

PRISM

VOL. 11, NO. 2 | SPRING 2026



PRISM

VOL. 11, NO. 2, SPRING 2026

EDITOR-IN-CHIEF

John A. Pennell, Ph.D.

ASSOCIATE EDITORS

COL Kevin D. Stringer, USA (Ret.),
Ph.D.

Joshua A. Hastey, Ph.D.

Sandor Fabian, Ph.D.

EDITOR-IN-CHIEF EMERITUS

Michael Miklaucic

COPY EDITOR

SGM Kanessa R. Trent, USA (Ret.),
MEd.

EDITORIAL ASSISTANT

V. Jocelynn Lake

DESIGN

Marco Marchegiani, U.S.
Government Publishing Office

EDITORIAL ADVISORS

COL (ret.) Prof. David A. Brown
Melanie Casey

Dr. William T. Eliason

Dr. Whitney Grespin

CAPT (ret.) William Hamblet

AMB (ret.) Philip S. Kosnett

Dr. Ajit Maan

Dr. Asta Maskaliunaite

Dr. C. Anthony Pfaff

Beth E. Sanner

Dr. George Spencer Terry

Dr. Michael G. Vickers

GEN (ret.) Joseph L. Votel

Dr. Vivian Walker

Prof. Jeffrey Zinsmeister, JD

ABOUT

PRISM: The Journal of Complex Operations is the U.S. Department of War (DOW) Irregular Warfare Center's (IWC) flagship journal of national and international security affairs. *PRISM*, which is published semiannually, aims to "provide unique insight for current and future national security leaders on emerging security challenges beyond the strictly military domain of the joint force, including transnational, multi-domain threats, gray zone conflict, the technological innovation challenge, and geoeconomic competition among the great powers." For more information, visit our website at <https://irregularwarfarecenter.org/prism/>.

SUBMISSIONS

PRISM: The Journal of Complex Operations welcomes unsolicited manuscripts from policymakers, practitioners, and scholars, particularly those that present fresh thought, enduring insight, or best practices related to the emerging national security environment. We seek to publish provocative, insightful, and well-reasoned submissions. We welcome contributions not only from established authorities in the field but also emerging voices, including early career practitioners, policymakers, and scholars.

PRISM accepts three types of submissions:

- Research articles
- Standard book reviews
- Extended book reviews

For additional information on submission requirements and the review process, visit our website at <https://irregularwarfarecenter.org/prism/> or contact us at PRISM@irregularwarfarecenter.org.

DISCLAIMER

This is the authoritative, official U.S. Department of War (DOW) edition of *PRISM: The Journal of Complex Operations*. Any copyrighted portions of this journal may not be reproduced or extracted without permission of the copyright proprietors. *PRISM* should be acknowledged whenever material is quoted from or based on its content. The opinions, conclusions, and recommendations expressed or implied within are those of the contributors and do not necessarily reflect the views of DOW or any other agency of the Federal Government, or any other organization associated with this publication.

FEATURES

- 3 **Editor-in-Chief's Introduction**
- 8 **When States Go Rogue: Criminal Tools in Hybrid Warfare**
By Roberta Koleva and Atanas Rusev
- 29 **Agriculture as a Domain of Hybrid Warfare: China's Strategy and U.S. Security Gaps**
Dr. Alicia Ellis and Sarah Shoer
- 46 **Understanding Cognitive Warfare: Beyond Information**
By Dr. Robert Schmidle, Lieutenant General (Retired, USMC)
- 64 **Medical Intelligence in Support of Irregular Warfare**
By Ryan M. Leone, Mason H. Remondelli, Victoria M. Perez, Kirsten Lalli, Regan F. Lyon, Jay B. Baker, Dan Hanfling, Ronald D. Hardin, Robert G. Cockerham, Derek J. Licina
- 77 **Strategic Culture – A Complex Model for a Complex Concept**
By Lawrence A. Kuznar, Nathan C. Heath, and George R. Popp
- 92 ***Maskirovka* and the Olympics: The Russian Choice to Initiate Conflict During the Olympic Games**
By G. Doug Davis, Michael Slobodchikoff, and Elizabeth Holley Dubose
- 109 **Soft Power by Design: China's United Front Strategy for Taiwan's Civil Society in the Age of Irregular Warfare**
By Yenting Lin
- 117 **Countering Hostile Chinese Lawfare: An Irregular Warfare-Based Approach**
By Crispin M. I. Smith
- 130 **From Saguntum to Taipei: The Hazards of Strategic Ambiguity**
By Robert Boudreau and James L. Johnsen
- 141 **Mapping the BRICS Plus Cryptocurrency Ecosystem: Is the BRICS Plus Bloc Effectively Using Cryptocurrency to Avoid Sanctions?**
By Kathleen Cassedy, Anne Walton, and Ian Conway
- 166 **Equity Chain Mapping: Adapting Counter Threat Finance for Great Power Competition**
By Ian Conway and Kathleen Cassedy
- 187 **Shadow Strategy: Air and Space Power in the Gray War**
By Dr. J. William (Bill) DeMarco
- 196 **Controlling Command: Is AI Capturing the Ethics of War?**
Dr. James Giordano and Dr. Elise G. Annett
- 204 **Preparing for Future Wars: Incongruent Beliefs on Autonomous Weapons**
By Major Nelson R. Godbolt, Craig Douglas Albert, PhD, Lance Y. Hunter, PhD, and Jeffrey Morris, PhD.
- 223 **Warfare in the Technology Arena: Cost-Imposition and Maneuver in the Electromagnetic Battlespace**
By Lt. Col. Sean "Nick" Blas

BOOK REVIEWS

234 *Human, Machine, War: How the Mind-Tech Nexus Will Win Future Wars*

Reviewed by Dr. Robert J. Bunker

241 *Those Who Face Death: The Untold Story of Special Forces and the Iraqi Kurdish Resistance*

Reviewed by Dr. Tom Searle

Editor-in-Chief's Introduction

I am deeply honored to assume the role of Editor-in-Chief of *PRISM: The Journal of Complex Operations*. As the distinguished journal of the U.S. Department of War's (DOW) Irregular Warfare Center (IWC), it is a privilege to continue the publication's storied tradition of excellence. I look forