McChord, where he deployed as an augmentee to 2nd Battalion, 75th Ranger Regiment, to Bagram, Afghanistan. After transitioning to military intelligence, MAJ Roling served as Brigade Assistant and Squadron Intelligence Officer at the 101st Airborne Division (Air Assault), where he deployed to North Africa in support of Special Operations Command-Africa. Subsequently, MAJ Roling taught English composition and literature at the United States Military Academy at West Point for three years. He currently serves as the Intelligence Plans and Policy Branch Chief at Joint Task Force-North.

MAJ Roling is a graduate of the US Army Ranger School, Air Assault School, and Airborne School. He obtained a B.S. from the United States Military Academy at West Point, an M.A. and Ph.D. in English from Vanderbilt University, and an M.S. in Science and Technology Intelligence from the National Intelligence University in Bethesda, MD.

ENDNOTES

1. William Egginton, *The Rigor of Angels: Borges, Heisenberg, Kant, and the Ultimate Nature of Reality* (Pantheon Books, 2023).
2. Werner Heisenberg, *Physics and Philosophy: The Revolution in Modern Science* (Harper Perennial, 2007).
3. Plato, *The Republic,* trans. G. M. A. Grube, rev. C. D. C. Reeve (Hackett Publishing Company, 1992).
4. René Descartes, *Meditations on First Philosophy,* trans. Donald A. Cress (Hackett Publishing Company, 1993).
5. John Locke, *An Essay Concerning Human Understanding,* ed. Peter H. Nidditch (Clarendon Press, 1975).
6. David Hume, *An Enquiry Concerning Human Understanding,* ed. Eric Steinberg (Hackett Publising Company, 1993).
7. William Egginton, *The Rigor of Angels: Borges, Heisenberg, Kant, and the Ultimate Nature of Reality* (Pantheon Books, 2023), 60.
8. Office of the Director of National Intelligence, Intelligence Community Directive 203 *(Analytic Standards),* June 2007, https://www.dni.gov/files/documents/ICD/ICD-203.pdf.
9. Frank Herbert, *Dune Messiah* (Berkley Books, 2008).

FUTURE OF INTELLIGENCE STUDIES: SELECT PAPER

DO MEMORY TECHNIQUES HAVE A PLACE IN THE ANALYST'S TOOLKIT?

Cody Herr

This article presents the findings of an experiment to test the effect of memory training on intelligence analysis. The results indicate a significant relationship between memory training and a boost in recall of key details from intelligence reporting. This strongly suggests a link between memory optimization and analytic performance. Overall, this article recommends a modest IC investment in memory training to better support policymaking.

Memory is a core component of human cognition and an essential skill for intelligence analysis. Analysts rely on memory for every facet of their job—from evaluating vast amounts of data to briefing and answering policymakers' questions. Recent studies in psychology and neuroscience show that memory training can improve cognitive performance. Top universities, tech companies, special operations units, and foreign intelligence services require memory testing and training. Yet, the US Intelligence Community (IC) does not provide its workforce with memory testing, education, or training.

The IC places tremendous demand on the intelligence analyst's memory. The measure of an analyst is determined in large part by their ability to recall details quickly and accurately. Thus, the IC's effectiveness is linked to the individual analyst's memory. The IC trains its analysts to mitigate cognitive biases but does not train them to improve cognition. Analysts develop expertise through education and experience but do not learn to optimize their memory to use that knowledge. The result is inconsistent performance across the IC workforce. This inefficient system lowers the quality of intelligence analysis provided to policymakers.

This article seeks to modestly advance Heuer and Sinclair's work on the role of memory in intelligence analysis. It is the first academic work to test the memory tasks associated with intelligence analysis and the first memory study to involve IC members. It is also the first study to train memory strategies to improve analysts' performance and, thereby, the analysis provided to policymakers.

Intelligence analysts must contend with ever-increasing amounts of information. They risk cognitive overload even as they use artificial intelligence and machine learning. Improved human memory can reduce this burden by optimizing information organization and recall skills—freeing up mental resources for critical and creative

thinking—tasks only humans can perform. As Sherman Kent noted, "Whatever the complexities of the puzzles we strive to solve, and whatever the sophisticated techniques we may use to collect the pieces and store them, there can never be a time when the thoughtful man can be supplanted as the intelligence device supreme."[1]

Improving the cognition of analysts formed an important part of the intelligence literature in the 1980s and 1990s. Richards Heuer devoted an entire chapter of *The Psychology of Intelligence Analysis* to memory improvement. He began this chapter claiming: "Differences between stronger and weaker analytical performance are attributable in large measure to differences in the organization of data and experience in analysts' longer-term memory."[2] Similarly, Robert Sinclair explored methods to harness heuristics and memory techniques to overcome memory's limitations in his groundbreaking 1984 *Center for the Study of Intelligence* monograph, "Thinking and Writing: Cognitive Science and Intelligence Analysis."[3]

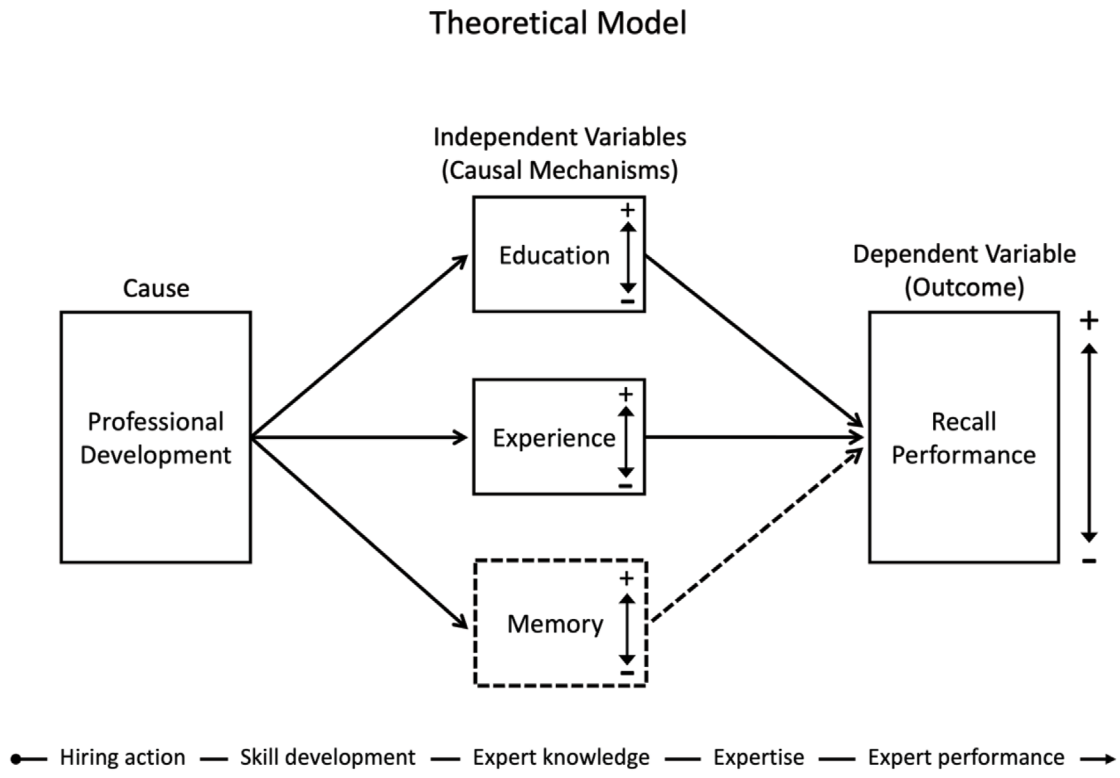
This article seeks to modestly advance Heuer's and Sinclair's work on the role of memory in intelligence analysis. It is the first academic work to test the memory tasks associated with intelligence analysis and the first memory study to involve IC members. It is also the first study to train memory strategies to improve analysts' performance and, thereby, the analysis provided to policymakers.

THEORY

We theorize that intelligence analysts' performance is a function of three independent variables. The first independent variable is education, which involves Intelligence Community Directives (ICD), analytic tradecraft, product creation, and briefing. The second independent variable is experience, which involves on-the-job practice and deployments. The third independent variable is memory, which involves encoding, organizing, and recalling the knowledge gained from education and experience. All three independent variables must be highly present for optimal analyst performance. Memory optimization is lacking in the IC, which results in inconsistent overall performance. This inconsistent performance results in suboptimal intelligence analysis provided to policymakers.

Intelligence analysts are not trained to optimize their memory to gain a return on investment in education and experience. Simply put, analysts do not learn how to learn. This is a gap in IC professional development.

Intelligence analysts receive education in IC doctrine and tradecraft as part of their professional development. They gain experience in the office and in the field. However, the IC does not train its analysts on how to encode and recall what they have learned. Intelligence analysts are not trained to optimize their memory to gain a return on investment in education and experience. Simply put, analysts do not learn how to learn. This is a gap in analyst professional development. Therefore, we assume the variables of education and experience are present and adequate causal mechanisms of the dependent variable of recall performance. Thus, we focused solely on the independent variable of memory. Specifically, we focused on memory's impact on recall performance, which is the dependent variable of the experiment.



DATA COLLECTION

We used a posttest-only control group experiment to test the hypothesis that memory training increases intelligence analysts' ability to recall key details, thereby improving their performance. The experiment subjects were randomly divided into two study groups: a memory training group and a control group. The memory training group received training on mnemonic devices that use mental imagery and spatial contextualization—specifically elaborative encoding, the major system, and the memory palace. The control group received no training. Both groups were tested with the same instrument. The testing involved both groups reviewing notional unclassified intelligence reporting containing 15 sequential pairings of actors with actions. After five minutes, participants were tested on their ability to match the actors and actions in the correct sequence. One week later, both groups were retested with the same instrument to gauge long-term memory retention of the material. All participants completed a demographic survey to identify moderating variables that could impact the results.

Data collected from the tests and surveys were used to determine if memory training increased analysts' ability to recall key details from reporting. Differences between the memory training group and control group were analyzed statistically via the t-test and Analysis of Variance (ANOVA) methods to interpret the results. The threshold for statistical significance was a p-value below 0.05. In other words, for the differences in mean values to be considered significant, at least 95 percent confidence that they are not due to random chance is required.

PARTICIPANTS

All 30 participants in this study were National Intelligence University (NIU) graduate students, US Federal employees, and active members of the IC. Every participant self-identified as an intelligence analyst or an intelligence officer with experience performing intelligence analysis. All participants completed a ten-week refresher course on intelligence analysis at NIU approximately two weeks before the experiment. Participants ranged in age between 26 and 43, with a mean age of 33. Fourteen participants self-identified as female (46.6 percent), which is in line with the 2022 Federal workforce and civilian labor force female ratios of 45.0 percent and 46.7 percent, respectively.[4] Military members of the IC comprised 56.6 percent of participants. Approximately one-third of participants (30 percent) claimed prior exposure to memory techniques in their personal experience. This ratio provided suitable variance to test the impact of prior exposure to memory techniques on recall performance and durability in this study. The study's sample size and variance were sufficient to perform ANOVA and t-tests.

Demographics								
Study Group	**n**	**Female (%)**	**Age (mean)**	**Advanced degree (%)**	**Experience in years (mean)**	**Prior exposure to memory techniques (%)**	**Occupation (analyst/ officer)**	**Military (%)**
Memory Training	15	7 (46)	32	4 (26)	6	5 (33)	7/8	9 (60)
Control	15	7 (46)	35	3 (20)	9	4 (26)	7/8	8 (53)

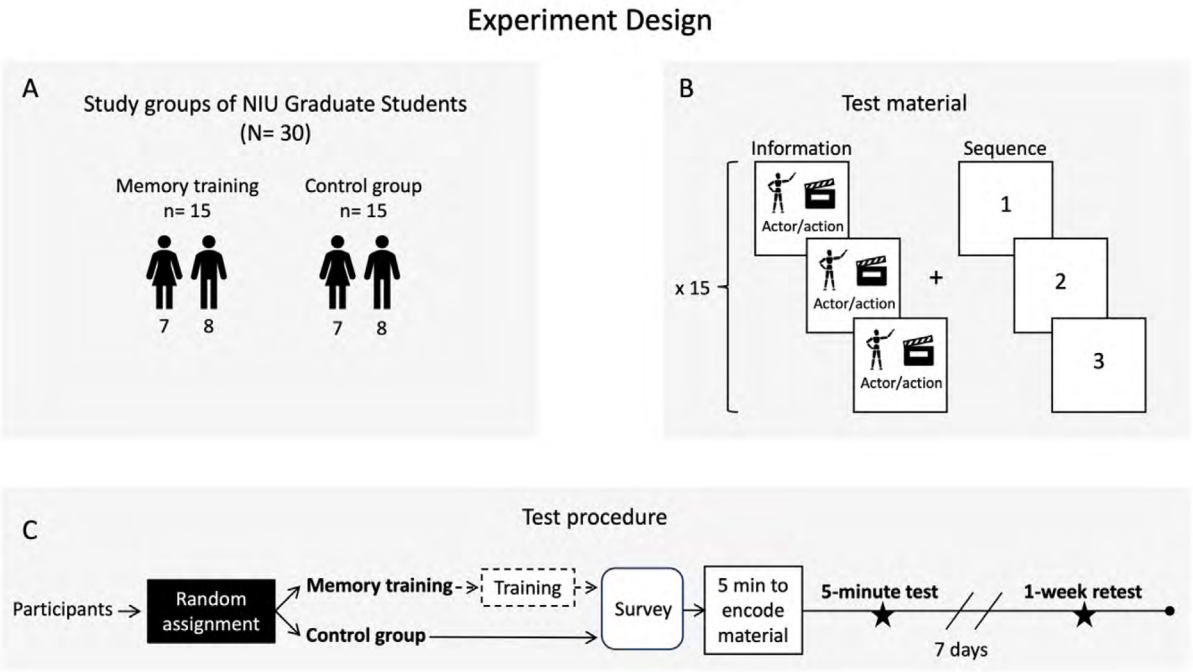
TEST PROCEDURE

Data collection occurred in person at NIU in a distraction-free classroom environment. Consent forms, tests, and surveys were hand-distributed and administered on paper copies. No digital media were used in data collection. The author of this article and at least one NIU faculty member were present for all data collection events.

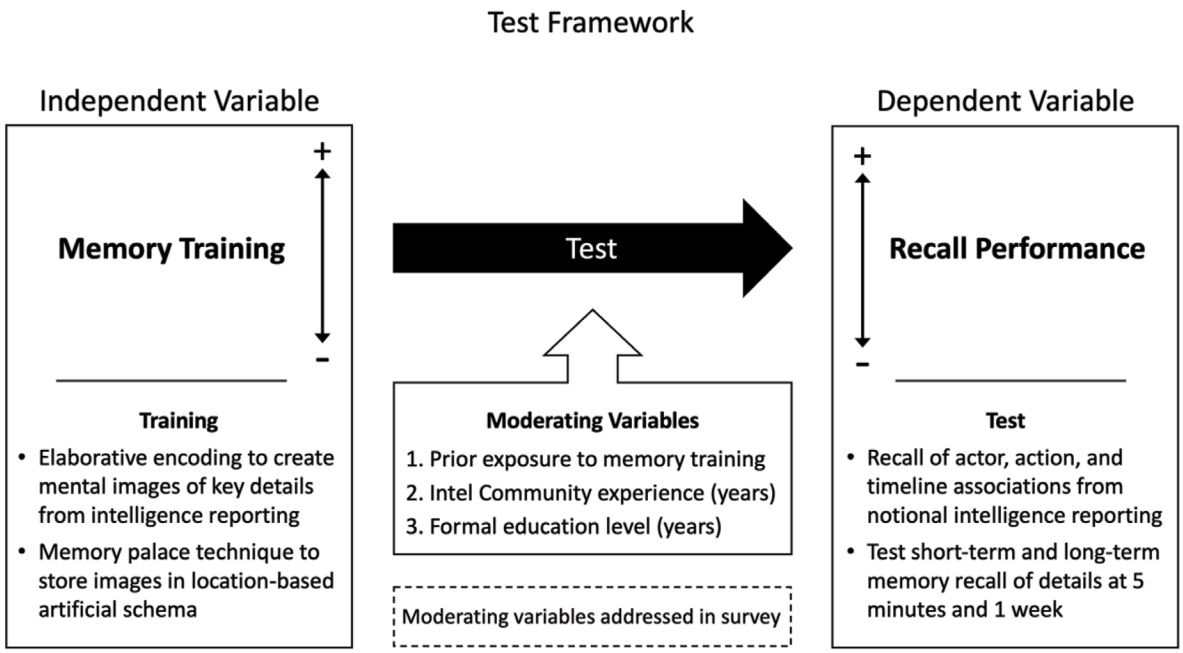
Data collection proceeded in three steps. First, participants were asked to memorize 45 items of information in five minutes. The information consisted of one sheet of paper with 15 pairs of actors with associated actions in sequential order. After five minutes, the information sheets were collected, and participants were given a five-minute break. Participants could socialize in place but were not permitted to discuss the test or write anything down. Second, after the five-minute break, participants were provided a blank information sheet and asked to recall and record as much of the previous information as possible from memory. Third, one week later, participants were again provided the blank information sheet and asked to recall and record the information from memory. Participants were asked not to write down any test information and had no prior knowledge of the one-week retest prior to its execution as a "pop quiz."

Finally, a demographic survey collected information on three moderating variables that could impact a participant's performance in the study. These moderating variables were (1) prior exposure to memory techniques,

(2) IC experience, and (3) education level. A separate descriptive survey collected participants' overall views of the experiment and their opinions on the potential for the IC to provide memory training to its analysts.



Experiment design. (A) Participants (N=30) were randomly assigned to a memory training group or control group. (B) Participants were given five minutes to memorize test material. (C) Participants' recall was tested at five minutes and one week.



SCORING

Incorrect responses were assessed with respect to the sequence of items in the original list. This involved counting the number of responses that were out of sequence and assigning a numerical value to the number of places out of sequence the item occurred. For example, if the sixth items on the list were written in the eighth place, a sequence value of 2 was assigned to that incorrect response. This is based on the concept of positional distance developed by Alec Solway et al.[5] In this study, the Sequence Index was introduced to correct for the phenomenon that an item recalled out of order necessarily introduces a second error in the place where the item would have appeared, whether or not the other item was recalled correctly.[6] For example, recall of the sequence 1,2,3,4,5 as 1,3,2,4,5 contains 2 positional errors of distance 1 resulting from the single reversal of (2,3).[7] The Sequence Index corrects for this and allows for straightforward computation of the magnitude of overall sequence accuracy. This allows for a more accurate and nuanced comparison of results across an entire item list using a single index for each participant and test.[8] The total sequence value (sum of positional distance errors) for each response sheet at each timepoint was converted to the sequence index (SeqI) using the formula:

$$SeqI = (\sum \textit{position errors} \div 2) \div (\textit{\# correct responses})$$

MEMORY TRAINING GROUP

Intelligence analysts struggle to recall details from reporting because the human mind is poorly suited to encode abstract information such as numbers, dates, and timelines. Evolutionary psychologists claim that modern humans and primitive hunter-gatherers share the same basic brain physiology.[9] Thus, modern humans are the inheritors of thousands of years of selective adaptation, which fashioned the ideal hunter-gatherer mind. Therefore, our minds are calibrated to remember predators, potatoes, and potential mates—not passwords, pin codes, or Pyongyang's military order of battle. To do that, memory techniques known as mnemonic devices act as software to run on our hunter-gatherer hardware. Mnemonic devices work by converting arbitrary information into vivid and emotionally charged images and scenes that stick in the mind.

> Heuer puts it this way:
>
> Specifically, information that is vivid, concrete, and personal has a greater impact on our thinking than pallid, abstract information … Mnemonic devices are useful for remembering information that does not fit any appropriate conceptual structure or schema already in memory. They work by providing a simple, artificial structure to which the information to be learned is then linked. The mnemonic device supplies the mental "file categories" that ensure retrievability of information. To remember, first recall the mnemonic device, then access the desired information.[10]

The following paragraphs describe the three mnemonic devices used in the experiment: (1) mental imagery and elaborative encoding, (2) the major system, and (3) the memory palace.

MENTAL IMAGERY AND ELABORATIVE ENCODING

Mental imagery optimizes memory by engaging parts of the brain involved in creativity and imagination. Indeed, the word imagination derives from the Latin word *imago* or image. Aristotle claimed that "to think is to speculate with images."[11] Albert Einstein and Marcel Proust claimed that mental imagery played a central role in their creative processes.[12] Simply put, the mind is optimized to remember what it engages with creatively, such as mental imagery.

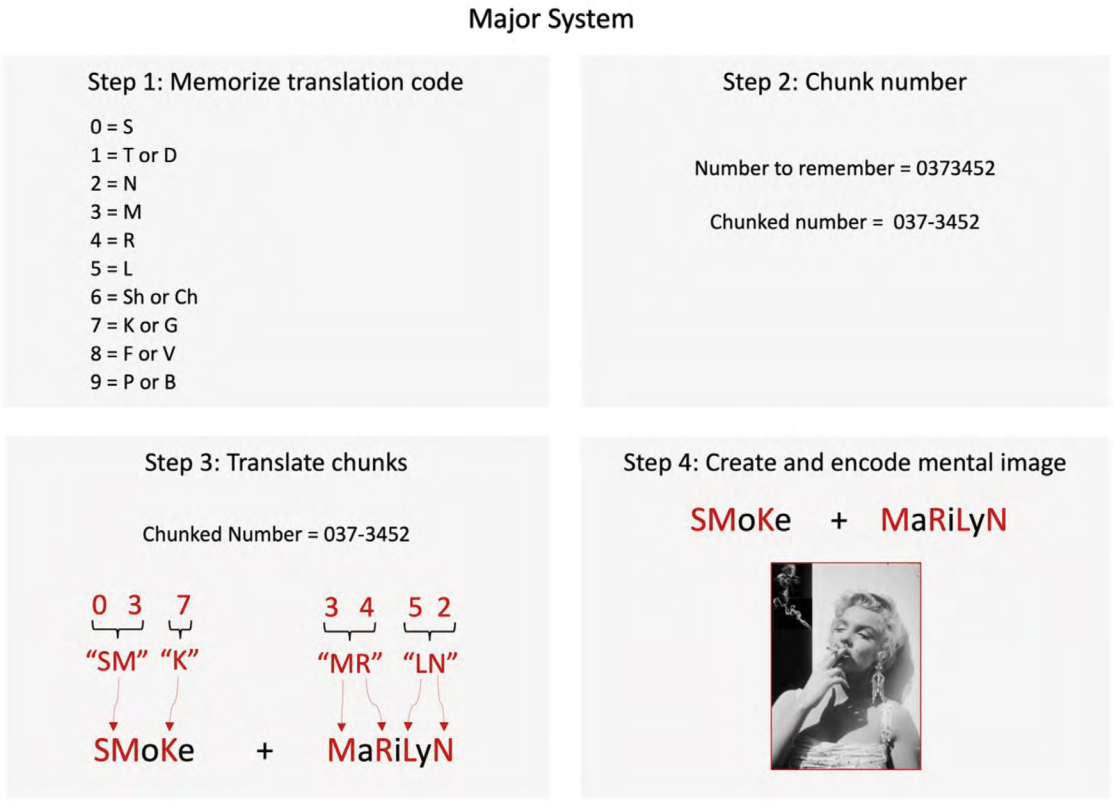
Elaborative encoding is a mnemonic device that imbues mental imagery with emotional cues to convert abstract information into vivid, emotionally charged—even racy—images and scenes. Elaborative encoding is a way to hack the hunter-gatherer mind's natural proclivity for threat avoidance, jovial social interaction, and mate-seeking. All the world's memory champions use elaborative encoding, often in conjunction with the other mnemonic devices used in the experiment.[13] In psychology, this phenomenon is known as the emotional arousal theoretical framework.[14] Elaborative encoding also operates according to the von Restorff effect, named for pioneering German female psychiatrist and pediatrician Hedwig von Restorff (1906–1962). The von Restorff effect states that people are more likely to notice and remember things that stand out from the norm, such as vivid, emotionally charged images or scenes.[15] Several neuroscience experiments using brain scans show that areas associated with emotion and memory are activated during elaborative encoding. This suggests that emotion "serves as a kind of turbo booster, strengthening the imprint of the memory."[16] Other laboratory experiments demonstrate that "emotional arousal, even from an unrelated source, is capable of modulating memory consolidation."[17]

Memory techniques known as mnemonic devices act as software to run on our hunter-gatherer hardware. Mnemonic devices work by converting arbitrary information into vivid and emotionally charged images and scenes that stick in the mind.

MAJOR SYSTEM

The major system is a mnemonic device for encoding and recalling long numbers. French scholar Aimé Paris (1798–1866) developed the system to aid in mathematics.[18] The major system translates numbers into basic phonetic sounds and uses elaborative encoding to transform these sounds into vivid mental images. These images are easier for the mind to remember than arbitrary numbers. The major system involves four steps. First, memorize the translation of numbers 0-9 into simple phonetic sounds. Second, separate the long number into manageable chunks of two to four numbers per chunk. George Miller's 1956 famous article "Magical Number Seven, Plus or Minus Two," describes the "chunking" process and is why US telephone numbers are separated into groups of three and four numbers.[19] Third, translate the chunks into words by adding vowels between the chunks. Last, create a memorable mental image of the word combinations. To recall the original number, reverse the process to translate the mental image back into numerical form using the memorized translation code. Memory champions use the major system to perform incredible memory feats, such as memorizing the mathematical constant pi out to thousands of digits.[20] The major system provides intelligence

analysts a tool for encoding and recalling details from intelligence reporting such as timelines, actor/action associations, military order-of-battle charts, equipment specifications, and mapping coordinates.



MEMORY PALACE

The memory palace is the world's oldest and arguably most powerful mnemonic device, particularly when combined with elaborative encoding and the major system. It uses mental navigation along well-known spatial routes stored in memory, such as a college campus, place of worship, or childhood home. To-be-remembered information is mentally placed at landmarks along the imagined route. The information is then recalled by mentally retracing the route, "picking up" the "placed" information along the journey.[21]

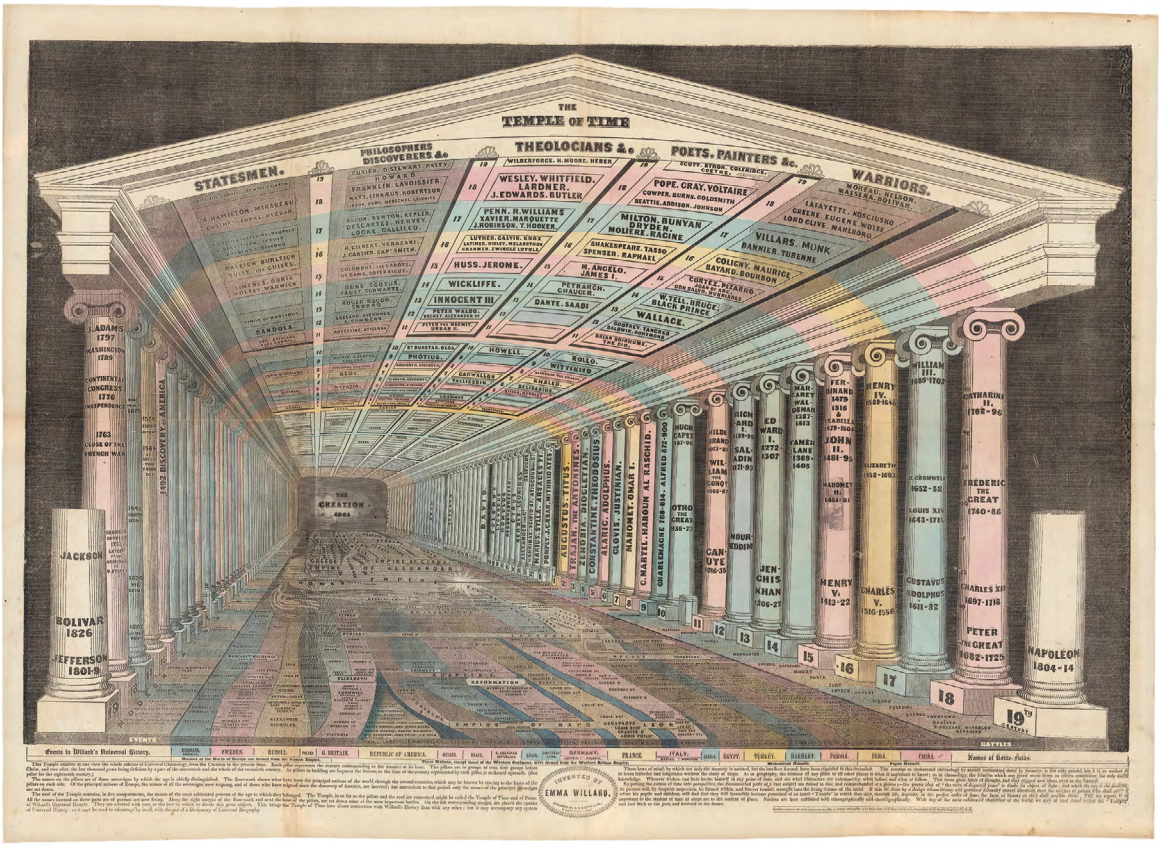
Heuer recommends the memory palace in *The Psychology of Intelligence Analysis*:

> Try to memorize the following items from a shopping list: bread, eggs, butter, salami, corn, lettuce, soap, jelly, chicken, and coffee. The list is difficult to memorize because it does not correspond with any schema already in memory. The words are familiar, but you do not have available in memory a schema that connects the words in this group to each other. If the list were changed to juice, cereal, milk, sugar, bacon, eggs, toast, butter, jelly, and coffee, the task would be much easier because the data would then correspond with an existing schema—items commonly eaten for breakfast. Such

a list can be assimilated to your existing store of knowledge with little difficulty, just as the chess master rapidly assimilates the positions of many chessmen.

To learn the grocery list of disconnected words, you would create some structure for linking the words to each other and/or to information already in long-term memory. You might imagine yourself shopping or putting the items away and mentally picture where they are located on the shelves at the market or in the kitchen. Or you might imagine a story concerning one or more meals that include all these items. Any form of processing information in this manner is a more effective aid to retention than rote repetition.[22]

In the quote above, Heuer cites the pioneering work of Francis S. Bellezza, Ohio State Professor of Psychology Emeritus and noted scholar of mnemonic devices.[23]



Memory Palace Taught in US Schools: Emma Willard's 1846 "Temple of Time"[24]

Emma Hart Willard (February 23, 1787–April 15, 1870) First published in the USA in 1846, Public domain, via Wikimedia Commons

The memory palace was taught in the Western educational system from ancient Greece until the late 19th century, including in US schools. One example of the memory palace in American classrooms is Emma Willard's 1846 *The Temple of Time*. This system taught world history through an imaginary walk through

a large, printed representation of an ancient Greek temple. Students followed along with the lessons by creating mental images of important historical events and persons, mentally "placing" the images along the temple's numbered columns.[25] The author of this article received special permission from the Library of Congress to view an original *The Temple of Time* wall hanging and workbook to aid in this research.[26]

FINDINGS

The results of the experiment revealed four key findings. First, memory training group participants scored 45 percent higher overall than controls. Second, memory training group participants recalled 57 percent more information after one week than controls. Third, memory training group participants were five times more likely to achieve a perfect score on long-term and short-term memory tests than controls. Last, participants of both groups with prior exposure to memory techniques scored 18 percent higher than participants with no prior exposure. These findings meet or exceed the standard of statistical significance and support the hypothesis that memory training increases intelligence analysts' ability to recall key details, thereby improving their performance.

STATISTICAL SIGNIFICANCE

The threshold for statistical significance used throughout the experiment was p-value below 0.05. In other words, for the differences in mean values to be considered significant, there is at least 95-percent confidence that they are not due to random chance. The t-test for the overall mean score comparison between the study groups revealed a p-value of 0.00000001, meaning that the results were almost certainly not due to random chance. Statistical analysis and graphing were performed with Stata 18.0 Basic Edition.

IMPACT OF MODERATING VARIABLES

A demographic survey collected information on three moderating variables that could impact the participants' performance in the study. These moderating variables were (1) prior exposure to memory techniques, (2) Intelligence Community experience, and (3) education level.

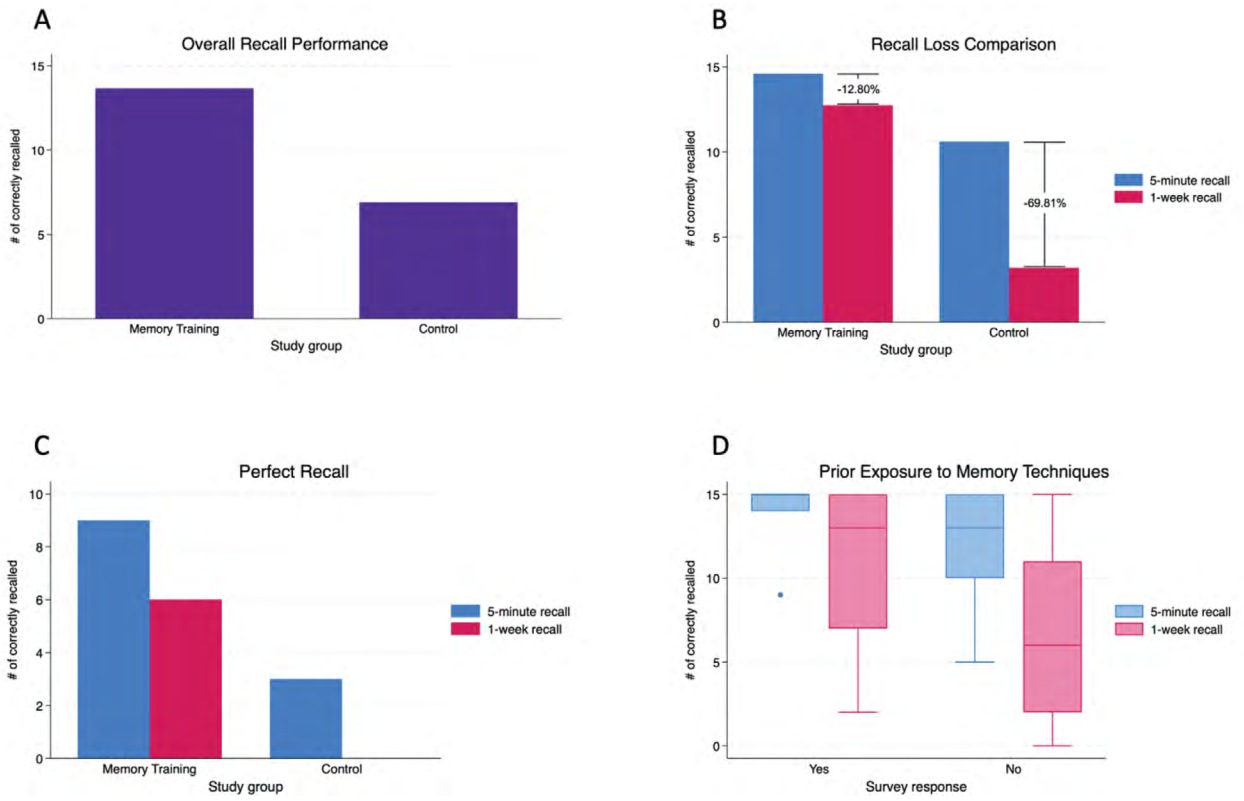
Analysis of the demographic survey and experiment results revealed:

1. Participants with prior exposure to memory techniques scored 18 percent higher than participants with no prior exposure (p-value = 0.026). This result is considered statistically significant.

2. There was no statistical significance in the difference in recall scores between participants with greater IC experience.

3. There was no statistical significance in the difference in recall scores between participants with advanced degrees versus undergraduate degrees.

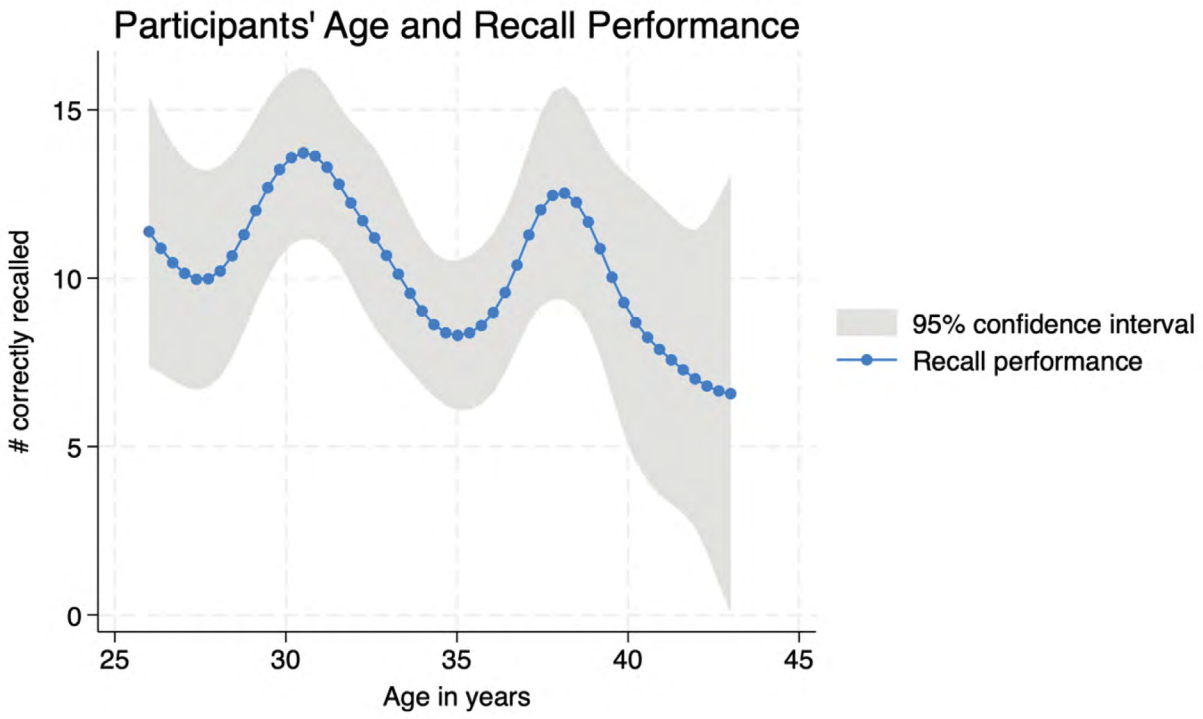
Key Findings		
Test	**Expected Outcome**	**Result**
Study Hypothesis	Memory training increases intelligence analysts' ability to recall actors, actions, and timelines.	**Supported:** Memory training group participants scored 45 percent higher overall than control group participants. Memory training group participants recalled 57 percent more information after one week than control group participants. Memory training group participants were also five times as likely to achieve a perfect score than controls.
Moderating Variable 1: Prior exposure to memory techniques	Participants with prior exposure to memory techniques will score higher on recall tests.	**Supported:** Participants with prior exposure to memory techniques scored 18 percent higher than participants with no prior exposure.
Moderating Variable 2: Intelligence Community experience	Participants with greater Intelligence Community experience will score higher on recall tests.	**Unsupported:** There was no statistical significance in the difference in recall scores between participants with between one and twenty years of Intelligence Community experience.
Moderating Variable 3: Education level	Participants with more formal civilian education will score higher on recall tests.	**Unsupported:** There was no statistical significance in the difference in recall scores between participants with advanced degrees versus undergraduate degrees.



Experiment Results. (A) Memory training group participants scored 45 percent higher overall than controls. (B) Memory training group participants recalled 57 percent more information after one week than controls. (C) Memory training group participants were five times more likely to achieve a perfect score on long-term and short-term memory tests than controls. (D) Participants of both groups with prior exposure to memory techniques scored 18 percent higher than participants with no prior exposure.

UNEXPECTED FINDINGS

The experiment revealed an unexpected correlation between increased age and lower recall performance. Participants aged 34 and older scored 21percent lower than those aged 33 and younger on both the short-term and long-term memory tests, regardless of study group. This result is statistically significant. A body of medical literature and common experience correlate increased age with memory loss. However, this study assumed that greater IC experience and higher education levels would compensate for age-related memory degradation. Of note, no other demographic but age on the participant survey yielded significant score variance. These demographics included sex, occupation (analyst vs. officer), and military experience.



We predicted that participants with greater IC experience and more formal education would score higher on memory recall tests. Surprisingly, the findings indicated no statistical significance in the difference in scores between participants with between one and twenty years of IC experience. There was also no significance in the difference in recall scores between participants with advanced degrees versus undergraduate degrees. This finding is likely due to the negative impact of age on memory performance addressed in the previous paragraph.

Despite the memory training group's superior overall performance, the group made significantly more "near miss" errors than controls. This result exposes a weakness in mnemonic devices that would require additional training to overcome.

Despite the memory training group's superior overall performance, the group made significantly more

"near miss" errors than controls. These errors involve minor semantic mistakes, such as recalling the verb "jump" or "leap" instead of the correct verb "hop." These errors likely occurred while the memory training group mentally "decoded" remembered mental images back into the original test information. This result exposes a weakness in mnemonic devices that would require additional training to overcome.

LIMITATIONS AND FUTURE RESEARCH

The experiment had three limitations. First, all 30 participants were IC members and intelligence analysts or officers, but not all served as full-time analysts. Although there was no significance in score variance between analysts and officers, the study was designed to test analysts. A larger sample of solely analysts would better gauge the impact of memory training on analysts' recall performance. Second, this study used notional unclassified intelligence reporting that did not contain violent or disturbing material. Future studies should use actual classified reporting to better replicate conditions in the field. Last, participants ranged in age between 26 and 43. Future studies should use a broader age distribution to better represent IC demographics and more accurately gauge the impact of age on memory. Last, the memory training group received training on the three best-known mnemonic devices that use mental imagery and spatial contextualization—elaborative encoding, the major system, and the memory palace. A future direction for research is to study the impact of individual mnemonic devices on specific intelligence analysis tasks, such as critical thinking, creative thinking, product creation, and briefing. Those findings would help analysts employ the best mnemonic device for the analytic task at hand.

RECOMMENDATIONS

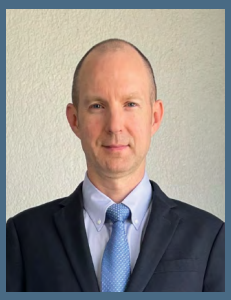
Intelligence analysts over the age of 34 would benefit most from memory training, based on the results of this study. Memory training is cost-effective and does not require special technology. For example, the results in this study were achieved in a one-hour block of instruction using only a short video, briefing slides, whiteboards, and paper handouts. Of note, according to a descriptive survey, all participants of the memory training group found the instruction valuable, and 96 percent of all participants think the IC should provide memory improvement training to its workforce.

CONCLUSION

This article presented the findings of an experiment to test the effect of memory training on intelligence analysis. The results indicate a significant relationship between memory training and a boost in recall of key details from intelligence reporting. This strongly suggests a link between memory optimization and analytic performance. Memory techniques that use mental imagery to convert abstract information into vivid, emotionally charged scenes are the most effective for intelligence analysis. As a result, we can proclaim with confidence that mnemonic devices have a place in the analyst's toolkit—just as Heuer and Sinclair

theorized in the 1980s and 1990s. Overall, this article recommends a modest IC investment in memory training to better support policymaking and improve the overall well-being of the workforce.

Cody Herr's paper was published under the title "Memory Techniques in the Intelligence Community: A Tool for Improving Analysis?" in *Studies in Intelligence* 69, no. 1 (March 2025), https://www.cia.gov/resources/csi/studies-in-intelligence/studies-in-intelligence-69-no-1-extracts-march-2025/memory-techniques-in-the-intelligence-community-a-tool-for-improving-analysis/.



Chief Warrant Officer 4 Cody Herr is a career US Army intelligence officer and graduate of the National Intelligence University's (NIU) Master of Science of Strategic Intelligence program. His area of research is cognitive performance enhancement for intelligence analysts. He has published in NIU's NI Press, *American Intelligence Journal,* and *Special Warfare Magazine.* His awards and decorations include the Bronze Star Medal, General Douglas MacArthur Leadership Award, Military Intelligence Corps Association Knowlton Award, and NIU's Denis Clift Award.

ENDNOTES

1. Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton University Press, 1966), xxiv.
2. Richards J. Heuer, *Psychology of Intelligence Analysis* (Center for the Study of Intelligence, Central Intelligence Agency, 1999), 17.
3. Robert S. Sinclair, *Thinking and Writing: Cognitive Science and Intelligence Analysis* (Nova Science Publishers, 2011), 8–14.
4. Office of the Director of National Intelligence, *Annual Demographic Report Fiscal Year 2022: Hiring and Retention of Minorities, Women, and Persons with Disabilities in the United States Intelligence Community* (ODNI, 2022), 14.
5. Alec Solway, Bennet B. Murdock, and Michael J. Kahana, "Positional and Temporal Clustering in Serial Order Memory," *Memory & Cognition* 40, no. 2 (February 1, 2012): 1–12, https://doi.org/10.3758/s13421-011-0142-8.
6. David Reser et al., "Australian Aboriginal Techniques for Memorization: Translation into a Medical and Allied Health Education Setting," *PLOS ONE* 16, no. 5 (May 18, 2021): 5, https://doi.org/10.1371/journal.pone.0251710.
7. Reser et al., "Australian Aboriginal Techniques," 5.
8. Solway, Murdock, and Kahana, "Positional and Temporal Clustering in Serial Order Memory," 1–12.
9. Leda Cosmides and John Tooby, *Evolutionary Psychology: A Primer* (Center for Evolutionary Psychology, 1997), 1–3.
10. Heuer, *Psychology of Intelligence Analysis*, 25–26, 116.

11. Aristotle, *De Anima,* trans. C. D. C. Reeve (Hackett Publishing Company, Inc., 2017), 50.
12. Stephen M. Kosslyn, William L. Thompson, and Giorgio Ganis, *The Case for Mental Imagery*, illustrated ed. (Oxford University Press, 2009), 4.
13. Joshua Foer, *Moonwalking with Einstein: The Art and Science of Remembering Everything* (Penguin Press, 2011), 165–68.
14. Robert B. Lull and Brad J. Bushman, "Do Sex and Violence Sell? A Meta-Analytic Review of the Effects of Sexual and Violent Media and Ad Content on Memory, Attitudes, and Buying Intentions," *Psychological Bulletin* 141, no. 5 (2015): 1022–48, https://www.apa.org/pubs/journals/releases/bul-bul0000018.pdf.
15. H. V. Restorff, "Ueber Die Wirkung von Bereichsbildungen Im Spurenfeld. Analyse von Vorgängen Im Spurenfeld. I. Von W. Köhler Und H. v. Restorff. [On the Effect of Field Formations in the Trace Field. Analysis of Processes in the Trace Field. I. By W. Kohler and H. v. Restorff.]," *Psychologische Forschung* 18 (1933): 299–301, https://link.springer.com/article/10.1007/BF02409636.
16. Jennifer Spohrs et al., "Repeated fMRI in Measuring the Activation of the Amygdala Without Habituation When Viewing Faces Displaying Negative Emotions," *PLoS ONE* 13, no. 6 (June 4, 2018): 1–12, https://doi.org/10.1371/journal.pone.0198244.
17. Kristy A. Nielson, Douglas Yee, and Kirk I. Erickson, "Memory Enhancement by a Semantically Unrelated Emotional Arousal Source Induced After Learning," *Neurobiology of Learning and Memory* 84, no. 1 (July 1, 2005): 49–50, https://doi.org/10.1016/j.nlm.2005.04.001.
18. Aimé Paris, *Expositions et Pratique Des Procédés de La Mnemotechniques, à l'usage Des Personnes Qui Veulent Étudier La Mnémotechnie En Général* (Imprimerie de C. Farcy, 1825), 592.
19. George A. Miller, "The Magical Number Seven, Plus or Minus Two: Some Limits on Our Capacity for Processing Information," *Psychological Review* 63, no. 2 (1956): 81.
20. Jason Week, *Memorize Pi Using the Major System* (Jason Week, 2020), 12; and Foer, *Moonwalking with Einstein*, 164–65.
21. Frances A. Yates, *The Art of Memory*, repr. (Bodley Head, 2014).
22. Heuer, *Psychology of Intelligence Analysis*, 24–26.
23. Francis S. Bellezza, "Mnemonic Devices: Classification, Characteristics, and Criteria," *Review of Educational Research* 51, no. 2 (1981): 247, https://www.jstor.org/stable/1170198.
24. Daniel Rosenberg and Anthony Grafton, *Cartographies of Time: A History of the Timeline*, illustrated ed. (Princeton Architectural Press, 2012), 22.
25. Rosenberg and Grafton, 22.
26. Emma Willard, *Willard's Historic Guide. Guide to the Temple of Time; and Universal History for Schools.* (A. S. Barnes & Co., H. W. Derby & Co., 1849); "Willard's Historic Guide. Guide to the Temple of Time; and Universal History for Schools.," online text, Library of Congress, accessed April 15, 2024, https://www.loc.gov/resource/gdcmassbookdig.willardshistoric00will/?sp=1&st=gallery.

FUTURE OF INTELLIGENCE STUDIES: SELECT PAPER

MAKING THE CASE FOR INTELLIGENCE STUDIES AS A DISCIPLINE: Praxis, Discipline, and the Challenge of Collective Efficacy

Stacey Pollard, Ph.D.

FRAMING THE DEBATE

Whereas biology, physics, or political science are firmly established as academic disciplines, intelligence studies continues to be contested in the academy. Critics, including intelligence academicians and scholars, dismiss it as too applied, policy-driven, or eclectic to constitute a discipline,[1] while advocates argue it meets or is approaching disciplinary criteria.[2] At the heart of this debate lies a tension: Is intelligence studies praxis or discipline?

IMAGINING INTELLIGENCE: DEFINING A CONTESTED PROFESSION

The evolution of intelligence as a profession has been marked by both functional necessity and conceptual ambiguity. Although intelligence organizations have long performed crucial roles in national security, their professional identity—and even the existence of the "intelligence community" as a coherent entity—remains contested. Scholars and practitioners alike have offered definitions of intelligence that reflect the field's complexity, but these definitions also expose fault lines regarding what unites intelligence as a vocation. This ambiguity suggests that the profession of intelligence, much like a nation, may be understood as a socially constructed identity that relies on shared narratives, symbols, and practices rather than a universally accepted essence.

Here, Benedict Anderson's notion of "imagined communities" provides a compelling analogy. Anderson argued that nations are not natural entities, but rather "imagined political communities" sustained by collective belief and shared experiences of belonging.[3] Similarly, the so-called "intelligence community" may best be understood as an imagined professional community—brought into being by the practices,

institutions, and discourses that bind together diverse agencies and practitioners under a common banner, even as disagreement persists over its scope, purpose, and legitimacy. Recognizing this imagined quality highlights the importance of critically examining how intelligence professionals construct, contest, and reproduce their collective identity over time.

Thus, the roles of the intelligence profession and the Intelligence Community (IC) have been subjects of extensive research and debate, with various scholars and practitioners offering definitions that reflect the complexity and breadth of these perspectives. For Mark Lowenthal, the intelligence profession encompasses the collection, analysis, and dissemination of information to support national security and foreign policy objectives. He emphasizes that intelligence professionals are responsible for providing insights that reduce uncertainty for policymakers, thereby facilitating informed decisionmaking. This perspective highlights the integral role of intelligence in shaping strategic initiatives and responses.[4]

Jennifer Sims builds on this view, emphasizing the role of "decision advantage" as the strategic use of intelligence to gain a competitive edge over adversaries. Through empirical case study analysis, she argues that, by effectively leveraging intelligence, decisionmakers can anticipate and counter opponents' moves, thereby achieving superiority in international politics. Sims' argument emphasizes that intelligence is not merely about information gathering, but involves the strategic application of that information to influence outcomes in favor of one's own nation.[5]

Sims' concept underscores the importance of intelligence in formulating strategies that provide policymakers with a decisive edge, enabling them to make informed choices that can alter the balance of power in international relations. Loch Johnson, on the other hand, underscores the importance of ethical conduct within the intelligence profession. He asserts that intelligence professionals must balance the necessity of secrecy with adherence to legal and moral standards. This balance ensures that the intelligence provided to decisionmakers is both reliable and ethically obtained, maintaining public trust and the legitimacy of intelligence operations.[6]

Similarly, Peter Gill and Mark Phythian highlight the significance of accountability in the intelligence profession. They argue that intelligence agencies must operate under robust oversight mechanisms to prevent abuses of power and to ensure that the information provided to decisionmakers is accurate and unbiased. This perspective emphasizes the need for transparency and checks and balances within intelligence operations.[7]

Through a historical analysis of the intelligence profession, Michael Warner examines its evolution from tactical military support to a broader strategic function. He observes that modern intelligence professionals not only gather information but also engage in activities such as counterintelligence and covert operations, thereby offering decisionmakers a comprehensive understanding of both opportunities and threats.[8] In the same vein, Michael Herman emphasizes the organizational aspects of the intelligence profession, defining it as a structured network of agencies responsible for collecting and analyzing information to support decisionmaking at the highest levels of government. He points out that effective coordination among these agencies is crucial for producing comprehensive intelligence assessments, thereby enhancing national security.[9]

Finally, Stephen Marrin discusses the professionalization of intelligence, suggesting that it encompasses specialized knowledge, a distinct set of skills, and a commitment to public service. He notes that the development of formal training programs and ethical codes has contributed to recognizing intelligence as a bona fide profession, with established norms and standards guiding practitioners.[10]

These perspectives demonstrate a clear consensus among scholars that the intelligence profession plays a pivotal role in informing national decisionmakers by providing timely, accurate, and ethically gathered information. They also collectively underscore the multifaceted nature of intelligence work, highlighting the importance of analytic rigor, decision advantage, ethical considerations, accountability, historical evolution, organizational structure, and professionalization.

Scholars and practitioners who argue that intelligence studies is praxis rather than an academic discipline often point to the mission-driven, applied nature of intelligence work. Intelligence is not primarily concerned with developing abstract theories or establishing generalizable knowledge in the way academic disciplines are; rather, it is focused on producing actionable insights for decisionmakers under conditions of secrecy, ambiguity, and urgency. Its methods are designed less for the sake of scientific rigor than for immediate operational utility—whether through the production of daily briefings, strategic estimates, or tactical warnings. Intelligence as praxis is embedded in the realities of national security decisionmaking, judged by its accuracy, timeliness, and impact rather than its theoretical contribution to an academic body of knowledge.

FROM KNOWLEDGE TO ACTION: INTELLIGENCE AS PRAXIS

Intelligence has always been grounded in praxis: it is an applied craft designed to reduce uncertainty for decisionmakers. Sherman Kent's classic definition emphasized intelligence's role in producing "knowledge upon which a state's security depends."[11] Its legitimacy stems from utility—whether intelligence products provide decision advantage, prevent surprise, or shape national security outcomes.

Praxis emphasizes mission-driven performance rather than theoretical development. Analysts integrate insights from political science, economics, psychology, or history only insofar as they aid operational needs. The art of intelligence is synthesis under uncertainty, judged by accuracy, timeliness, and impact.[12] This outcome orientation, combined with secrecy and politicization, reinforces the argument that intelligence studies resists disciplinary codification and remains first and foremost a craft.

THE ANATOMY OF AN ACADEMIC DISCIPLINE

In its broadest sense, an academic discipline is understood as a structured field of study with shared theoretical frameworks, research methods, and institutional recognition. It is characterized by a distinct domain of knowledge, established paradigms, and a community of scholars engaged in advancing, critiquing, and disseminating knowledge. Disciplines are embedded within universities and research organizations, where

they shape curricula, professional development, and intellectual inquiry. Over time, they evolve in response to new theoretical developments, technological advancements, and societal change.

Scholars frequently highlight the dual foundations of disciplines: their philosophical coherence and their institutional embodiment. The higher education scholar Tony Becher explains: "Disciplines are characterized by their own particular objects of research, their own epistemological foundations, and their own criteria for what counts as valid knowledge. They also have their own technical language, a body of concepts, and a community of scholars."[13] Similarly, Armin Krishnan underscores the convergence of intellectual and organizational consensus emphasizing, "[D]isciplines must have some institutional manifestation in the form of subjects taught at universities or colleges, respective academic departments, and professional associations connected to it. Only through institutionalisation are disciplines able to reproduce themselves."[14]

Building on these perspectives, the foundation of any academic discipline rests on three interrelated philosophical components—ontology, epistemology, and methodology—supported by institutional structures. Ontology, the study of what exists and what can be known, defines a discipline's assumptions about reality. Ontological perspectives determine whether phenomena are treated as objective and independent of perception or as socially constructed. In the social sciences, realism posits that social structures exist independently of human awareness, while constructivism argues that social realities are shaped by human interactions and interpretations.

Epistemology concerns the nature and scope of knowledge: how it is acquired, validated, and justified. Different disciplines adopt different epistemological stances, which influence the types of questions asked and the standards of truth applied. The natural sciences, for example, often adhere to positivist epistemologies emphasizing empirical observation and falsifiability, while the humanities may embrace interpretivist or constructivist epistemologies that value subjective meaning-making and historical context.

Methodology links epistemology and ontology to practical investigation. It provides the systematic approaches through which disciplines generate and validate knowledge—whether through quantitative, qualitative, or mixed-methods research. Economics, for instance, often employs mathematical modeling and statistical analysis, while anthropology integrates ethnographic fieldwork and interpretive analysis.

Finally, these philosophical foundations are sustained by institutional support, which provides the organizational infrastructure necessary for disciplines to function. Universities, research centers, academic journals, and professional societies ensure that disciplines reproduce themselves through curricula, training, scholarly exchange, and standards of professional practice.

Together, ontology, epistemology, methodology, and institutional support delineate the intellectual and organizational boundaries of an academic discipline. They guide the formulation of research questions, influence theoretical developments, and establish the criteria by which scholarly contributions are judged. Understanding these foundational elements is essential for evaluating the maturity, coherence, and legitimacy of any field of study in the broader academic landscape.

INTELLIGENCE STUDIES AND THE QUESTION OF DISCIPLINARY LEGITIMACY

The debate over whether intelligence studies constitutes a legitimate academic discipline has been a recurring theme in the scholarly literature. Early critiques emphasized the field's conceptual and methodological shortcomings. Klaus Knorr argued that intelligence research lacked the theoretical rigor and systematic methodology necessary to sustain disciplinary status, suggesting instead that intelligence functioned primarily as an applied craft within state institutions rather than an autonomous academic field.[15] Similarly, Warner highlighted the definitional ambiguity at the very core of intelligence studies. He noted that scholars and practitioners alike struggled to agree on what "intelligence" actually encompassed—whether it should be understood as a process, a product, or an institution—casting doubt on the possibility of establishing a coherent body of knowledge around it.[16]

Building on these critiques, Marrin argues that intelligence studies, despite its growing body of scholarship, fails to meet the standard of a mature academic discipline because it lacks cumulative theory-building. Whereas established fields develop shared paradigms and progressively refine knowledge through systematic empirical inquiry, intelligence studies has remained fragmented, with scholars and practitioners offering competing definitions of "intelligence" and employing disparate methodological approaches. Marrin attributes this problem in part to the field's origins in professional practice rather than academic theory, which has encouraged ad hoc analysis over sustained theoretical development. He points out that the reliance on classified data inhibits hypothesis testing, replication, and generalizable theory-building, leaving the field dependent on practitioner accounts and single case-based studies rather than systematic inquiry. At the same time, he suggests that the field can advance toward disciplinary status by cultivating greater methodological rigor, fostering a more cohesive community of scholars, and building a cumulative research agenda that integrates both academic and practitioner perspectives.[17]

Taken together, these arguments illustrate both the fragility and promise of intelligence studies. While Knorr and Warner highlight the field's definitional and methodological weaknesses, Marrin identifies pathways toward legitimacy by institutionalizing research infrastructure and advancing methodological innovation.

Despite its origins in practice, intelligence studies has increasingly been institutionalized. Globally, hundreds of intelligence studies programs, professional journals, and research centers have emerged.[18] The field now possesses a definable subject matter (intelligence in national security and decisionmaking), theoretical frameworks (politicization, intelligence failure, and epistemic uncertainty), and methodological innovations (classified and unclassified datasets and qualitative, quantitative, and mixed methods data analytic tools).

This institutional and intellectual infrastructure suggests that intelligence studies already meets three of the four classic criteria of a discipline: ontology, epistemology, and institutional support. Where it falls short is methodology, particularly systematic empirical inquiry. Classified sources limit hypothesis-testing, replication, and generalizable theory-building.[19] This problem is exacerbated by the persistence of practitioner-derived analytic traditions, which do not easily translate into the standards of academic research. Much of academic

intelligence research and analysis continues to borrow from tradecraft—structured analytic techniques, scenario construction, or heuristic-based judgments—that are oriented toward producing timely and actionable insights rather than generating replicable, falsifiable, or theory-driven findings. In effect, the methodological toolkit of intelligence studies remains heavily indebted to its origins in praxis, privileging utility over scientific rigor. This legacy constrains the field's ability to establish itself on the same empirical foundations as other academic disciplines, further slowing the development of cumulative bodies of knowledge and theoretical testing.

THE INTELLECTUAL ARCHITECTURE OF INTELLIGENCE STUDIES

Intelligence studies is undergirded by a coherent ontology and epistemology:

Ontology: *Intelligence is knowing; knowledge is power.* Knowing more than adversaries provides relative advantage, prevents surprise, and strengthens state power.[20] For intelligence studies, ontology is not merely an abstract philosophical exercise; it goes to the heart of the field's existence. At its core, intelligence studies is premised on the belief that knowledge—and the ways of organizing, interpreting, and deploying that knowledge—constitute a form of power central to statecraft. Intelligence thus occupies a unique ontological space: it treats information as both an object of inquiry and a strategic resource, simultaneously real in its effects and constructed in its meaning. This dual foundation shapes how intelligence is practiced, studied, and contested, anchoring the discipline's claim to scholarly legitimacy.

Epistemology: Addresses how knowledge is generated, validated, and used within a discipline. In intelligence studies, epistemology is operationalized through the distinctive ways in which the profession categorizes and privileges knowledge. Historically, intelligence knowledge has been dominated by what might be called categories of knowledge hegemony—espionage, deception, sabotage, and, increasingly, open-source collection and analysis. These categories reflect not only technical practices but also normative assumptions about what types of knowledge are deemed authoritative or decisive in statecraft.

In practice, these epistemological foundations are instantiated through specialized intelligence disciplines, or "INTs," each of which channels collection and analysis through distinct methodological logics. Human intelligence (HUMINT) privileges interpersonal access and interpretation, and signals intelligence (SIGINT) emphasizes interception of communications. Geospatial intelligence (GEOINT) relies on imagery and spatial analysis, and measurement and signature intelligence (MASINT) deploys scientific instruments to detect unique physical signatures. Open-source intelligence (OSINT), which has expanded dramatically in the digital age, challenges older hierarchies by asserting that publicly available information can, under certain circumstances, provide insights equal or superior to those derived from clandestine sources.

Together, these epistemological categories form a complex mosaic of knowledge practices, each with its own methods of collection, validation, and authority claims. The interplay among the INTs reflects both complementarity and competition; while the INTs provide multiple pathways to insight, they also reinforce the contested nature of what counts as valid knowledge in intelligence studies. This dynamic underscores a

central epistemological tension of the field—whether knowledge is defined by its secrecy and exclusivity or by its analytic rigor and explanatory power.[21]

Methodology: Encompasses the systematic techniques by which a discipline investigates phenomena, acquires new knowledge, and integrates or corrects existing knowledge. In the social sciences, this involves adherence to the philosophy of science and the scientific method, privileging observable, empirical, and measurable evidence and subjecting it to the laws of reasoning. For intelligence studies, however, methodology remains the discipline's most underdeveloped foundation. Intelligence has historically privileged tradecraft developed for operational utility—collection through HUMINT, SIGINT, GEOINT, MASINT, and increasingly OSINT—rather than systematic research methods designed for transparency, replicability, or cumulative theory-building. This reliance on practitioner heuristics, case-based reasoning, and classified sources produces actionable insights but rarely contributes to cumulative, generalizable knowledge.

Yet this methodological weakness is being overcome in institutional contexts such as the National Intelligence University (NIU), RAND Corporation, and MITRE where efforts are already underway to bridge operational tradecraft with academic research design. These organizations demonstrate how intelligence analysis can be integrated with qualitative, quantitative, and mixed-methods approaches that conform more closely to the standards of the philosophy of science. Internationally, institutions of higher education, such as the National Intelligence and Research University of Kenya, apply standard research methods to intelligence studies, providing additional opportunities to strengthen methodological innovation in diverse security environments.

Moreover, the increasing availability of unclassified data—particularly through OSINT—offers a unique testing ground for applying scientific rigor to intelligence research. By harnessing large-scale open sources and applying creative—as well as critical—thinking, intelligence studies can embrace hypothesis testing and modeling, and can apply qualitative, quantitative, and mixed methods analytic techniques without being constrained by the inaccessibility of classified sources. This approach not only democratizes the field but also enables broader scholarly participation and cross-disciplinary fertilization.

Ultimately, strengthening methodology in intelligence studies requires leveraging context-specific opportunities: classified academic institutions that can instill research design, think tanks and applied research centers that can test methods in policy settings, and unclassified OSINT-based projects that can demonstrate the value of systematic, replicable inquiry. By institutionalizing these practices, intelligence studies can shift from a profession rooted in ad hoc praxis toward a discipline grounded in transparent, cumulative, and scientifically informed research.

Taken together, these ontological, epistemological, and methodological foundations provide a coherent worldview for both intelligence professionals and scholars. Ontology situates intelligence in statecraft as knowledge-as-power; epistemology organizes that knowledge through hegemonic categories and operationalized INTs; and methodology offers the pathway—still maturing but increasingly rigorous—for transforming intelligence from practitioner tradecraft into cumulative, transparent, and scientifically informed research. Methodology anchors intelligence studies in a coherent intellectual project, distinguishing it from adjacent disciplines while offering the basis for cumulative inquiry.

RESOLVING THE DISCIPLINE DEBATE: A DIALECTICAL FRAMEWORK FOR INTELLIGENCE STUDIES

Drawing on dialectical reasoning, we can conceptualize the debate as follows:

- **Thesis (Praxis)**: Intelligence is a craft, mission-driven, evaluated by utility.
- **Antithesis (Discipline)**: Intelligence studies can develop cumulative theory, methods, and institutional legitimacy as an academic field.
- **Synthesis**: Intelligence studies is best understood as a hybrid—an evolving discipline rooted in praxis, where practice provides empirical realities and scholarship supplies theoretical rigor and critical reflection.

This dialectical view rejects false binaries. Praxis and discipline are not mutually exclusive but interdependent: theory informs practice, practice tests theory, and together they refine the field.

Figure 1. Intelligence Studies as Praxis and Discipline: A Dialectical Framework

Dimension	Praxis	Discipline	Synthesis (Evolving Discipline)
Purpose	Deliver decision advantage, reduce uncertainty.	Advance knowledge, test theory.	Use theory to inform practice and practice to refine theory.
Stakeholders	Policymakers, military leaders, intelligence agencies.	Scholars, students, academic institutions.	Communities in dialogue.
Outputs	Briefings, reports, estimates.	Peer-reviewed scholarship, curricula.	Integrated theory and practice, professionalized workforce.
Validation	Utility, accuracy, timeliness.	Peer review, replication, theoretical contribution.	Dual validation: operational impact and academic rigor.
Constraints	Secrecy, politicization, time pressure.	Access limits, academic legitimacy.	Methodological innovation bridging secrecy with scholarship.

SCAFFOLDING A DISCIPLINE: PROGRAMS AND NETWORKS IN INTELLIGENCE STUDIES

A recent survey identified approximately 50 academic programs in intelligence studies across the United States, spanning undergraduate, graduate, and certificate levels. Internationally, initiatives remain more limited—such as Germany's Master of Intelligence and Security Studies and the Intelligence College in Europe, which signal the field's emerging academic footprint abroad.

These programs often spring from disciplines including political science, international relations, criminal justice, science and technology studies, and cybersecurity. Their curricula typically rest on three pillars: procedural tradecraft (collection and analysis methods), core disciplinary theory (intelligence theory and decisionmaking),

and domain specialization (cyber, regional studies, and policy). Schools such as The Citadel offer robust BA and MA degrees infused with intelligence and homeland security leadership training, while institutions such as American Military University provide comprehensive tracks across bachelor's, master's, and doctoral levels. Texas A&M's Bush School, staffed by intelligence practitioners, blends academic rigor with operational relevance.

Professional Academic Associations: Professional organizations have played an important role in legitimizing and advancing intelligence studies as a field of academic inquiry. Groups such as the Association of Former Intelligence Officers (AFIO) and the Military Intelligence Corps Association (MICA) sustain professional identity and heritage by supporting current and former practitioners while creating educational opportunities for broader publics. Other associations emphasize the integration of intelligence into both government and private sector practice. For example, the Association of International Risk Intelligence Professionals (AIRIP) and Strategic and Competitive Intelligence Professionals (SCIP) focus on business, risk, and strategic intelligence, demonstrating the breadth of intelligence beyond national security. The Armed Forces Communications and Electronics Association (AFCEA) and the Intelligence and National Security Alliance (INSA) facilitate collaboration among government, military, industry, and academia, addressing shared challenges in innovation, technology, and policy. At the academic core, the International Association for Intelligence Education (IAFIE) promotes professional standards in intelligence training and pedagogy, while the International Association of Law Enforcement Intelligence Analysts (IALEIA) develops analytical rigor for law enforcement. Finally, the Intelligence Studies Section (ISS) of the International Studies Association anchors intelligence research within the broader international studies community, highlighting the field's growing scholarly legitimacy.

Publishers and Academic Journals: Publishers and academic journals reinforce the professional networks by providing outlets for scholarship, debate, and dissemination of best practices. The *Studies in Intelligence* journal, published by CIA, serves as a forum for both historical reflection and contemporary analysis, helping practitioners connect lessons learned to future challenges. In the academic domain, NIU's National Intelligence Press (NI Press) strengthens the field of intelligence studies by publishing intelligence-focused books, monographs, edited volumes, and *Research Shorts* and *Notes* on topics ranging from the future of the IC to various issues of national security concern. *Intelligence and National Security,* a peer-reviewed journal from Taylor & Francis, has established itself as a leading venue for scholarly research, complemented by more specialized platforms, such as *Global Security and Intelligence Studies,* an open-access journal encouraging both practitioner and academic contributions, and the *Journal of European and American Intelligence Studies,* which situates intelligence within global geopolitics. Together, these publishers and professional organizations form the institutional infrastructure of the discipline, ensuring that intelligence studies continues to mature through collaboration, critical exchange, and scholarly publication.

National Intelligence University: A Unique Institutional Anchor: NIU stands out as the only accredited university dedicated to intelligence studies within the IC. NIU offers degrees in intelligence and strategic, technical, and science-intensive intelligence curricula, and it is fully accredited by the Middle States Commission on Higher Education. NIU comprises two academic units—the College of Strategic Intelligence and the Oettinger School of Science and Technology Intelligence—and supports interdisciplinary study of topics from cybersecurity and WMD to regional and leadership studies.[22]

In addition to NI Press, NIU's scholarly research ecosystem includes:

- The Ann Caracristi Institute for Intelligence Research (CIIR), advancing robust academic inquiry in support of the IC.
- The NIU Library, housing more than 2.5 million items, specialized analytic tools, and a classified research collections archive.
- The iRES Lab, established in 2024, functioning as a technical hub supporting open-source research and collaboration with public and private sectors.
- A Student Thesis Repository with more than 750 digitized theses and capstones dating back to the 1960s.
- The Office of Research and Engagement, which manages partnerships, oversees the Caracristi Institute and NI Press, and supports RAND-led reviews for enhancing research culture and capacity.

NIU faculty regularly lead research-method workshops at conferences—including the International Studies Association, American Political Science Association, and the University of Central Florida's Workshop on Intelligence Teaching—further embedding methodological rigor into the profession.

TOWARD A CULTURE OF INTELLECTUAL DEBATE IN INTELLIGENCE STUDIES

In the past five years, intelligence academicians and scholars have explored, theorized, and advanced important new perspectives that expand the field's horizons. Yet a central question remains: Who has critiqued, argued with, or built upon these perspectives in subsequent publications? In a mature discipline, intellectuals interact not just by producing original research but also by publishing thoughts about one another's ideas, methods, and theories—testing, refining, and contesting them in order to improve collective knowledge about critical phenomena. Despite notable institutional strengths, intelligence studies still struggles with this vital cycle of intellectual engagement.

A small sampling of intelligence scholarship demonstrates the breadth of inquiry. For example, Frederic Baron argues that the intelligence profession is unprepared for the workforce demands of the future amid accelerating change driven by artificial intelligence and global competition.[23] Adrian Wolfberg theorizes—drawing on primary evidence—how ordinary analysts achieve insight to solve novel intelligence problems,[24] while he and Stacey Pollard also expound on the research design process for academic intelligence research, particularly the relationship between research questions and research types, as well as the challenge of establishing causality.[25] Julie Ferringer investigates how to integrate intelligence operators and analysts to maximize organizational outputs,[26] while Josh Kerbel critiques the field's lingering Cold War lens, faulting

its overemphasis on data collection rather than nuanced understanding of complex, evolving threats and how to think about them.[27]

Methodological innovation also features prominently. Kerbel and Tom Pike advocate computational methods and complexity theory as tools for modeling intelligence phenomena.[28] Mark Bailey raises concerns about the lack of frameworks for the safe and competitive application of AI, a gap that could limit the field's adaptation and growth.[29] Alongside Bailey, Richard Uber highlights US vulnerabilities in AI competition vis-à-vis China,[30] while Stephen Hood develops a framework for understanding human–AI compatibility—an effort to better anticipate how analysts and machines can operate effectively together.[31] Thomas Dolan analyzes decisionmaking in war, emphasizing how emotion shapes leaders' bargaining behavior.[32] Similarly, Johnathan Proctor painstakingly examines the practice of warning across the IC and defense, theorizing how it might be better institutionalized.[33]

Empirical case-based contributions are equally rich. Amy Sturm assesses the effectiveness of the Global War on Terror (GWOT) by evaluating terrorist behavior before and after Foreign Terrorist Organization designation; she finds that across 20 years and billions of dollars, designation did not in a single case degrade threats as measured by membership, target hardening, or attacks.[34] Pollard et al. extend this critique, arguing that the GWOT itself helped create conditions favorable to contemporary violent extremists, whose state-making ambitions differ fundamentally from earlier groups seeking policy change through terrorism,[35] while Dennis King theorizes that instability generated by humanitarian crises should become a focal point of intelligence.[36]

Emerging research also highlights regional and thematic depth. Phuong Hoang argues that assessing China's Belt and Road Initiative requires examining failed as well as successful projects, while she and Janice Hinton analyze the economic implications of China's and other Asian government's resilience. David Shin expands his theory of totalitarianism as regime security in North Korea, adding conceptual rigor to the study of closed regimes.

At the same time, scholars are advancing the institutional fabric of the discipline. Phuong Hoang, Mayur Gosai, and Debora Pfaff exemplify the bridging of academia, industry, and government, working at the highest levels of government and in intelligence-adjacent academe to bring world-class talent together on China-related challenges, public engagement, trust, and the scholarly identity of intelligence studies. This cross-sector collaboration signals progress toward addressing the field's low collective efficacy and persistent fragmentation.

Taken together, these contributions underscore the vitality of recent scholarship on critical issues. Yet they also reveal a gap. A mature discipline is not built merely on diverse individual insights but on an ongoing intellectual conversation—debates, rebuttals, refinements, and theoretical contests that sharpen arguments and strengthen knowledge claims. Intelligence studies has made significant strides in breadth and institutional support, but it has yet to cultivate a sustained culture of scholarly engagement where ideas are systematically interrogated and advanced in relation to one another. Building such a culture will be essential for intelligence studies to consolidate its disciplinary identity and achieve intellectual maturity.

UNITY AND IDENTITY: BUILDING COLLECTIVE EFFICACY IN INTELLIGENCE STUDIES

Despite ontological coherence, epistemological clarity, and institutional support, intelligence studies continues to struggle with weak collective efficacy. Albert Bandura defines collective efficacy as a group's shared belief in its ability to achieve common goals, and within intelligence studies this shared belief remains elusive.[37] Scholars remain divided over whether the field should be understood primarily as praxis, as an interdisciplinary arena, or as a fully autonomous discipline. This lack of consensus fragments the field and undermines its growth. Without collective efficacy, intelligence studies cannot consolidate a unified research agenda, codify methodological standards, or attract sustained resources. As Bandura observes, low collective efficacy reduces resilience, weakens identity, and inhibits progress.[38] For intelligence studies, it perpetuates a condition of liminality—neither fully profession nor fully discipline.

CONSOLIDATING INTELLIGENCE STUDIES: PATHWAYS TO DISCIPLINARY MATURITY

The evidence presented in this paper demonstrates that intelligence studies already meets many of the criteria for a discipline: it has a shared ontology that views knowledge as power,[39] an epistemology organized around modes of knowing and the INTs,[40] and growing institutional support in the form of academic programs, professional associations, journals, and dedicated centers. Its enduring weaknesses lie in methodology[41] and in the collective efficacy of its scholarly community.

Moving forward, members of the academic IC must focus not on rehearsing the field's deficits but on actively cultivating solutions. Three priorities stand out:

1. **Methodological Innovation**: Scholars must expand the use of comparative methods, open-source intelligence datasets, and mixed-methods designs to compensate for classified restrictions and to advance transparent, replicable, and cumulative research.[42]

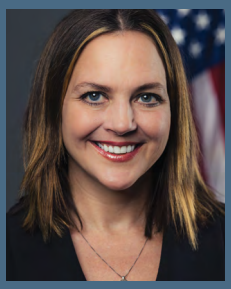
2. **Collective Efficacy**: The community must rally around a shared vision of intelligence studies as a discipline, building consensus on research standards and agendas while fostering the resilience and identity needed to sustain progress.[43]

3. **Dialectical Integration**: Praxis and discipline must be treated as mutually reinforcing. Praxis grounds intelligence in operational realities; scholarship elevates those realities into theory, generating a feedback loop that enriches both.[44]

Institutions such as NIU and other university intelligence studies programs, RAND, MITRE, and international partners already demonstrate that the capacity for innovation exists. OSINT, in particular, provides fertile ground for methodological experimentation that can broaden participation and democratize

intelligence research.[45] What is needed now is a collective commitment to refine, integrate, and institutionalize these practices.

If the community succeeds, intelligence studies will move beyond its liminality and consolidate its identity as a mature and respected discipline. In doing so, it will not only enrich academic inquiry but also provide a rigorous foundation for intelligence practice—ensuring that in a rapidly evolving global security environment, decision advantage continues to rest with those who treat knowledge as the ultimate currency of power.[46]



Stacey Pollard, Ph.D., directs the Ann Caracristi Institute for Intelligence Research and codirects the Center for Global Politics and Societies intelligence research center at the National Intelligence University. Dr. Pollard specializes in research methods and pedagogy, international political systems, global competitive influence, and conflict and instability in the developing world, particularly in the regions of the Middle East and North Africa. She has two decades of experience conducting field research in Egypt, Iraq, Jordan, Lebanon, Syria, and the United Arab Emirates, including applied research in support of operations and intelligence in US warzones. She also taught political science and Middle Eastern studies courses at Western Michigan University and British University in Cairo. Dr. Pollard studied international development at the University of Bonn in Germany, international law at the University of Utrecht in the Netherlands, and Islamic studies at Washington University in Saint Louis, Missouri, prior to earning her Ph.D. in political science at Western Michigan University.

ENDNOTES

1. Dr. Tobias O. Vogt (LTC, USA), "Defining the Discipline of Intelligence Studies," *American Intelligence Journal* 31, no. 2 (2013): 49–53, https://www.jstor.org/stable/26202071.
2. Stephen Marrin, "Improving Intelligence Studies as an Academic Discipline," *Intelligence and National Security* 31, no. 2 (May 2014): 1–14, https://doi.org/10.1080/02684527.2014.952932.
3. Benedict Anderson, *Imagined Communities: Reflections on the Origin and Spread of Nationalism,* rev. ed. (Verso, 2006), 6.
4. Mark M. Lowenthal, *Intelligence: From Secrets to Policy,* 7th Ed. (CQ Press, 2017).
5. Jennifer E. Sims, *Decision Advantage: Intelligence in International Politics from the Spanish Armada to Cyberwar* (Oxford University Press, 2022).
6. Loch K. Johnson, *National Security Intelligence: Secret Operations in Defense of the Democracies* (Polity, 2012).
7. Peter Gill and Mark Phythian, *Intelligence in an Insecure World,* 3rd Ed. (Polity, 2018), 118.
8. Michael Warner, "Intelligence in Cyber—and Cyber in Intelligence," in *Understanding Cyber Conflict: Fourteen Analogies,* eds. George Perkovich and Ariel E. Levite (Georgetown University Press, 2017), 22.

9. Michael Herman, *Intelligence Power in Peace and War* (Cambridge University Press, 1996), 100–12.
10. Marrin, "Improving Intelligence Studies as an Academic Discipline."
11. Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton University Press, 1949), 3–4.
12. Rob Johnston, *Analytic Culture in the US Intelligence Community: An Ethnographic Study* (CIA, Center for the Study of Intelligence, 2005).
13. Tony Becher, *Academic Tribes and Territories: Intellectual Enquiry and the Cultures of Disciplines* (Open University Press, 1989), 41.
14. Armin Krishnan, "What Are Academic Disciplines? Some Observations on the Disciplinarity vs. Interdisciplinarity Debate," Economic and Social Research Council/National Centre for Research Methods (ESRC/NCRM), NCRM Working Paper Series 03/09 (NCRM, January 2009), 9, https://eprints.ncrm.ac.uk/id/eprint/783/.
15. Klaus Knorr, *Foreign Intelligence and the Social Sciences* (University Press of America, 1986).
16. Michael Warner, "Wanted: A Definition of 'Intelligence': Understanding Our Craft," *Studies in Intelligence* 46, no. 3 (2002), https://www.cia.gov/resources/csi/static/Wanted-Definition-of-Intel.pdf.
17. Marrin, "Improving Intelligence Studies as an Academic Discipline."
18. Christopher Andrew, *The Secret World: A History of Intelligence* (Yale University Press, 2018).
19. Gill and Phythian, *Intelligence in an Insecure World.*
20. Richard J. Aldrich, *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency* (HarperCollins, 2010).
21. Lowenthal, *Intelligence: From Secrets to Policy.*
22. National Intelligence University, *Catalog for Academic Year 2025-26*, accessed August 29, 2025, https://www.ni-u.edu/wp-content/uploads/2025/08/NIUs-Academic-Catalog-25-26_Final_Web.pdf.
23. Frederic Baron, "Why Define Intelligence?" Ann Caracristi Institute for Intelligence Research, National Intelligence Press, *Research Short,* March 28, 2024, https://www.ni-u.edu/wp-content/uploads/2024/04/Why-Define-Intelligence.pdf.
24. Adrian Wolfberg, "In Pursuit of Insight The Everyday Work of Intelligence Analysts Who Solve Real World Novel Problems," Ann Caracristi Institute for Intelligence Research, National Intelligence Press, *Research Monograph,* Spring 2022, https://www.ni-u.edu/wp-content/uploads/2023/09/NIUMonographWolfberg2022_DNI2022_02011.pdf.
25. Stacey Pollard and Adrian Wolfberg, "Establishing Causation in Political Science and Public Administration Research," in *Teaching Graduate Political Methodology,* eds. Mitchell Brown, Shane Nordyke, and Cameron G. Thies (Edward Elgaronline, 2022), https://www.e-elgar.com/shop/usd/teaching-graduate-political-methodology-9781800885271.html.
26. Julie Ferringer, "The Science of Teamwork in the Intelligence Community," Ann Caracristi Institute for Intelligence Research, National Intelligence Press, *Research Short,* September 30, 2024, available upon request to: NIU_NIPress@niu.odni.gov.
27. Josh Kerbel, "The US Talks a Lot About Strategic Complexity. Too Bad It's Mostly Just Talk," *Defense One,* March 9, 2021, https://www.defenseone.com/ideas/2021/03/us-talks-lot-about-strategic-complexity-too-bad-its-mostly-just-talk/172549.
28. Josh Kerbel and LTC Tom Pike (USA), "Anticipatory Intelligence and Adaptive Influence: A New Paradigm for Foreign Policy Development," Ann Caracristi Institute for Intelligence Research,

National Intelligence Press, *Research Short,* July 10, 2020, https://www.ni-u.edu/wp-content/uploads/2023/11/NIUShort_07102020_20C_167ITWOrd.pdf.
29. Mark Bailey, "Understanding and Mitigating the Long-Term Risks of AI Operationalization," Ann Caracristi Institute for Intelligence Research, National Intelligence Press, *Research Short,* March 1, 2023, https://www.ni-u.edu/wp-content/uploads/2023/11/NIUShort_20230301_DNI_2023_0085_LTR.pdf.
30. Richard Uber, "China's Artificial Intelligence Ecosystem," Ann Caracristi Institute for Intelligence Research, National Intelligence Press, *Research Monograph,* December 21, 2020, available upon request to: NIU_NIPress@niu.odni.gov.
31. Stephen Hood, "The Devil You Don't Know: The Need for Joint Human-AI Decisionmaking Outcomes Assessments for Human-in-the-Loop AI Models," Ann Caracristi Institute for Intelligence Research, National Intelligence Press, *Research Monograph,* Summer 2023, https://www.ni-u.edu/wp-content/uploads/2023/09/NIUMonographHood2023_DNI_2023_02676.pdf.
32. Thomas M. Dolan, "Emotion and Strategic Learning in War," *Foreign Policy Analysis* 12, no. 4 (October 2016): 571–90. https://www.jstor.org/stable/26168122.
33. Dennis J. King, "Channeling Cassandra Humanitarian Intelligence and Decisionmaking in the Age of Complexity," Ann Caracristi Institute for Intelligence Research, National Intelligence Press, *Research Monograph,* Fall 2024, https://www.ni-u.edu/wp-content/uploads/2024/11/NIUMonograph King2024_DNI_2024_04334.pdf.
34. Amy Sturm, "Assessing the Global War on Terror: Measuring the Impact of US Foreign Terrorist Organization Designation on Salafi Jihadis Group Behavior," Ann Caracristi Institute for Intelligence Research, National Intelligence Press, *Research Monograph,* Spring 2023, available upon request to: NIU_NIPress@niu.odni.gov.
35. Stacey Pollard et al., "Islamic State Resurgence in the Era of COVID-19," Ann Caracristi Institute for Intelligence Research, National Intelligence Press, *Research Short,* March 17, 2021, https://ni-u.edu/wp-content/uploads/2023/11/NIUShort_03172021_21C099Gaza.pdf.
36. King, "Channeling Cassandra."
37. Albert Bandura, *Self-Efficacy: The Exercise of Control* (W. H. Freeman, 1997), 477.
38. Albert Bandura, "Exercise of Human Agency Through Collective Efficacy," *Current Directions in Psychological Science* 9, no. 3 (2000): 75–78, https://www.jstor.org/stable/20182630.
39. Bandura, "Exercise of Human Agency Through Collective Efficacy."
40. Herman, *Intelligence Power in Peace and War.*
41. Gill and Phythian, *Intelligence in an Insecure World.*
42. Marrin, "Improving Intelligence Studies as an Academic Discipline."
43. Sims, *Decision Advantage.*
44. Warner, "Intelligence in Cyber—and Cyber in Intelligence."
45. Anderson, *Imagined Communities.*
46. Johnson, *National Security Intelligence.*

EXPLORING THE EVOLUTION OF CYBER INTELLIGENCE (CYINT): A Disciplinary Debate and Practical Implications for Intelligence Professionals

James (Jim) Austin

INTRODUCTION

Cyber intelligence (CyINT) is emerging as a standalone discipline distinguished from traditional intelligence disciplines due to its focus on the digital realm and its unique challenges. When asked the question, artificial intelligence (AI) stated the same and quoted sources that identified CyINT as becoming a disciplined methodology,[1] characterised it as an all-source intelligence product,[2] and emphasised the importance of clearly understanding CyINT in the broader cybersecurity arena.[3] None of these examples specifically supports the premise of CyINT as a discipline, and AI categorised CyINT as emerging.[4] In fact, the views differ because the majority of intelligence disciplines overlap the cyber realm. This paper explores this question from the perspective of cyber overlapping all intelligence domains using research conducted in the maritime domain, and the development of a multinational CyINT course.

Examination of the general cyber threat environment demonstrates the dangers dealt with around the globe and provides further context to the maritime Cyber Threat Intelligence (CTI) research. Continuing further into the maritime domain this research scrutinises recent maritime cyber events, exploring the current state of digitisation in port facilities, and reviews case studies for valuable learnings. Investigation of the current state of maritime CTI and recent incidents relating to submarine cables demonstrate the reliance these critical infrastructures have on CyINT, and conversely, the reliance of society on them. Considering all these facets contextually against the future challenges of maritime CTI demonstrates a requirement for CyINT over CTI, supporting the premise that—discipline or not—CyINT is a requirement.

Building on this premise, the paper then scrutinises the process and observations derived during the redevelopment of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) CTI course

into a CyINT course. Developed from a multinational operations mindset, the process provides valuable insight supporting the concept of applying current intelligence processes into the cyber realm. Differentiating between CyINT and CTI, the course redevelopment reveals a common international requirement for intelligence professionals to understand their tradecraft as it applies to the cyber domain. Finally, the research considers these points as applied to research and development providing guidance on the way forward and examples of current and future research intent.

GENERAL THREAT ENVIRONMENT

The cyber threat landscape is a complex and challenging environment; advances in critical and emerging technologies offer both a bane and a boon in dealing with cyber threat. Advanced persistent threats (APT) target government and military entities, critical infrastructure, and industry using ever more advanced methodologies to conduct espionage, exert influence, disrupt, and interfere in pursuit of their goals. During 2024, national cyber security agencies released joint advisories highlighting state-sponsored cyber activities. These assessments advised that China is likely prepositioning for disruptive actions while maintaining extant espionage activities, and that Russia is further developing sophisticated techniques with a particular focus on cloud platforms.[5] Advancements in defensive threat technologies and awareness have seen adversaries increasingly use complex tactics, techniques, and procedures (TTP) that allow them to move more rapidly and remain undetected.[6]

At their core, a diversity of threats are consolidated into categories for the purpose of analysis. The prime threat categories in the cyber environment are 1) ransomware, 2) malware, 3) social engineering, 4) threats against data, 5) threats against availability, 6) information manipulation, and 7) supply chains.[7] According to Google, ransomware, data theft extortion, and multifaceted extortion are major threats for 2025 and have already affected more than 100 countries and every industry vertically. Infostealer malware to gather credentials is expected to remain a primary threat vector, and while not a new threat, it has advanced in sophistication.[8] These threats are consistent, with the result that the threats faced by the maritime industry are similar regardless of geographical location; that is, in general the APTs and TTPs used by them are the same if not similar in Europe, the Americas, and the Asia-Pacific region. Therefore, rather than addressing the threat landscape from the perspective of specific APTs and TTPs, analysis and observations herein are based on issues identified as relevant to CTI in the maritime environment and port facilities as they may relate to critical infrastructure.

MARITIME THREAT ENVIRONMENT

Maritime infrastructure and its supporting information technology (IT) and operational technology (OT) are vital for civil society and military operations. These networks face a multitude of dangers from APTs that continuously develop TTPs to evade detection and overcome generic security measures. Rising in frequency and complexity, response times to cyberattacks are decreasing, and boundaries of responsibility

are no longer permanent.[9] This development can be demonstrated by the discovery of ArcaneDoor in May 2024, which was reported to use custom malware leveraging known vulnerabilities to collect maritime and financial intelligence. Consisting of significant IT infrastructure, the campaign spread across coastal facilities in numerous countries that were identified as strategically important.[10]

CURRENT STATUS OF DIGITALISATION IN MARITIME PORT FACILITIES

Carrying more than 90 percent of global trade and between 8 and 12 percent of global gross domestic product (GDP), the maritime industry is the lifeblood of global trade. Digital technology's integration into the maritime industry has revolutionised port operations by enabling real-time tracking, and predictive maintenance, and by automating cargo handling. The continued growth of maritime trade requires evolution into smart, interconnected hubs to address operational bottlenecks and pave the way for ports to become crucial nodes in the global supply chain. Conversely, these advancements also increase the threat surface of exploitable vulnerabilities, which necessitate effective and resilient cybersecurity practices.[11]

Digitalisation efforts in maritime port facilities vary significantly across geographical regions reflecting differing levels of technological adoption and investment. Key technologies shaping the digital landscape of ports include:

Internet of Things (IoT): IoT is used extensively for real-time monitoring and management of cargo, equipment, and environmental conditions. Sensors embedded in containers and port infrastructure provide continuous data streams, enabling predictive maintenance and reducing downtime; i.e., the Port of Hamburg, Germany, employs IoT to optimise traffic management and environmental monitoring.

Blockchain: Blockchain technology is being used in port documentation and transaction processes as a secure and immutable ledger to ensure transparency and traceability of cargo movements and trade documents; i.e., the Port of Antwerp, Belgium, has implemented blockchain-based solutions to streamline customs processes, reducing clearance times and enhancing security.

Digital Twins: Digital twins are virtual replicas of physical port assets, which enable real-time simulation and analysis. This technology provides port operators the ability to test scenarios, optimise operations, and predict potential issues before they occur; i.e., the Port of Rotterdam, Netherlands, is a pioneer in the use of digital twins, employing them to enhance asset management and operational efficiency.

Artificial Intelligence: AI-driven analytics and machine learning algorithms are increasingly being adopted to optimise logistics, automate administrative tasks, and enhance decisionmaking; i.e., ports, such as Singapore's PSA International, leverage AI to improve container-handling efficiency and resource allocation.[12]

LESSONS LEARNED FROM THE MARITIME APT CASE ANALYSIS

The adoption of digital technologies in maritime port facilities offers numerous advantages—such as operation efficiency, cost reduction, transparency, and customer experience—along with security and sustainability. Conversely, disadvantages include high initial investment costs, lack of standardisation, increased cybersecurity risk, and job displacement. In the context of these advantages and disadvantages, analysis of APT cases targeting the maritime sector has provided valuable lessons learnt for consideration in the maritime environment.

Case Study 1: Chinese APT Groups Targeting Maritime Shipping

Increasingly, Chinese APT groups target the maritime industry by installing malware on critical port infrastructure, such as cranes,[13] to disrupt operations and gather intelligence. This example highlights the vulnerability of OT systems within port facilities and demonstrates a need for robust security and assurance measures for OT systems, along with the requirement to share that knowledge within the maritime community.[14]

Case Study 2: DONOT APT's Attack on Maritime and Defence Manufacturing

The DONOT APT group, also known as APT-C-35, has targeted maritime and defence manufacturing sectors in South Asia using malicious link (LNK) files disguised as ransomware task force (RTF) documents. The files deployed and executed stager malware, an initial payload that established persistence and communicated with command-and-control (C&C) servers aimed at exfiltrating sensitive information and disrupting operations. This type of attack is significantly negated by educating employees about social engineering and phishing attack vectors, and implementing advanced threat detection and response mechanisms. The combination of education and technological defence—that is, endpoint detection—can meaningfully mitigate these threats.[15]

Case Study 3: APT Groups in India Targeting Geostrategic Zones

APT groups in India actively target geostrategic maritime infrastructure in countries such as Pakistan, Sri Lanka, and Bangladesh. Often involving cyber espionage and disruption of critical maritime operations, this activity appears to be escalating, which underscores the need for heightened cybersecurity measures in the region. Collaboration and information sharing via joint exercise and sharing threat intelligence can collectively enhance regional cybersecurity, particularly when combined with regular system updates and security assessment to maintain resilience.[16]

Case Study 4: NotPetya Cyberattack on Maersk's Global Operations

The 2017 NotPetya cyberattack exemplifies the risks associated with inadequate maritime cybersecurity via its disruption of Maersk's global operations which cost the shipping company an estimated US $300 million.[17] This attack leveraged a compromised third-party software update to exploit unpatched vulnerabilities that allowed malware to spread rapidly through Maersk's network. The flat network employed by Maersk facilitated the malware's lateral movement, demonstrating the value of segmented networks in cyber security; fortunately, critical data were backed up allowing for an expedited recovery, again demonstrating regular data backup as a best practice. Similarly, professional

patch management would have greatly reduced the network's vulnerability to exploitation, and regular employee awareness training would support a best-practice culture. The final lesson derived from this case study is possibly the most topical; i.e., the threat originating from a third-party supply chain identifies the need for stringent vetting and monitoring of vendor security practices.[18]

CRITICAL INFRASTRUCTURE

In terms of critical infrastructure, 99 percent of digital communications transit the globe via submarine cables that extend approximately 1.3 million kilometers.[19] Additionally, submarine cables are now influenced by more external factors, including large-scale cloud and content providers and the strategic actions of major powers and minilateral groups. Cyber vulnerabilities within legacy and third-party IT and OT cable landing systems (CLS)—such as interconnecting terrestrial networks—require attention in conjunction with the physical aspects. Disregarding natural disaster, submarine cables are vulnerable to physical tampering and—when concentrated in chokepoints, such as the Luzon Strait and Malacca Strait, or in contested waters, such as the South China Sea—are particularly vulnerable.[20] These vulnerabilities have been highlighted recently by several incidents worldwide; i.e., Finland seized the alleged Russia-linked ship Eagle S, suspected of breaking submarine cables in the Baltic Sea.[21] Sweden, Finland, and Lithuania also halted a Chinese-flagged commercial ship over its possible involvement in similar activities in the Baltic, and Taiwan is investigating another potentially China-linked vessel for damaging undersea cables connecting Taiwan to the internet.[22]

MARITIME CYBER THREAT INTELLIGENCE

Use of CTI is growing within the public and private sectors, increasingly in conjunction with threat-hunting and vulnerability management. Using CTI sources external to the enterprise, particularly open-source intelligence (OSINT), has become a focus of consumers. In its current state, CTI technology can collect and analyse large amounts of data easily, manage indicators of compromise (IoC) effectively, and disseminate IoCs effortlessly. The negative impact of CTI's use is losing sight of intelligence requirements and stakeholder needs within the deluge of information. Therefore, in the constantly dynamic maritime CTI environment, the cost-benefit calculus of tools-to-personnel ratios needs to be continually assessed, knowledge management principles established, and processes developed to deliver an intelligence function over a technological focus.[23]

To maintain a holistic threat picture inclusive of other intertwined domains, maritime CTI must endeavour to capture both the obvious and esoteric threats to the domain. This need is exemplified by analysis from Microsoft identifying that China-based threat actors have targeted entities in the South China Sea, with a particular focus on the Association of Southeast Asian Nations (ASEAN). One APT successfully penetrated military and executive assets within both the Indonesian and Malaysian maritime systems prior to naval exercises in June 2023.[24] Separate analysis of global traffic at Akamai Technologies further identifies a rise in distributed denial of service (DDoS) attacks targeting Europe. Second only to the United States,

these DDoS attacks are trending toward domain name systems (DNS), indicating a need for protection via mitigation controls, intimate system knowledge, and contemporary response plans. This research also found that using hybrid platforms and environmental stress testing can build resilience.[25] Information from another source demonstrates that, although GPS spoofing has been a prominent maritime threat for a few years, the combined use of GPS jamming and spoofing appears to be an emerging trend.[26] When directly related to the maritime environment, example 1 appears to be peripheral, example 2 unconnected, and example 3 maritime-specific. In combination, however, they identify maritime intent, a likely attack vector, and a potential threat outcome, demonstrating the need for a holistic hybrid CyINT function.

FUTURE CHALLENGES TO MARITIME CYINT

The major external challenges occurring in the cyberspace threat landscape are adversaries taking control of unmanned assets and AI-enabled cyberattacks. Organisations also face, however, the internal challenge of overcoming the reluctance to share information with partners and industry for a holistic threat picture. Digitising legacy systems, collaborative combat, complex supply chains, and trustworthy AI are additional challenges within an evolving threat landscape. Accenture has identified that AI is reshaping the threat landscape via its use for disinformation campaigns, targeting and malware automation, honing social engineering and deepfakes, and monitoring for insider threat activity. The offensive capability of APT actors is increasing as AI has improved the efficiency of large-scale attacks and enhanced reconnaissance and intelligence gathering. As an example, APTs attributed to China, Russia, and the DRPK all conducted cyber espionage activities utilising AI in 2024, and hacktivism also saw the use of AI for vulnerability identification and exploitation.[27]

As technology and process mature together, there is an opportunity to develop a truly integrated maritime cybersecurity community inclusive of government, academia, and industry. Extant examples exist, such as the Nordic Maritime Cyber Resilience Centre (NORMA) that provides its members with threat intelligence, incident response, and penetration testing services.[28] In the United States, the National Maritime Intelligence-Integration Office (NMIO) has established the Global Maritime Community of Interest (GMCOI), consisting of the Intelligence Community, other non-intelligence government departments of all levels, academia, industry, and foreign partners.[29] In 2018, the Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP) was identified as an information-sharing centre of excellence.[30] Whether truly successful integration of maritime information has been achieved is open to interpretation, however, as holistic information sharing was identified as a challenge as recently as September and October 2024, and there is definitely room for improvement.

SHOULD CYINT BE DOMAIN SPECIFIC?

As the boundaries and responsibilities between national and international, and public and private entities are blurred, maritime cybersecurity requires enhancement to ensure its safety. The maritime sector remains

a high-risk cyber environment requiring a comprehensive understanding of the maritime IT and OT ecosystem.[31] Consequently, the hybrid nature of the maritime environment cannot be overlooked; specifically, IT and OT underpin all land- and sea-based maritime operations. As an example, reports of suspicious Russian vessels near critical infrastructure are numerous, and emerging technologies such as maritime drones are being utilised effectively in Ukraine.[32] Research also shows that China uses hybrid operations including maritime aggression, cyber operations, economic coercion, and information operations.[33] A positive example is the use of this technology to analyse Baltic Sea maritime traffic after damage to the Baltic connector gas pipeline in Finland's economic zone and to two submarine communications cables in Estonia's economic zone. The assessment determined the incidents were interconnected and identified a suspect vessel under a Chinese flag.[34] The interlinkages between the maritime and other domains highlight that what happens in one domain will ultimately affect others, and that the information domain is generally the domain most used to cause disruption.[35] Essentially, the multitude of interactive services and requirements utilised within the maritime environment establishes that it cannot protect itself in isolation.

This analysis of the maritime environment from a cyber intelligence perspective demonstrates that the problems faced there are not distinctly maritime-related. The IoT, blockchain, AI, and their derivatives are all widely known agents of change identified in almost every strategic assessment.[36] Threats manifesting in the maritime environment, both specific and general, are analogous to other industries and environments; i.e., case study one (Chinese APT Groups) shares similarities with cyberattacks against automotive industry OT, specifically air-powered torque wrenches called nutrunners,[37] and case study two (DONOT APT) fits the profile of a myriad of other supply chain attacks.[38] What is distinctly different is the physical environment in which the IT and OT are expected to operate and which by itself brings significant challenges.[39] When analysed from the CyINT viewpoint, however, the cybersecurity risks, issues, and challenges are inherently comparable to the majority of other operating environments.

The divergence and congruity within these examples demonstrate that the argument of CyINT as an individual intelligence discipline is irrelevant because, either way, the intelligence profession must deal with the cyber realm. This assertion has led to the redevelopment of the NATO CCDCOE CTI course as a cyber for intelligence professionals course.[40] Observations and discussions during the development of the CyINT course generally support the argument that the intelligence process is applied to the cyber domain, as opposed to any need to develop new cyber-related intelligence techniques.

CYBER THREAT INTELLIGENCE OR CYBER INTELLIGENCE

Research has identified that, although all domains use the cyber domain to conduct intelligence activities to differing extents, the same intelligence processes are used across domain-specific assets and resources. As an example, when conducting the intelligence process for intelligence, surveillance, and reconnaissance (ISR) in any domain, cyber is used to facilitate the intelligence process and is rarely if ever the sole driver for conducting it. Due to its technical nature, CTI is not in itself CyINT, but more a contributor to it.[41] Additionally, CyINT is not recognised as an intelligence discipline and, although similarities exist within

friendly nations, no recognised or consistent taxonomy can be applied.[42] Defining CyINT has evolved, but no consensus exists; one definition posits that CyINT is based on analysis of data extracted from hostile adversarial cyber domains, while another contradicts by stating that CyINT is an analytical discipline derived from traditional intelligence.[43] As recently as 2023, Izzat Alsmadi, author of *The NICE Cyber Security Framework,* stated that CyINT has evolved as a discipline; however, it deals with an elusive and dynamic spectrum of intelligence that can pivot on a single piece of malware.[44] Consequently, there is a requirement to differentiate between CyINT and CTI because, while not dissimilar, they differ in scope and purpose.[45] Interestingly, despite the differing views on CyINT as an individual intelligence discipline, all agree that the majority of intelligence disciplines overlap the cyber realm.

CYBER INTELLIGENCE COURSE DEVELOPMENT

Because the CCDCOE is a NATO-accredited training centre, the cyber intelligence course was developed in line with the systems approach to training (SAT) methodology.[46] Definitions of the SAT vary; however, it is safe to say that SAT is a methodology for managing training programs and it uses orderly and logical approaches for determining training requirements in relation to a particular job or profession.[47] While CCDCOE is a cyber-specific institution that provides research, education, and counsel on conducting operations in the cyber realm, intelligence expertise still remains within the Intelligence Community. Therefore, the Intelligence Community is best placed to identify what is needed to write and maintain intelligence doctrine, with advice and guidance from subject matter experts (SME) such as CCDCOE. The doctrine custodial perspective also identifies significant resources that are required when writing and maintaining doctrine. Therefore, developing a CyINT process is nation-specific and should be supported by SMEs.

The CCDCOE cyber for intelligence professionals course has its roots in both the Multinational Capability Development Campaign (MCDC) and the CCDCOE. The MCDC is a group of 25 nations with a focus on collaboratively developing and accessing concepts and capabilities to address the challenges associated with conducting coalition and multinational operations.[48] A combined effort saw intelligence and education professionals from multiple nations unite for a set of working groups that developed the course control documents (CCD) in line with the SAT process. During this process both intelligence and education SMEs continually challenged the premise of CyINT as a discipline. Education specialists maintained directive control, giving intelligence experts the freedom to continually challenge each other's opinions. These deliberations ultimately resulted in consensus that delivering a product that guides and advises the intelligence process into and through the cyber environment should be the goal. The process was further enhanced by including specialists from multiple nations to provide the varied expertise needed to design a product of use in many sectors. Because the MCDC is a conceptual entity, it was decided that the CCDCOE, an organisation with both resources and expertise, would develop and deliver the product.

To ensure the integrity of the process and validate assumptions, the final product of the workshops and coordinated feedback sessions—that is, the CCD III—required further socialisation. The CyINT CCD

III was then disseminated to likeminded nations and academic SMEs with a request for feedback. All feedback agreed that the premise of a CyINT course that overlays the extant intelligence process across the cyber domain was correct, and that the intended course content aligned with extant national concepts. The majority of feedback centred around process configuration, lexicon development, lesson expansion, and effective knowledge delivery methodology.[49] The CyINT course development process and external feedback, therefore, further supports the assertion that whether CyINT is a discipline is irrelevant: there is a requirement for intelligence application to the cyber domain, the current intelligence process applies, and how practitioners gather and interpret the knowledge is crucial. This agreement has led the CCDCOE to commit future resources for CyINT research and development.

RESEARCH AND DEVELOPMENT

CyINT is developing independently across the globe at varying rates dependent on national, industry, and academic priorities. The US Cybersecurity and Infrastructure Security Agency (CISA) cites the following objective in its *Cybersecurity Strategic Plan for FY 2024-2026*: Plan for, exercise, and execute joint cyber defence operations and coordinate the response to significant cybersecurity incidents.[50] This response indicates improving the extant process and procedure rather than developing new ones. The Australian *2023-2030 Cyber Security Strategy* demonstrates a shift from technical cyber to a whole-of-nation approach with a focus on better support to civilians and industry.[51] Both these documents have similarities with intended outcomes—resilience, critical infrastructure, and societal partnerships[52]—but the pathways to achieving the outcomes appear to be somewhat divergent. The maturity of the different cyber landscapes may play a role in differing approaches, particularly when resource and economic size are factored in the strategy. A small country such as Estonia has economic limitations that the United States and Australia do not have, yet a country's smaller size can provide an advantageous agility when implementing new technology or cultural change.[53] As demonstrated in the context of CyINT, current research and opinion agree that CyINT is a requirement, and the application and training to achieve effective CyINT requires further analysis. As an example, a CISA-endorsed Cyber Intelligence Professional certification includes intelligence, investigation, crime, and analysis modules that significantly rely on technical achievement,[54] yet this would appear to be more CTI-relevant.

In developing the CyINT course described above, the CCDCOE has moved significantly down the path toward developing a consistent taxonomy and consensus at the operational level. The first official course scheduled for November 2025 will further these endeavours. Concurrently, CCDCOE is conducting research into a CyINT framework with the intent of delivering a CyINT handbook in 2026-2027. The MCDC will also be validating previous research and products during its 2025-2027 project cycle that will inform CyINT operational research, particularly from a multinational perspective. Several nations have recently developed parallel courses and some are in the process, while others await research results before committing to a particular path. Applicable to strategic, operational, and tactical levels, CyINT is now a required capability for all nations, and conducting CyINT in the best, most efficient manner should be a research and development focus for all.

CONCLUSION

This paper argues that whether CyINT is a distinct discipline does not matter in the grand scheme because the intelligence profession must deal with the cyber realm. Our research identified that the difference between the maritime cyber threat landscape and the general cyber threat is not significant. Examination of cyber incidents has provided lessons that apply across all intelligence domains, including critical infrastructure, and illustrated a requirement for a holistic and inclusive CyINT approach. The requirement exists to practice intelligence skills within the cyber realm regardless of the domain; therefore, any CyINT should facilitate the intelligence process using cyber methodologies. Operationally, this objective has been recognised and has been, or is being, developed in multiple nations and by multinational organisations. Although CyINT as a necessity has never been in dispute, a lack of clarity for application and definition has retarded the ability to understand exactly what is needed. Producing a common lexicon across multinational boundaries inclusive of standardised training objectives will deliver the effective communication required to deliver a holistic and inclusive CyINT capability to all intelligence domains.

James Austin is currently working as the Australian defence liaison officer at the NATO Cooperative Cyber Defence Centre of Excellence. As a senior researcher in the Operations Branch, he serves as the project lead of Cyber Intelligence and Capability Development projects. Mr. Austin has more than 20 years of experience in analysis, investigation, project management, and risk and change management. He has developed and implemented innovative concepts for government agencies and presented at the International Political Science Association World Congress in Korea, Portugal, and Finland, along with the International Association of Intelligence Education in Treviso, Italy.

ENDNOTES

1. George Bamford et al., *Operational Levels of Cyber Intelligence,* Volume 1 of INSA Cyber Intelligence Task Force white paper (Intelligence and National Security Alliance, 2013), https://books.google.com/books/about/Operational_Levels_of_Cyber_Intelligence.html?id=JbZQnwEACAAJ.
2. Christopher Seedyk, "Characterizing Cyber Intelligence as an All-Source Intelligence Product," Defense Systems Information Analysis Center, November 2, 2019, https://dsiac.dtic.mil/articles/characterizing-cyber-intelligence-as-an-all-source-intelligence-product/.
3. Matteo E Bonfanti, "Cyber Intelligence: In Pursuit of a Better Understanding for an Emerging Practice," *Cyber, Intelligence, and Security* 2, no. 1 (May 2018): 105–21, https://www.inss.org.il/wp-content/uploads/2018/05/Cyber-Intelligence-In-Pursuit-of-a-Better-Understanding-for-an-Emerging-Practice.pdf.
4. "Define CyINT," Copilot Application Questioned, January 3, 2025, 1:27pm.

5. *Annual Cyber Threat Report 2023-2024,* Australian Signals Directorate, November 20, 2024, https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024.
6. *2024 Global Threat Report,* CrowdStrike, accessed January 3, 2025, https://www.crowdstrike.com/en-us/resources/reports/crowdstrike-2024-global-threat-report/.
7. *ENISA Threat Landscape 2024,* European Union Agency for Cybersecurity (ENISA), April 30, 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.
8. Adam Greenberg, *Emerging Threats: Cybersecurity Forecast 2025,* Google Cloud, November 13, 2024, https://cloud.google.com/security/resources/cybersecurity-forecast-2025.
9. Cooperative Cyber Defence Centre of Excellence (CCDCOE), "Strategic View, Cyber Defence Concepts, and the Threat Landscape" in *Cyber Commanders Handbook* (CCDCOE, 2025).
10. "China-Linked Hackers Suspected in ArcaneDoor Cyberattacks Targeting Network Devices," *The Hacker News,* May 6, 2024, https://thehackernews.com/2024/05/china-linked-hackers-suspected-in.html.
11. CCDCOE, *Maritime Critical Infrastructure Project: Port Cyber Threat Intelligence Analysis,* February 2025.
12. CCDCOE, *Maritime Critical Infrastructure Project.*
13. US Congress, House, Committee on Homeland Security, "WTAS: Joint Investigation into CCP-Backed Company Supplying Cranes to US Ports Reveals Shocking Findings," News, March 12, 2024, https://homeland.house.gov/2024/03/12/wtas-joint-investigation-intoccp-backed-company-supplying-cranes-to-u-s-ports-reveals-shocking-findings/.
14. Edwin Taylor, "Maritime Shipping: Cyber Actors Threaten Global Routes," *Grey Dynamics,* October 26, 2024, https://greydynamics.com/maritime-shipping-cyber-actors-threaten-global-routes/.
15. Cypriaan Sueur and Lisa Luijkx, "All Hands on Deck: Attackers Have Entered the Maritime Industry," Hunt and Hackett, September 30, 2021, https://www.huntandhackett.com/blog/all-hands-on-deck-attackers-have-entered-the-maritime-industry.
16. Taylor, "Maritime Shipping."
17. Joachim Rosenoegger, "The Rogue Wave of NotPetya Sent Shockwaves Through the Maritime Industry," LinkedIn, December 15, 2024, https://www.linkedin.com/pulse/rogue-wave-notpetya-sent-shockwaves-through-maritime-rosenoegger-sp5me.
18. International Maritime Organization, "NotPetya Cyberattack: Lessons for the Maritime Sector," 2018.
19. Author's general observations and discussions, September 18, 2024.
20. Jocelinn Kang and Jessie Jacob, "Connecting the Indo-Pacific: The Future of Subsea Cables and Opportunities for Australia," Australian Strategic Policy Institute, September 25, 2024, http://www.aspi.org.au/report/connecting-indo-pacific-future-subsea-cables-and-opportunities-australia/.
21. Alexander Martin, "Finland Identifies Seven Suspects Among Crew of Alleged Russian 'Spy' Tanker," The Record, December 31, 2024, https://therecord.media/finland-suspects-identified-alleged-russian-spy-ship.
22. Meaghan Tobin, Muyi Xiao, and Amy Chang Chien, "Taiwan Says It Suspects a Chinese-Linked Ship Damaged an Undersea Internet Cable," *New York Times,* January 2025, https://www.nytimes.com/2025/01/07/world/asia/taiwan-internet-cable-china.html.

23. Andreas Sfakianakis, "CTI in the Age of AI: Emerging Trends, Challenges, and Transformative Technologies," presentation at the 8th NMIOTC Conference on Cyber Security in the Maritime Domain, Crete, Greece, September 19, 2024, https://nerocybersecurity.eu/events/8th-nmiotc-conference-cybersecurity-maritime-domain-2024.
24. *Microsoft Digital Defense Report 2024: The Foundations and New Frontiers of Cybersecurity,* Microsoft Threat Intelligence, October 2024, https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf.
25. Richard Meeus, "Lessons from Analysing Global Traffic: Europe's Rise as the Top DDoS Target," presentation at the 2024 ENISA Cyber Threat Intelligence Conference, Brussels, Belgium, October 1, 2024, https://www.enisa.europa.eu/sites/default/files/2024-11/2024_cti_conference_agenda-4.pdf.
26. Yann Bozac, "Operationalising the Maritime Cyberspace: Continuing the Conversation," presentation at the 8th NMIOTC Conference on Cyber Security in the Maritime Domain, Crete, Greece, September 18, 2024, https://nerocybersecurity.eu/events/8th-nmiotc-conference-cybersecurity-maritime-domain-2024.
27. Valentino de Sousa, "Threat Analysis and Artificial Intelligence," presentation at the 2024 ENISA Cyber Threat Intelligence Conference, Brussels, Belgium, October 1, 2024, https://www.enisa.europa.eu/sites/default/files/2024-11/2024_cti_conference_agenda-4.pdf.
28. Nordic Maritime Cyber Resilience Centre (NORMA), "Members Get Access to Centralised Cyber Security Functions and Services Tailored for the Maritime Industry," NORMA Cyber, accessed January 3, 2025, https://www.normacyber.no/en/services.
29. "About NMIO," National Maritime Intelligence-Integration Office (NMIO), accessed January 3, 2025, https://nmio.ise.gov/About/.
30. "About ReCAAP Information Sharing Centre," ReCAAP Information Sharing Centre, accessed January 3, 2025, https://www.recaap.org/about_ReCAAP-ISC.
31. Emre Halisdemir et al, "Cyber Threat Intelligence: Mitigating Risks to Maritime Security," CCD-COE, 2023.
32. Henrik Praks, "Russia's Hybrid Threat Tactics Against the Baltic Sea Region: From Disinformation to Sabotage," European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE Working Paper 32, May 2024, https://www.hybridcoe.fi/wp-content/uploads/2024/05/20240530-Hybrid-CoE-Working-Paper-32-Russias-hybrid-threat-tactics-WEB.pdf.
33. Todd Helmus et al., *Understanding and Countering China's Maritime Gray Zone Operations,* RAND Corporation, November 20, 2024, https://www.rand.org/pubs/research_reports/RRA2954-1.html.
34. Estonian Internal Security Service, *Annual Review 2023-2024,* December 2024, https://news.err.ee/1609309593/internal-security-service-publishes-2023-2024-annual-review.
35. Anneli Ahonen et al., *Russia's Information Influence Operations in the Nordic – Baltic Region,* NATO Strategic Communications Centre of Excellence, November 2024, https://stratcomcoe.org/publications/russias-information-influence-operations-in-the-nordic-baltic-region/314.
36. *ENISA Threat Landscape 2024,* European Union Agency for Cybersecurity.

37. Eduard Kovacs, "Bosch Nutrunner Vulnerabilities Could Aid Hacker Attacks Against Automotive Production Lines," *Security Week,* January 9, 2024, https://www.securityweek.com/bosch-nutrunner-vulnerabilities-could-aid-hacker-attacks-against-automotive-production-lines/.
38. "Supply Chain Attacks: Impact, Examples and 6 Preventive Measures," Hackerone Knowledge Center, accessed January 3, 2025, https://www.hackerone.com/knowledge-center/supply-chain-attacks-impact-examples-and-6-preventive-measures.
39. "Guidelines on Maritime Cyber Risk Management," International Maritime Organization, accessed January 3, 2025, https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.2%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat)%20(1).pdf.
40. CCDCOE, "Cyber Threat Intelligence Course (October 2025)," accessed August 20, 2025, https://ccdcoe.org/training/cyber-threat-intelligence-course-october-2025/.
41. Jared Ettinger et al., *Cyber Intelligence Tradecraft Report: The State of Cyber Intelligence Practices in the United States (Study Report and Implementation Guides),* Software Engineering Institute, Carnegie Mellon University, May 21, 2019, https://insights.sei.cmu.edu/library/cyber-intelligence-tradecraft-report-the-state-of-cyber-intelligence-practices-in-the-united-states-study-report-and-implementation-guides/.
42. Jim Austin, "Open Source Intelligence: Introduction, Best Practice, and Legal Considerations," guest lecture at the TALTECH University, Master of Cyber Law, Tallinn, Estonia, December 12, 2024.
43. Fabio Biondi, Giuseppe Guonocore, and Richard Matthews, "Generative Adversarial Networks from a Cyber Intelligence Perspective," CCDCOE, 2021, https://ccdcoe.org/uploads/2021/08/Generative-Adversarial-Networks-from-a-Cyber-Intelligence-view.pdf.
44. Izzat Alsmadi, "Cyber Intelligence Analysis" in *The NICE Cyber Security Framework,* 2nd Ed. (Springer, 2023).
45. Thalia Ngan, Jocelyn Fenton and Celia Oakley, "Building a Cyber Intelligence Capability with the Future in Mind," *International Journal of Contemporary Intelligence Issues* 1, no. 2 (2024), https://search.informit.org/doi/10.3316/informit.T202403180000409014367973 2.
46. NATO, "S7-136 - NATO Systems Approach to Training," accessed January 3, 2025, https://www.natoschool.nato.int/Academics/ResidentCourses/Course-Catalogue/Course-description?ID=133.
47. Daniel Berchev and Milko Stefanov, "The Systems Approach To Training in the Military Educational System: Aggregation of Integration Processes," *Knowledge International Journal* 30, no. 6 (March 2019): 1457–62, https://www.academia.edu/43904942/The_Systems_Approach_to_Training_in_the_Military_Educational_System_aggregation_of_integration_processes.
48. "MCDC Overview," Multinational Capability Development Campaign, accessed January 3, 2025, https://cdissz.wp.mil.pl/u/MCDC_Overview.pdf.
49. Jim Austin, "NATO CCDCOE CyINT Course CCDIII Combined External Feedback."
50. Cybersecurity and Infrastructure Security Agency (CISA*), Cybersecurity Strategic Plan FY2024-2026,* August 2023, https://www.cisa.gov/sites/default/files/2025-01/FY2024-2026_Cybersecurity_Strategic_Plan508.pdf.

51. Department of Home Affairs, *2023-2030 Australian Cyber Security Strategy,* November 2023, https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy.
52. "UK, US, and Australia Cyber Strategies: A New Era of Collaborative Cyber Security," BAE Systems, May 14, 2024, https://www.baesystems.com/en-uk/story/uk-us-and-australia-national-cyber-strategies.
53. Ministry of Economic Affairs and Communications of Estonia, "Cybersecurity Strategy 2024–2030: Cyber-Conscious Estonia," DigWatch, February 2024, https://dig.watch/resource/cybersecurity-strategy-2024-2030-cyber-conscious-estonia.
54. CISA, "Certified Cyber Intelligence Professional (CCIP)," National Initiative for Cybersecurity Careers and Studies, September 19, 2024, https://niccs.cisa.gov/education-training/catalog/mcafee-institute/certified-cyber-intelligence-professional-ccip.

INTELLIGENCE STUDIES REDEFINED: Designing an Attractive, Structured, and Future-Ready Discipline in Service to the Nation

Anthony Ioannidis, Ph.D.
Anastasios-Nikolaos Kanellopoulos

INTRODUCTION

The discipline of intelligence studies must evolve to address the shifting dynamics of national security, private-sector collaboration, and global intelligence cooperation. This paper proposes redefining intelligence studies by transforming the National Intelligence University (NIU) into a mega-university**,** modeled after large-scale, technology-driven, globally networked educational institutions. In this vision, NIU would serve as the nucleus of a global intelligence studies ecosystem, integrating business administration, political science, international relations, security studies, and emerging technologies to create a comprehensive, interdisciplinary, and future-ready discipline.

Mega-universities utilize cutting-edge digital infrastructure, global partnerships, and interdisciplinary collaboration to deliver accessible, high-impact, and innovation-driven education. By adopting this model, NIU would transcend its traditional role, expanding intelligence education beyond physical and jurisdictional boundaries. Through hybrid and online learning, strategic partnerships with public and private institutions, and immersive, classified environments for hands-on intelligence training, this transformation would democratize access to high-level intelligence education, ensuring that intelligence professionals across the United States and allied nations can participate in a globally interconnected intelligence studies ecosystem.

At the core of this transformation, business administration would equip intelligence professionals with essential skills in strategic planning, organizational leadership, and financial management—facilitating their seamless transition into both public and private sector roles. Political science, international relations, and security studies provide expertise in geopolitical analysis, diplomacy, and security policy, ensuring

graduates possess the analytical acumen needed for intelligence operations. Coupled with advancements in artificial intelligence, big data analytics, and cybersecurity, this interdisciplinary approach strengthens intelligence studies as a rigorous, market-relevant, and innovation-driven field.

By expanding NIU into a mega-university, this model transforms intelligence education into a globally networked, interdisciplinary, and technology-enhanced ecosystem. Leveraging its classified learning environment and its unique position as the US Intelligence Community's university, NIU would become a hub for experiential learning, real-world problem-solving, and cross-sector collaboration. Through strategic partnerships with private enterprises, public institutions, and international allies, this new global intelligence studies ecosystem fosters a pipeline of highly skilled intelligence professionals prepared to address emerging security challenges. This transformation positions intelligence studies as a prestigious, structured, and future-ready discipline, essential for safeguarding national and global security in the 21st century.

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 effectively serve national security and the public good. Lack of industrial alignment, interdisciplinary integration, and standardization have long plagued intelligence education. Although other academic disciplines—such as data science, cybersecurity, and business administration—have developed to draw top talent and satisfy labor market demands, the field of intelligence studies is 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*—practical abilities such as cybersecurity, risk management, and analysis. However, intelligence programs frequently overlook these crucial elements, which keeps students from gaining a thorough, multidisciplinary grasp of their role in preserving national security.[2] This view is supported by other research that emphasizes the need for multidisciplinary learning, technology integration, and professional relationships[3] 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] In the absence of an organized and innovation-driven educational paradigm, 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.

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 in Bryan Penprase's and Noah Pickus's *The New Global Universities*.[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.

By implementing the mega-university model, intelligence education can transcend outdated paradigms and concentrate on experiential learning, multidisciplinary cooperation, and strategic business connections. This change would create highly qualified professionals dedicated to preserving democratic principles. They would be ethically sound and analytically strong, in addition to being technically proficient. This redefining of 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

Forming intelligence studies into 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 both the US and international higher education systems.[6] This structure is shaped by faculty research output, accreditation standards, and university rankings that 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] 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.

Academic and Professional Impact: High-impact research, notable publications, and active industry participation are necessary to establish intelligence studies as an elite field.[8] 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 depends primarily on hiring renowned academics and professionals.[9] 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. The mega-university idea, whereby professional intelligence groups and academia work together to create training and scholarship that is operationally relevant, is reflected in this transdisciplinary expertise.

Global Partnerships and Intelligence Networks: A globally connected intelligence education model must create strategic partnerships across multiple sectors to enhance institutional standing and ensure intelligence education remains aligned with industry trends.[10] 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 intelligence studies apart from more conventional academic fields is experiential and applied learning, which goes beyond encouraging collaboration and recruiting faculty.[11] In intelligence education, case-based learning, simulation-based training, and field experiences must be given priority over 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 critical components of contemporary intelligence education.

PILLAR 2: CREATING A SUSTAINABLE BUSINESS MODEL

Even when a start-up university 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.[12] 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.

Addressing the Financial Challenges of a New Intelligence Mega-University: A primary challenge that 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 adopt innovative financial strategies to ensure sustainability from inception.[13] To navigate this challenge, a mega-university

for intelligence studies must move 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 would be strengthened by government funding, which would be essential for supporting intelligence training programs, classified research, and national security projects. Diversifying financial sources is crucial because relying only on government support could result in regulatory restrictions.

The university's financial sustainability would 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 would, in turn, gain access to talent pipelines and intelligence-driven insights. These partnerships guarantee that the curriculum remains in line with industry needs. 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 make use of innovative educational models to create sustainable revenue streams while increasing its global reach.[14] Executive education and certification programs tailored to 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 would allow the university to scale its offerings beyond physical classrooms, increasing both financial sustainability and accessibility.

Significant financial support could 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: REBUILDING AND RELAUNCHING

Once the initial vision, prestige generation, and financial strategies are in place, the rebuild-and-relaunch 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.[15]

Incubation Phase To Refine 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.[16] 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.

Using a Codesign Process To Build 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.[17] This process fosters a student-centered learning environment, promoting innovation and adaptability in response to emerging trends in intelligence education and practice. However, a successful codesign requires a well-defined governance structure, ensuring that decisionmaking 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.[18]

A Phased Launch To Scale 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 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 giving priority to strategic planning, a methodical incubation process, and solid collaborations with the government and industry.

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.[19] At NIU, faculty members play a crucial role in shaping institutional culture, driving research excellence, and delivering high-quality education that meets the needs of both the US Intelligence Community and 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.[20]

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. 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. 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 an alignment between faculty expertise and NIU's interdisciplinary and applied intelligence focus.[21] 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 needed 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 give priority to 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 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 US IC'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. 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 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 crucial for attracting the best talent. Additionally, fostering an institutional culture that gives priority to 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 that are often constrained by historical precedents and rigid disciplinary structures, a reimagined National Intelligence University can adopt a forward-thinking approach that integrates intelligence studies with business, technology, and experiential learning. This opportunity allows 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.[22]

Building an Interdisciplinary Intelligence Curriculum: The core curriculum must give priority to 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 embrace 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, instead emphasizing a structured approach to intelligence as a strategic discipline that intersects with national security, international affairs, and business operations.

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 decisionmaking, and the application of AI to 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 government and private-sector intelligence roles.

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 decisionmaking 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. 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.

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. To overcome this obstacle, NIU must 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. 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.

Leveraging Accreditation To Enhance Institutional Prestige: Accreditation should not be viewed merely 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.

Balancing Innovation with Academic Credibility: The curriculum and accreditation strategy at NIU must strike a delicate balance between innovation and credibility. Although 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. The function of conventional brick-and-mortar campuses is being reexamined, however, as education becomes more digital. Some argue physical campuses are no longer required because online learning has proven so flexible and affordable. 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. To establish an ideal learning environment that strikes a balance between the advantages of both physical and virtual environments, NIU, as a forward-thinking university, must manage these conflicting viewpoints.

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 onsite 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 can 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 to preparing students for intelligence operations, where classified information and real-time decisionmaking are integral to their professional responsibilities.

Integrating Emerging Technologies in Intelligence Education: Institutions such as 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 analytic tools can offer real-time intelligence scenario modeling, and VR-based intelligence simulations can let students participate in immersive information-gathering activities. Additionally, by allowing students to collaborate on intelligence challenges with experts and peers worldwide in real time, 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 is likely to 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 to 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 decisionmaking 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 US higher education has long been both a source of strength and a challenge to innovation. Authority is typically distributed among faculty, administrators, and board members, with faculty often holding significant influence over curriculum and pedagogy. Although 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. 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 Decisionmaking: Managing the interaction between official decisionmaking processes and the unofficial institutional culture that develops over time is one of the main issues in shared governance. Universities frequently must balance the interests of private sector stakeholders looking for innovation and workforce preparedness, academics promoting academic traditions, and legislators focused on national security imperatives. 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 needs to form a hybrid strategy that permits strategic decisionmaking without undue bureaucracy.

Integrating Academic and Industry Collaboration: To address these governance issues, NIU must set in place a collaborative governance framework that unites stakeholders from government, business, and academia. 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. NIU must uphold a dual focus, however, 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. 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 among academia, government, and industry, guaranteeing open decisionmaking, 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 both national security and private-sector intelligence functions with unparalleled academic and professional rigor.

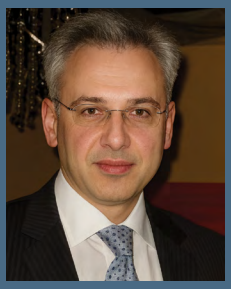
By expanding NIU into a mega-university, intelligence studies can adopt cutting-edge educational models, ensuring that students and faculty engage with real-world intelligence challenges through experiential learning, digital innovation, and global partnerships. The mega-university model facilitates 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 decisionmaking.

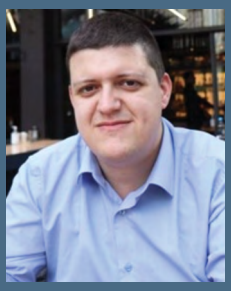
Eventually, intelligence education must evolve to embrace both traditional and open intelligence methodologies, ensuring accessibility while maintaining national security imperatives. A hybrid campus and digital learning model will enhance accessibility, security, and collaboration, ensuring that intelligence 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 not only elevate intelligence studies as a prestigious and indispensable field but also serve national security, public service, and global intelligence cooperation in an era of unprecedented challenges and opportunities.

This paper by Dr. Anthony Ioannidis and Anastasios-Nikolaos Kanellopoulos was published under the same title in *American Intelligence Journal* 42, no. 1 (Spring 2025), https://nmif.org.



Anthony Ioannidis, Ph.D., is an assistant professor of management at the Department of Business Administration, Athens University of Economics and Business, Greece. He also taught at the University of Patras, Greece; University of La Verne, California; and Baruch College, City University of New York. Dr. Ioannidis was a management consultant with leading consultancy firms, working in the telecommunications, media, and technology arenas in Greece and the United States. His research interests include intelligence education and practice, strategy formation, organizational design, public-private partnerships, and entrepreneurship. He holds a B.S. from the University of Athens, and an M.B.A., an M.Phil., and a Ph.D. from Baruch College.



Anastasios-Nikolaos Kanellopoulos is a Ph.D. candidate at the Athens University of Economics and Business in Greece and holds a master's degree in international relations, strategy and security from the University of Neapolis Pafos in Cyprus, a bachelor's degree in business administration from the Athens University of Economics and Business, and a bachelor's degree in public security from Hellenic Police Academy. He is a certified security risk analyst from Frontex and the Hellenic Ministry of Citizen Protection. His research interests include competitive intelligence and counterintelligence frameworks application in modern business environments.

ENDNOTES

1. Stephen Marrin, "Improving Intelligence Studies as an Academic Discipline," *Intelligence and National Security* 31, no. 2 (2014): 266–79, https://doi.org/10.1080/02684527.2014.952932.
2. Jules Gaspard and Giangiuseppi Pili, "Root Values and Root Skills: A New Model for Intelligence Education," *Intelligence and National Security* 39, no. 7 (2024): 1194–1212, https://doi.org/10.1080/02684527.2024.2390762.
3. Peter de Werd et al., "Special Forum on Intelligence and Theory," *Intelligence and National Security* 39, no. 7 (2024): 1230–53, https://www.tandfonline.com/doi/full/10.1080/02684527.2024.2324534.
4. Nicholas Eberstadt and Evan Abramsky, "America's Education Crisis Is a National Security Threat," *Foreign Affairs*, September 26, 2022, https://www.foreignaffairs.com/world/america-education-crisis-national-security-threat.
5. Bryan Penprase and Noah Pickus, *The New Global Universities* (Princeton University Press, 2024).
6. Corbin M. Campbell et al., "Prestige or Education: College Teaching and Rigor of Courses in Prestigious and Nonprestigious Institutions in the US," *Higher Education* 77, no. 4 (2019): 717–38, https://link.springer.com/article/10.1007/s10734-018-0297-3.
7. Orhan Dursun, and C. Altin Gumussoy, "The Effects of Quality of Services and Emotional Appeal on University Reputation: Stakeholders' View," *Quality Assurance in Education* 29, no. 2/3 (2021): 166–82, https://doi.org/10.1108/qae-08-2020-0104.
8. Carolin Nast et al., "Sourcing Insights Elsewhere: The Positive Influence of Academic Engagement on Scientific Impact," *Technovation* 139 (January 2024), https://doi.org/10.1016/j.technovation.2024.103112.
9. Adam Williams et al., "Scholars' Influence on Their Institutions: Reputation, Prestige, and Rankings," *Teaching Public Administration* 38, no. 3 (February 2020): 233–56. https://doi.org/10.1177/0144739420901741.
10. Stephan von Delft et al., "Leveraging Global Sources of Knowledge for Business Model Innovation," *Long Range Planning* 52, no. 5 (October 2019), https://www.sciencedirect.com/science/article/pii/S002463011730496X.
11. Stephen Marrin, "Understanding and Improving Intelligence Analysis by Learning from Other Disciplines," *Intelligence and National Security* 32, no.5 (2017): 539–47, https://doi.org/10.1080/02684527.2017.1310913.
12. Abdulrahman O. AI-Youbi et al., eds., *International Experience in Developing the Financial Resources of Universities* (Springer International Publishing, 2021).
13. Cameron Mirza, "Financial Models for Universities Must Go Beyond Student Numbers," *Higher Education Digest*, February 4, 2025, accessed June 3, 2025, https://www.highereducationdigest.com/financial-models-for-universities-must-go-beyond-student-numbers/.
14. 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, accessed June 3, 2025, https://medium.com/emerge-edtech-insights/how-to-build-a-unicorn-by-partnering-with-universities-to-diversify-their-revenue-streams-part-2-6b3215f26d55.
15. Maribel Guerrero and Marina Dabić, eds., *Re-Building University Capabilities: Public Policy and Managerial Implications to Innovation and Technology* (Springer International Publishing, 2023).

16. M. Tina Dacin et al., "Institutional Theory and Institutional Change: Introduction to the Special Research Forum," *The Academy of Management Journal* 45, no. 1 (February 2002): 45–56, https://www.jstor.org/stable/3069284.
17. Lawerence Susskind et al., "A Critical Assessment of Collaborative Adaptive Management in Practice," *Journal of Applied Ecology* 49, no. 1 (2011): 47–51, https://www.jstor.org/stable/41433323.
18. Byron Williams et al., *Adaptive Management: The U.S. Department of the Interior Technical Guide, MIT Science Impact Collaborative,* US Science and Decision Center, December 1, 2009, accessed June 3, 2025, https://scienceimpact.mit.edu/labs/adaptive-management-us-department-interior-technical-guide.
19. Liam Gearon, ed., *Education, Security, and Intelligence Studies* (Routledge, 2018).
20. William C. Spracher, "National Intelligence University: A Half Century Educating the Next Generation of U.S. Intelligence Community Leaders," *Intelligence and National Security* 32, no. 2 (2016): 231–43, https://www.tandfonline.com/doi/full/10.1080/02684527.2016.1248316.
21. Malin Henningsson and Lars Geschwind, "Recruitment of Academic Staff: An Institutional Logics Perspective," *Higher Education Quarterly* 76, no. 1 (2021): 48–62, https://doi.org/10.1111/hequ.12367.
22. Gearon ed., *Education, Security, and Intelligence Studies.*

A DEEPER SHADE OF RED

Robert Levine, Ph.D.

A common experience in the United States defense and intelligence world involves civilians or military officers play-acting the roles of foreign national leaders, making decisions in a crisis- or war-game with hardly anything distinguishing their actions as "foreign." Many of us have heard these officers explain their decisions simply and honestly as, "Well, that's what I would do if I were in that position." Similarly, it is hard to keep track of the number of papers drafted as fictional "For the Prime Minister's Eyes Only" or "Letters from an Afghanistan Cave" that barely reflect the culture, ideology, history, perceptions, or intentions of foreign actors. What distinguishes these flawed attempts at Red Teaming from others in which officers and analysts appear to have a real grasp of foreign thinking and decisionmaking? Just as importantly, how do we prepare officers and civilians to develop "a deeper shade of red?"

This paper explores a handful of key investments that contribute to the "dyeing" process. No magic bullet or short cut exists. Winston Churchill famously characterized the Soviet Union, in October 1939, as " … a riddle wrapped in a mystery inside an enigma." He went on to say, " … but perhaps there is a key. That key is Russian national interest." I am not going to gainsay Churchill, but it is fair to ask: How are we to predict Russian national interests? Moreover, even where national interests are transparent, do they map one-to-one with foreign initiatives or responses, with no contradictions, inconsistencies, or trade-offs? Hardly.

From my observations of intelligence analysts, almost all of whom fulfill the role of Red Teamers, four general realms of information define their success or lack of success. We can picture these as concentric rings. As we discuss these rings, two features will become apparent. The outer rings are broader and less bounded. As we look at the inner rings, the information is more narrowly defined and far more closely held.*

RED TEAM AS A SPECIFIC ACTOR

In this paper, the term Red Team is used to identify a **group assigned to play the role of a specific foreign entity**. The group's actions, such as in a crisis- or war-game, should reflect the best estimate of how

* Examples from the Cold War are used throughout this paper because essential elements and specific experiences have been declassified and can be cited. The concepts illustrated by the examples apply widely today. Red Teams from the Intelligence Community regularly participate in wargames and military exercises playing the roles of different, specific adversaries.

the foreign actor would perceive a situation, weigh options, and make choices. Its considerations are thus a combination of perceptions, intentions, and assessed capabilities. An excellent example of this kind of Red Team was the early incarnation of PROJECT CHECKMATE, a group that was formed within United States Air Force planning in the 1970s to study in detail Soviet air operations and develop effective counteractions. That small, professional cell had access to detailed, classified information about Soviet equipment, organization, doctrine, training, operations, logistics, and all the other major components that went into shaping how the Soviets and their allies might have operated in a war.

Other forms of Red Teaming have had significant successes in challenging military plans and approaches. A number of these exploit Blue vulnerabilities and operate as adversaries in ways that could prove highly effective. Their actions, however, are not consistent with the way specific foreign powers appear to behave. For example, years ago several RAND analysts created a scenario for a secret, no-warning Warsaw Pact attack in Central Europe. Clever as it was, it violated virtually everything we knew about how the Pact organized, planned for, prepared for, and was likely to fight a campaign.

Red Teaming as described in this paper is not intended to pose the greatest possible threat or worst case. The Red Team might, in fact, reveal its own vulnerabilities that Blue planners might choose to exploit in real world planning.

THE FOURTH (OUTERMOST) RING: CULTURE, IDEOLOGY, HISTORY, AND THE CONTOURS OF SOCIETY

New intelligence analysts, like all Red Teamers, face the daunting task of getting to know the general subject of their work. Individuals raised in any country acquire a vast array of explicit as well as tacit knowledge that provides the essential backdrop to understanding situations, events, and trends. (Those of us with immigrant parents or spouses can recount any number of stories that demonstrate this fact by its absence.) The value placed on foreign regional expertise and language skills in the Intelligence Community hiring process is a recognition of the necessary and substantial investment in time and effort to acquire such knowledge—and the difficulty of doing so after an analyst is assigned an account. Short survey courses ("Middle East Realities" is one of a series that has been offered for decades at the CIA) and orientation visits have their place, but no one thinks they are paths to profound understanding. (See Annex, "Exploring Cultures.")

Red Teamers should be encouraged to view any assignment as a long-term commitment that requires their continuous personal investment to develop a feel for the foreign entity. The process and gains from learning in breadth and depth about the country or society will seldom, if ever, result in an immediate payoff. Rather, just as studying art history, painting techniques, and the influence of one artist on another allows one to look at a single painting and extract more from it, regional knowledge leads to analytic insights about particular activities. It helps us gain and offer perspective—the single most important contribution that any analyst can provide to senior policymakers.[1]

The negative side to this issue is equally important. Analysts working on South Asia, for example, who had but a sketchy sense of the history of the region, the roles and policies of colonial powers, and the area's geographical and ethnic diversity (among other dimensions) could hardly be in a position to interpret the motivations and durability of local insurgencies. Even the most recent follower of Middle Eastern affairs knows, for example, that they must study and understand the background and nature of the Sunni-Shia divide. A quick Google search and Wikipedia helps, but is no substitute for sustained study.

I saw a telling instance of the importance of a general sense of how a country works in the months following the collapse of the Soviet Union. As nations such as Ukraine, Lithuania, Latvia, and Estonia asserted their independence and resolve to distance themselves from Moscow, some pundits (and analysts in the Intelligence Community) postulated that whole chunks of Russia—such as Siberia and the Far East—would spin off centrifugally. One of my colleagues who had spent years in the USSR, spoke Russian fluently, and was immersed in its political culture summed up the pundits' claims pithily: "Understanding that some areas like the Baltics will leave shows a grasp of the basics. Thinking this means Siberia is lost shows a failure to understand the core features of the country."

As important as it is to develop a broad perspective about a foreign entity, Red Teamers run the risk of viewing foreign actors as stereotypes or caricatures. All of us have bristled at some point or another when a foreign commentator refers, for example, to "the typical American trait of impatience." We might hope that American analysts will not repeat the insulting and misleading characterizations of the Japanese before 1941 that influenced our inadequate pre-war military preparations. As the Joint Intelligence Center, Pacific Ocean Areas (JICPOA) explained in February 1943: "[W]ith more than a year of war behind us and with experience gained in fighting ... we can begin to see how much we have misunderstood the [Japanese]."[2] My observations of, and experiences in, the Intelligence Community suggest the distance from such prejudices to more recent times may not be as great as we would like.

This first, outer ring is hard to pin down because its foci are so diverse, unbounded, and multidisciplinary in nature. One final point, however, deserves a quick stopover. The British historian, Christopher Andrew, has spoken and written frequently about what he refers to as "Historical Attention Span Deficit Disorder."[3] Andrew argues convincingly that historical awareness is often lacking in Western analysis. Conversely, when analysts or Red Teamers provide historical perspective, it establishes credibility and lays a foundation for explaining an ongoing situation and suggesting where things might lead. Several years ago when I presented analysis on potential tensions between China and India, for example, it seemed that none of the policymakers briefed had a good sense of their 1962 conflict, if they even knew it had occurred. By displaying the course and scale of the conflict, and each country's post-conflict reactions, more recent flare-ups and activities could be discussed in context, not ahistorically. †

† Parallels can be striking, and legacies long lasting. As William Faulkner put it, "The past is never dead. It's not even past."

THE THIRD RING: THE ETHOS OF THE DISCIPLINE

Specialization occurs as we move from the fourth to the third ring. Whereas the fourth ring is multidisciplinary and open-ended, in the third ring Red Teamers develop an understanding of a **particular culture within a discipline**, such as a foreign entity's politics, society, economics, science and technology, or military. We will take the last as our example.

Anyone aspiring to act as a military representative in a Red Team needs to be comfortable seeing situations and events as would a foreign officer who has been molded by the military culture of the country. Of course, there are shared perspectives held by all pilots or tank commanders, no matter their background and uniform. But an immersion into a foreign military's history, geography, past behavior, composition, and place in society—just to mention a few facets—yields insights that go much further.‡

The importance of this third ring should be easily grasped. Consider the differences, for example, between the general sense that American military officers have of geography, distance, and time from many (perhaps all) of our allies or potential opponents. Americans are used to projecting force thousands of miles, and as General Pagonis titled his book about logistics in the Gulf War, moving mountains to support them. Our home front traditionally has been largely free of direct threat.§ Our preference traditionally has been to respond to threats after they have asserted themselves on the battlefield, coming to the aid of allies who bear the initial blow.

Other countries face military threats only minutes of flying time and hours of driving time from their borders, their primary bases, their leaders, and their families. It is inconceivable that such countries would share with us identical views of readiness, mobilization, or a willingness to forego preemptive military actions.

Though bounded, this third realm of knowledge is large and rich, and for the most part relatively accessible. Countries do not try to hide the basic facts of their military geography, history, and structure. One of the arguments made in the past was that open-source publications (including histories) published in closed societies were intended primarily to deceive Western audiences. Our experiences with Soviet and Warsaw

‡ Former US military officers who became intelligence analysts often had a difficult time accepting what they judged to be inefficient, even ineffective, foreign military approaches. Economists, scientists, and others sometimes fell into this same difficulty. A number of us who worked on foreign Weapons of Mass Destruction programs used a phrase to capture (some of) the tension between technical and regional experts. Science is science, but engineering has a lot of wiggle room. For example, a nuclear weapon requires a critical mass of fissionable material. You can't cheat Mother Nature. But its manufacture presents many options in terms of speed, cost, safety, willingness to violate international agreements, desirability of testing to establish confidence, etc.

§ The advent of Soviet nuclear-armed bombers and nuclear-tipped missiles changed all that, of course, for a certain class of conflict. Nevertheless, the United States fought wars in Korea, Vietnam, the Balkans, and the Persian Gulf (not to mention smaller conflicts) with no real threat to the homeland. The emergence of cyberweapons almost certainly will change US concerns.

Pact publications suggest that fear was largely unwarranted. We found classified descriptions that tracked closely with articles that appeared in the Moscow-published *Military History Journal* (*Voyenno-Istoricheskiy Zhurnal*) and other unclassified and widely disseminated Soviet periodicals. As any serving officer will tell you, the cost of sowing confusion in one's own forces—as the "it's all deception" argument implies—would overwhelm any possible gain.

One of the first places to turn is the military history of the country as written by their historians, and contrast that with the history as written by opponents and outsiders. Wars and campaigns described by natives of a country capture not only the events, but the **stories and myths** that help shape a country's military culture. Reading into a country's military history can yield the terms, analogies, and reference points that that country's officers are likely to apply to future situations. For a senior Russian officer, the implications of June 22, 1941[¶] are as readily available (or even more salient) as the implications of December 7, 1941 for an American. It is hard to imagine a senior Israeli officer who does not have a visceral reaction to the "conceptziya" (concept) that influenced Israel Defense Force planning before October 1973, leading to shocking early setbacks in that war.

While unclassified and easily accessible sources can enrich one's understanding of a foreign military culture, there is an additional resource that frequently requires security clearances to access. **Emigres and defectors** who have served in a foreign country's armed forces can reveal, through interviews, ground truth about an organization's workings. As an intelligence officer, few of my professional investments of time and effort paid off as handsomely as multiple debriefings I conducted of Soviet and Warsaw Pact intelligence and military officers who had emigrated or were secreted out of their countries. Reading classified minutes of Pact intelligence officers or collection tasking was enlightening. But sitting down with former opponents over tea, coffee, or a beer and hearing firsthand about procedures, personnel, incentives, and disincentives, etc. made the documents come alive.

Defectors and emigres who have been thoroughly debriefed may not be able to offer additional intelligence information with immediate impact. In the context we are discussing, their knowledge and experiences have a much longer half-life—one measured in years. Organizational cultures are slow to form and equally slow to change. For that reason, CIA quietly arranged for former Pact military officers to address US commands and engage with them.

THE SECOND RING: THE NUTS AND BOLTS OF HOW THEY OPERATE

Shortly after I joined the CIA in 1985 my immediate branch chief brought me into his office and asked me to close the door. He told me that we possessed a body of material that was especially sensitive because

¶ Many of us read A. M. Nekrich's book alongside German accounts and later British and American histories to learn the Soviet perspective and compare it to others.

it was acquired through the human espionage of a number of agents operating in the Soviet Union and Warsaw Pact countries over a span of years. Protecting the sources meant protecting the lives of courageous people who had agreed to work with us. We walked over to a small, nondescript room with its own cipher lock (this room was inside a vault in which we worked—the equivalent of a safe inside a safe, inside one of the most secure buildings in the country). This room, perhaps twelve by ten feet, was chockfull of locked file cabinets and safes. Inside these were tens of thousands of pages of documents that had borne our opponent's classifications of SECRET and TOP SECRET, and now had our highly restrictive classifications.**

The documents laid out, in detail, how the Warsaw Pact was organized and how it functioned. We could read the minutes of many of the most sensitive negotiations and agreements, and look at weapons purchases, command relationships, and information exchanges.†† Most remarkably, we could read notes, manuals, and other materials from the Soviet's Voroshilov General Staff Academy—the seniormost educational component of the Soviet and Warsaw Pact militaries.[4] It was a treasure trove, paid for at incredible risk and, indeed, in lives. I spent months in that little room, reading and taking notes that themselves became part of the repository.

Acquiring such a repository is an expensive, risky, long-term collective work. Using it well demands that a Red Teamer accept the need for an entire re-education. Mining such treasures requires new vocabularies and new understandings. The time and effort spent on this can change how one reads unclassified works and interprets activities detected by other means. This can be illustrated with a declassified example.

For decades NATO was confronted by forces it assessed, rightly, as substantially greater in number than its own. At the same time, NATO funding for ammunition and the resulting stockpile was deemed inadequate. In the depths of the Cold War, it could be assumed that a conflict could lead to nuclear escalation because our forces and their inadequate sustainability would crack under the weight of a Pact attack.

The highly classified documents we possessed allowed us to track an evolution in Pact perceptions. As NATO forces increased in size and quality in the 1980s, an attack from the east no longer looked (from the Soviet perspective) like a quick breakthrough and rapid pursuit, but rather a grinding, highly destructive assault that might well fail to break NATO defenses. Anticipated higher attrition rates called for larger Pact assault forces. Those forces would take time to mobilize and deploy in a crisis and would demand substantial increases in sustainment (ammunition, fuel, maintenance capability, etc.).[5] From the Pact perspective, what had been a

** Dozens if not hundreds of these documents can now be accessed through the CIA Freedom of Information Act (FOIA) website: https://www.cia.gov/readingroom/.

†† There is a wealth of information, for example, on the negotiations concerning the "Wartime Statute of the Combined Armed Forces," a highly contentious agreement about how the Soviets would control their Pact allies in a war. The Polish pushback is detailed in a lengthy Polish General Staff Memorandum, which was originally classified by the Poles as SECRET OF SPECIAL IMPORTANCE. (*Source:* "Wartime Statute of the Combined Armed Forces*," Intelligence Information Special Report,* November 28, 1979, https://www.cia.gov/readingroom/docs/1979-11-28.pdf.)

decisive advantage in sustainment slipped to a serious vulnerability. NATO would have more time to mobilize as greater Pact forces mobilized, exacerbating the very problem that handed NATO more time.‡‡

If someone looked at Pact activities from the outside, its increases in forces and its preparations for a more intense conflict might look like increased hostile intentions and greater confidence. Our access into Pact perceptions, plans, and calculations told a story almost diametrically opposite. Their confidence had faded, and they saw no viable path to restoring their conventional military dominance in a potential war in Central and Western Europe. Whether the CIA saw the coming collapse of the Soviet Union, we wrote and briefed about a growing Soviet pessimism for years before the December 1991 disappearance of our military and ideological rival.[6]

THE FIRST (INNERMOST) RING: STUDYING OURSELVES TO STUDY OTHERS

Quite a number of years ago I was asked to drive over to the Pentagon to brief a senior Defense Department official on Soviet perceptions of the military balance. My work at the Central Intelligence Agency had focused on Soviet and Warsaw Pact military perceptions, as discussed above. A small group of us were developing what we felt was a nuanced sense for how Soviet and Pact planners viewed the challenges they faced in peacetime and would face in a crisis and war.

The briefing went wonderfully for some time. Because of the official's high security clearance, I could cite specific examples and describe the nature of our sources and how confident we were in our judgments. As I warmed to my subject, the topic turned to potential weaknesses the Soviets appeared to have in a sensitive area, as demonstrated by specific, highly classified materials we had acquired. I described Soviet concerns and how those concerns led to preparations and investments. At one point—after outlining what I considered a particularly fretful Soviet apprehension—I said something like, "Frankly, as much as I hate to use the word, it is difficult to view Soviet fears about potential, specific American actions against this target set as anything short of paranoid."

The senior DOD official, who had been very engaged and forthcoming up to this point, more-or-less froze, staring at me without saying a word. I looked at him and the proverbial lightbulb went off. I said, "My God. It's real. That's what we are planning."

I do not really remember how the rest of the briefing went. What I had seen was something that would reoccur, somewhat disturbingly, throughout my career. The Soviets, or some other foreign actor, would have a better idea of what the United States was up to than did my colleagues and I in the US Intelligence Community.

---

‡‡ Moreover, the emerging Pact vulnerability suggested NATO targeting options that would compound Pact problems in a war.

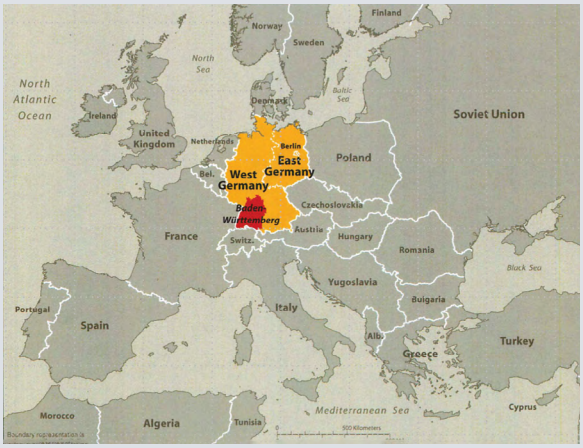
Feeding Soviet Concerns about German Revanchism

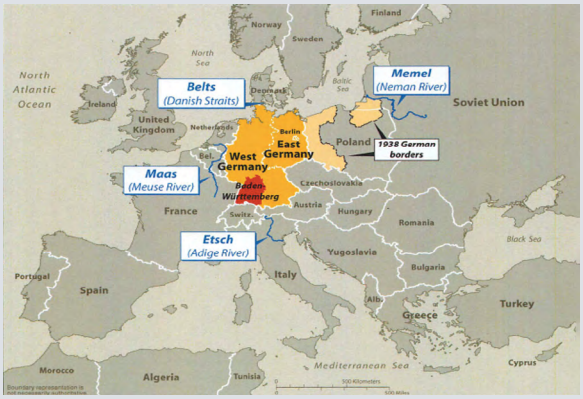
Soviet writings portrayed West Germany as a potential threat in part because of its unsettled borders. Western analysts largely discounted Soviet fears and were not attuned to how they might be fueled. Germany may have inadvertently fed such fears.

"Deutschland uber Alles?"

West Germany substituted the third verse as the official words of the national anthem in 1952. In the late 1980s, however, the first verse was being taught in schools in Baden-Wurttember:

Germany, Germany above all,
Above all in the world,
When, for protection and defense,
It always stands brotherly together.
From the **Meuse** to the **Memel**,
From the **Adige** to the **Belt**,
Germany, Germany above all,
Above all in the world!





The German anthem appeared to claim territory in more than half-a-dozen countries, including the USSR.

Moreover, all German official documents were required to display the 1938 German borders. Imagine how Soviet officials might view clandestinely acquired, classified German documents that appeared to lay claim to extensive territories in Poland and in the USSR.

The original version of this material appeared in CIA Directorate of Intelligence Research Paper, *The Nature of Soviet Military Doctrine*, SOV 89-10037CX, April 1989, declassified and released in 2000, https://www.cia.gov/readingroom/docs/DOC_0000499601.pdf.

LOOKING ON BOTH SIDES OF THE HILL

The Duke of Wellington famously stated, "The whole art of war consists of guessing at what is on the other side of the hill." There is an assumption built into that claim that my experience suggests is not justified. It assumes that we know what is happening on **our side of the hill**. Moreover, it slights the critical interaction of commanders' (on both sides) perceptions of what is going on. My rather clumsy Pentagon interaction was all too convincing.

The innermost ring focuses on the need to dig even deeper into foreign perceptions than initial gleanings may suggest. Those highly classified Pact documents described above hinted what we needed to do, but there was a second step.

Our potential military opponents had conducted detailed studies of the United States' and NATO's strengths and weaknesses. They were not just glancing "on the other side of the hill" (that is, our side of the hill). They were staring at us and examining us with a professionalism that I could not help but admire. We learned over time how they acquired detailed information—through vast signals intelligence interception operations, overhead imagery collection, and a network of agents that included people who compromised our most sensitive capabilities and plans.[§§] In brief, it was obvious that the Soviets had their own little rooms filled with purloined NATO materials.

The first-order exploitation of this material was a matter of piecing together Pact perceptions about issues critical to deterrence and war planning. My first foray[¶¶] was a study that has not been declassified, but whose title has been: *Warsaw Pact Military Perceptions of NATO Nuclear Escalation*. Soviet and Pact documents revealed that they were convinced that a war could escalate to nuclear use because NATO would feel compelled to initiate nuclear use in a conflict. The Pact's conventional military superiority (before it started to fade, as described above) would allow them to take the offensive (even if they believed a war might start with a NATO attack) and threaten NATO's cohesion and existence in Western Europe. The NATO alliance's official declaratory position—reinforced by our preparations and capabilities—was that we reserved the right to respond to Pact aggression with nuclear weapons. The Pact leadership needed to consider how, when, where, and why (in what circumstances) NATO might initiate nuclear use and escalate beyond that first use. Our understanding of their perceptions could bolster deterrence in a crisis or war, and potentially prevent the unintended escalation that could result from unintended and false signaling of imminent nuclear use.

When I briefed my paper to a four-star general at Supreme Headquarters Allied Powers Europe (SHAPE) in Mons, Belgium, the general asked a simple question: "You tell me they see these things in our exercises and plans. I believe you. Are they right?" That opened the door to a yearlong study of **exactly what messages we were sending—intentionally or not, knowingly or not**—to listening Pact ears about our capabilities and intentions.

---

§§ Years later I came across a case that shocked me, after I thought I was thoroughly jaded. An East German agent, Rainer Rupp, codenamed Topaz, had handed over virtually every sensitive document from NATO headquarters. When I found gaps earlier in SHAPE's archive, l had proposed in jest that perhaps we could ask the Soviets for their copies of missing documents. It turns out the Soviets really did have copies.

¶¶ I was not by any means the first to see the analytic opportunities in exploiting Pact perceptions. See, for example, a contemporaneous document: CIA, "Soviet Perceptions of US Naval Strategy," Research Paper SOV 86-1009D, July 1986, https://www.cia.gov/readingroom/docs/DOC_0000500708.pdf. Most analyses, however, included Pact perceptions as an explanation for their programs and policies. Almost no analyses compared Soviet or Pact perceptions to the reality of our capabilities or activities.

Again, the paper and results remain classified. Suffice it to say that our seniormost NATO officers had no idea what basic messages we had been sending for over 20 years. Soviet perceptions that had made no sense in the past suddenly revealed their origins.

It was becoming apparent that a key to understanding our opponents' actions was to enter the **analytic wilderness of mirrors**—to study what we (the United States and NATO) did, how the Pact and Soviets perceived our activities, and what their reactions were. Looking at the problem strictly from what we knew that they knew was simply not enough—it would always leave us with a terribly incomplete picture.***

One critical piece of my two studies has been almost entirely declassified,[7] and it could not be a clearer example of the need to study both sides of the hill. Starting in the early 1980s the Soviet Union initiated an intelligence collection and analysis surge—the largest since the Cuban Missile crisis—that has come to be known as the War Scare. Soviet authorities came to believe, for a number of reasons, that the United States was contemplating a sudden nuclear attack. Soviet fears were fueled by a combination of such activities as confrontational, even aggressive presidential rhetoric (for example, President Reagan's "ash heap of history" speech, accusations over the shootdown of the Korean airliner in 1983); a large budgetary increase and subsequent nuclear and conventional military buildup; the Strategic Defense Initiative; fielding of nuclear-tipped Pershing II missiles in Europe with short flight times to Moscow; and aggressive air and sea exercises.

There are two critical points about the War Scare for our purposes:

1. We were largely blind to it for the first several years. A Special National Intelligence Estimate (SNIE) on the issue published in May 1984—three years after the War Scare started—essentially dismissed the notion that the Soviets were scared.[8, †††] The first major (classified) published acknowledgment of the War Scare occurred in May 1986.

2. No one was charged with connecting our activities to opponents' perceptions. Moreover, no allowance was made to "read people into" the most sensitive activities of the United States Government so they could look for connections.‡‡‡

*** I wrestled with describing this simply at the time and never reached a satisfactory solution. At one time I displayed an iceberg and said the visible part above the waterline represents what we know they know about our activities. Underneath, that unseen mass represents all the things they know that we do not know they know. If we wait to collect what they know, we will always lag in the action-perception-reaction cycle. A recent history of World War II provides another analogy. Our collection of opponents' perceptions and reactions is like a peephole in a shut door to a large room. Most of what happens in that room is at the wrong angle to spot through the peephole. (*Source:* Gershom Gorenberg, *War of Shadows* (Public Affairs, 2021), 287).

††† One aspect of the SNIE is especially ironic. It is one of the few papers that discussed Soviet perceptions in light of real-world US and NATO activities. The SNIE, however, omitted several of the most critical occurrences of the time, including the Strategic Defense Initiative, the Korean Airliner downing, and the provocative rhetoric of President Reagan.

‡‡‡ The United States and its allies have a mixed history in this field. In the Second World War, deception operations

Former Director of Central Intelligence Robert Gates used to say that the only country that CIA analysts do not understand is their own country. It is worse. We frequently do not understand our country or know its actions,[§§§] and do not recognize (much less study) their impact.[¶¶¶] Red Teamers cannot afford to fall into that trap.

AN EDUCATION PROGRAM FOR RED TEAMERS

Readers might look over the four rings or realms of knowledge sketched out in this paper and shake their heads in disbelief: how can that much be asked of Red Teamers? Even if the general direction makes sense, how can such an ambitious agenda be tackled? The answer is, through a combination of individual, group, and bureaucratic efforts.

Individuals charged with becoming Red Teamers need to develop "professional empathy" for the foreign entity. They do not need to be fond of, or endorse, that entity's politics, economics, societal norms, etc. (the derogatory term used to describe that crossing over is "going native"). Their long-term investments will lead to intuitive or instinctive awareness of how a situation looks from the other side of the hill.

Scattershot reading can be terribly inefficient, but there is no reason to follow the principle of "ready, fire, aim." Rather, from their first days Red Teamers should reach out to the wide variety of experts in academia, think tanks, NGOs, and all parts of the government to help guide their education. Most experts are willing and enthusiastic promoters of awareness of their region of study. Red Teamers should not hesitate to ask experts for their recommendations for the best materials, but should also probe to find

---

such as those preceding the Normandy invasion examined what the Allies were doing and how our activities would be perceived. We took carefully crafted actions to plant misleading information to influence German force dispositions and reactions and monitored the effect of the misinformation.

§§§ There is also a risk in defining "our country's actions" too narrowly, for example, by looking only at Executive Branch activities. After the Indian and Pakistani nuclear tests in 1998, creative South Asian lobbying in Congress (involving a threat to forego purchases of American wheat) changed the course of US diplomacy. (*Source:* Robert M. Hathaway, "Confrontation and Retreat: The US Congress and the South Asian Nuclear Tests," *Arms Control Today* 30, no. 1 (January/February 2000): 7–14) And it is not only parts of the US Government that deserve our attention. KGB instructions sent to its Residents in NATO countries suggested that church leaders and senior bank authorities might have been brought into the process of preparing for a NATO nuclear strike on the USSR. We are dealing with perceptions here, not necessarily reality. (*Source:* Christopher Andrew and Oleg Gordievsky, *Comrade Kryuchkov's Instructions: Top Secret Files on KGB Foreign Operations, 1975-1985* (Stanford University Press, 1993), 73.) Finally, does anyone doubt that a Florida pastor's burning of Korans in 2012 had an impact among jihadists? Recall how the 2005 publication in a Danish newspaper of editorial cartoons depicting Muhammed led to violent demonstrations and protests in some Muslim countries.

¶¶¶ Several years later I discovered that a remarkably close-hold US covert action probably triggered a Soviet reaction that was frightening in its potential consequences. No one had been in a position to connect the actions and reactions.

contentious issues and different schools of thought. They need to find and pursue not just the points of consensus, but the fissures.

At the group or team level we can find several opportunities for greater efficiencies. Ideally an organization should create Red Teams, not just Red Teamers. Leaders need to provide time, access, resources (including funding), and encouragement for a critical mass of Red Teamers. When team members can build on each other's knowledge, and gain from specialization while sharing common findings, the results conform to the tried (and tired) saying that the whole is more than the sum of the parts. A number of us working on the Soviet military, taking different facets—Soviet perceptions and capabilities tied to ground and air readiness, ammunition sustainability, breakthrough and pursuit operations, air operations, and force requirements—found connections and a bigger picture that none of us saw, or likely would have seen, individually.

Teams could also be encouraged to learn principles of understanding foreign military cultures by exploring cases together. A structured study of how a particular foreign power operated in the past can yield fruitful analogies. A number of readily available, well-crafted books can be used for such an effort (see the Annex).

Bureaucratic clout and sustained efforts are required as well. Gaining knowledge in the second ring means fighting for access to highly classified materials and developing handling and storage procedures that are anything but easy. Nevertheless, those demands are more easily met than the ones linked to the innermost first ring. Senior military officers, for example, often are not inclined to share the closely guarded details of their activities and capabilities (or to approve using the limited billets required for access). Senior intelligence officers in the past have looked askance at officers trying to match up Blue actions and Red perceptions and reactions. (One senior intelligence manager said, "You want to spy on the United States! That's not our job!") It will take a coordinated, persistent effort to crack this challenge. Without it, we will always be lagging real-world developments.

LIMITATIONS

We have already mentioned a potential limitation in the event Red Teamers believe they have a firmer grasp of the target culture than they actually have. This can lead to missing or misinterpreting likely foreign perceptions, and suggesting foreign actions that are based on an overly selective, skewed body of evidence. At worst, this kind of behavior may appear as stereotypes or caricatures. Professionals committed to learning foreign cultures and history are unlikely to fall into this trap. The other limitations, however, are more serious.

A Red Teamer with a well-developed understanding of a target country and organization will face situations in which she is asked to **project potential foreign perceptions and reactions beyond anything that has happened in the past**. When anyone extrapolates beyond the bounds of experience the odds of picking an

"incorrect" perception or response increases. Thus, someone steeped in the culture, history, organization, and operations of a foreign entity that suddenly is presented with a capability unlike any that entity had in the past may have little to build upon. The proliferation of offensive cyber capabilities is likely to present hundreds of sovereign foreign entities with just such a new capability—perhaps with little notion of how to absorb and use it.

Depending on the structure of the foreign entity being red-teamed, the importance of multiple sources of foreign perception and complex decisionmaking increases. **Outcomes result from a complex mixture of individual choices, bureaucratic bargaining that generates a decision, and standard operating procedures that channel implementation**. It is hard to prepare Red Teamers to develop an understanding of a particular subculture in a foreign entity as well as an all-encompassing grasp of the processes that go into producing and executing a foreign initiative or response. Even then, in our own country we have seen initiatives and responses that little resemble the individual inputs or intentions from a number of diverse actors.

The final limitation harks back to one of the most important and prominent cognitive biases—the **fundamental attribution error**. In brief, people overemphasize the importance of other actors' personalities or dispositions, relegating those actors' circumstances or situation to secondary status. That is, people ascribe foreign actions to "who those foreign actors are" rather than the positions in which the foreign actors find themselves. The irony of the fundamental attribution error is that people do the exact opposite when considering their own actions—ceding primacy to the situation rather than their own dispositions. Red Teamers and the whole red team approach may be particularly vulnerable to this error.

None of these limitations invalidate the usefulness of red teaming, and especially the value of an investment in learning a foreign entity's culture, history, geography, organizational culture, etc. They do suggest where those using red teams must beware and remain cautious.

ANNEX: EXPLORING CULTURES

There is a tendency for some Red Teamers, like some military analysts, to focus on the concrete and measurable dimensions of foreign military capabilities: weapon characteristics, numbers, and order of battle. This needs to be balanced by a **long-term, persistent exploration of the cultures**[****] that strongly influence all the preparations and conduct of war—strategies, operations, tactics, organizations,

**** Anthropologists, and in particular ethnographers, have played an increasingly important role in US military operations, as well as in US corporations. "Ethnography is the branch of anthropology that involves trying to understand how people live their lives. … Ethnography has proved so valuable at Intel that the company now employs two dozen anthropologists and other trained ethnographers, probably the biggest such corporate staff in the world." (*Source:* Ken Anderson, "Ethnographic Research: A Key to Strategy," *Harvard Business Review* 87, no. 3 (March 2009): 24, https://hbr.org/2009/03/ethnographic-research-a-key-to-strategy).

doctrines, personnel policies, training, etc. As two authorities on the subject put it, "Everything that military organizations must perform in the pursuit of national security objectives ultimately rests on their cultural foundations."[9]

There are many definitions of culture. We can combine them to offer the following:

> A **culture** is the collection of beliefs, values, ideas, attitudes, assumptions, norms, and learned behavior of a group of people—expressed or reflected in symbols, rituals, myths, and practices—that shape how that group functions and adapts to external stimuli. Culture gives sense and meaning to members of a group.[10]

In studying any foreign entity—for example, the ground forces of a country—we must recognize and understand a **cascade of cultures**: the general societal culture, the strategic culture,†††† the military organizational culture, and the subcultures (not only the services, but specialties within the services, such as armored or airborne forces within the army). At all levels, cultures share a number of critical characteristics:

1. They change slowly.
2. They are hard to change.
3. They can have both positive and negative consequences (e.g., on military effectiveness).
4. They are generally hidden beneath more obvious symbols, structures, and official doctrine.
5. They create identities through specific attributes.
6. They influence how members will behave, and are expected to behave.
7. They influence how organizations function.

No one should assume that developing an understanding of a foreign military culture will be a quick or easy matter. For example, many of the overt, observable facets of a culture (its artifacts)—such as its weaponry and command relationships—may reflect aspects of its true nature, but, "An organization's culture … is reflected more in what leaders demonstrate through their behavior than what is written down or inferred from visible structures, systems, rituals, stories, or published doctrine."[11]

---

†††† Enduring geographic, economic, social, and demographic circumstances along with its historical experiences shape a **nation's strategic culture**. That strategic culture defines how the nation perceives and uses all of the elements of national power—including how it defines war and uses force.

The Red Teamer who hopes to think red has to understand an organization's beliefs and values (the features that provide guidance and reveal motivations and rationale), and its basic assumptions (the unseen and unconscious beliefs that guide actions and perceptions).

There is no cookbook approach to attack this challenging task. Two techniques have proven useful and are recommended:

1. **Study the well-documented military culture of a country from the past**. Look at how the Germans, French, or British created their military cultures in the 19th and first half of the 20th centuries, and how those cultures manifested themselves in the preparation and conduct of war at the tactical, operational, and strategic levels.[12]

2. **Study one of the subcultures of our own military**. This is not to encourage mirror-imaging, but rather to learn the skills of teasing out embedded beliefs, values, etc. and to see how they affect behaviors and decisions. An excellent case study of the US Army's way of war is explained in Brian McAllister Linn, *The Echo of Battle: The Army's Way of War* (Harvard University Press, 2007).‡‡‡‡

Robert Levine, Ph.D., is a lecturer at Johns Hopkins University. After a 33-year career, Dr. Levine retired from the Central Intelligence Agency (CIA), where he served as a senior military analyst and ran the internal analytic quality evaluation program for the Directorate of Analysis. He taught intelligence and national security policy at the National War College, CIA, within the Intelligence Community, and at Mercyhurst College. Dr. Levine has published in *Studies in Intelligence* and *Intelligence and National Security* and co-edited *The CIA Intelligence Analyst: Views from the Inside* (Georgetown University Press, 2024). He holds a Ph.D. from the RAND Graduate Institute.

‡‡‡‡ Linn argues in his book, " … the [US] army's way of war has been shaped as much or more by its peacetime intellectual debate as by its wartime service." During peacetime military intellectuals can reference their own and other countries' histories to draw lessons, and can consider new weapon systems, tactics, operations, strategies, organizations, structures, opponents, and locations—all components of a service's or nation's way of war. Linn's identification of three distinct US Army schools of thought and their evolution, arguments, and influences provides a rich example of military culture at work. Future Red Teamers could profitably compare Linn's findings with Carl H. Builder, *The Masks of War: American Military Styles in Strategy and Analysis* (Johns Hopkins University Press, 1989), as well as chapters on the US armed services in Mansoor and Murray.

ENDNOTES

1. Walter Russell Mead, *Special Providence: American Foreign Policy and How It Changed the World* (Routledge, 2002). Mead discusses four distinct historical patterns in US foreign policy and shows how each has asserted its influence on foreign policy. For a quick look at the power of broad schemes to provide perspective, see also the book review by H. W. Brands, "The Four Schoolmasters," *The National Interest,* December 1, 2001, https://nationalinterest.org/legacy/the-four-schoolmasters-1181.
2. Douglas Ford, "Japanese Ground Warfare Tactics and the Army's Campaigns in the Pacific Theatres, 1943–1945: Lessons Learned and Methods Applied," *War in History* 16, no. 3 (July 2009): 325. See also Antony Best, "'This Probably Over-Valued Military Power': British Intelligence and Whitehall's Perception of Japan, 1939–41," *Intelligence and National Security* 12, no. 3 (1997): 67–94, https://tandfonline.com/doi/abs/10.1080/02684529708432431; Wesley K. Wark, "In Search of a Suitable Japan: British Naval Intelligence in the Pacific Before the Second World War," *Intelligence and National Security* 1, no. 2 (1986): 189–211, https://tandfonline.com/doi/abs/10.1080/02684528608431849; and John Ferris, "'Worthy of Some Better Enemy?': The British Estimate of the Imperial Japanese Army 1919-41 and the Fall of Singapore," *Canadian Journal of History* 28, no. 2 (Summer 1993): 223–56, https://utppublishing.com/doi/abs/10.3138/cjh.28.2.223.
3. Christopher Andrew, "Intelligence Analysis Needs To Look Backwards Before Looking Forward," *History and Policy,* June 1, 2004, https://www.historyandpolicy.org/policy-papers/papers/intelligence-analysis-needs-to-look-backwards-before-looking-forward/.
4. "USSR General Staff Academy Lectures: The Preparation and Conduct of Front and Army Offensive Operations," CIA/DO Report FIRDB-312/01545-78, July 28, 1978, https://www.cia.gov/readingroom/docs/1978-07-28.pdf (one of a series of seven lectures prepared for publication by the First Directorate (Operations) of the General Staff at the (Soviet) SECRET level); and "The Front Offensive Operation," *Intelligence Information Special Report,* June 15, 1979, https://www.cia.gov/readingroom/docs/1979-06-15.pdf (formerly Soviet TOP SECRET lecture materials).
5. CIA, "Warsaw Pact Ammunition Logistics in the Western Theater: Sustainability for Offensive Operations," SOV 89-10057CX, June 1989, https://www.cia.gov/readingroom/docs/1989-06-01.pdf.
6. CIA, "Warning of War in Europe: Changing Warsaw Pact Planning and Forces," National Intelligence Estimate (NIE) 4-1-84, September 1989, https://www.cia.gov/readingroom/docs/CIA-RDP94T00754R000200160012-0.pdf.
7. Nate Jones (project director), "The Able Archer 83 Sourcebook: The Definitive Online Collection of Over 1,000 Pages of Declassified Documents on the 1983 War Scare," National Security Archive, https://nsarchive.gwu.edu/project/able-archer-83-sourcebook; for one of the best summaries, see Ben B. Fischer, "A Cold War Conundrum: The 1983 Soviet War Scare," Intelligence Monograph, September 1997, https://www.cia.gov/readingroom/docs/19970901.pdf.
8. CIA, "Implications of Recent Soviet Military-Political Activities," Special National Intelligence Estimate (SNIE) 11-10-84/JX, May 18, 1084, https://www.cia.gov/readingroom/docs/DOC_0000278546.pdf.
9. Peter R. Mansoor and Williamson Murray, eds., *The Culture of Military Organizations* (Cambridge University Press, 2019), 14. Red Teamers will profit from the introductory and concluding chapters

and theoretical frameworks (by the editors and contributors Leonard Wong, Stephen J. Gerras, and David Kilcullen), as well as the specific cases.

10. Mansoor and Murray, *The Culture of Military Organizations,* 19.
11. Mansoor and Murray, *The Culture of Military Organizations,* 31.
12. Eugenia C. Kiesling, *Arming Against Hitler: France and the Limits of Military Planning* (University Press of Kansas, 1996), and translations of French classified discussions and French exercise critiques from the 1920s and 1930s, provide grist for discussions on French defense planning in a Johns Hopkins University graduate course. Two excellent examples of examining strategic geography are Robert J. Young, "Land, Resources, and Strategic Planning," in *In Command of France: French Foreign Policy and Military Planning, 1933-1940* (Harvard University Press, 1978), 13–32 (endnotes on 264–67); and A. W. Mitchell, *The Grand Strategy of the Habsburg Empire* (Princeton University Press, 2018), 21–51. Rich cases for other nations can be found in P. R. Mansoor and W. Murray, eds., *The Culture of Military Organizations* (Cambridge University Press, 2019); Kenneth M. Pollack, *Armies of Sand: The Past, Present, and Future of Arab Military Effectiveness* (Oxford University Press, 2019); Williamson Murray, Alvin Bernstein, and MacGregor Knox, eds., *The Making of Strategy: Rulers, States, and War* (Cambridge University Press, 1996); and Allan R. Millett and Williamson Murray, eds., *Military Effectiveness, Volume 2: The Interwar Period,* 2nd Ed. (Cambridge University Press).

INTELLIGENCE STUDIES SUMMIT 2026

Visit the NIU website, NI-U.edu,
for updates about future ISS dates
and locations.

Defining the Discipline **Shaping the Future**

https://www.ni-u.edu

https://www.linkedin.com/school/nationalintelu

https://www.facebook.com/NationlIntelU

NIU_Engagement@niu.odni.gov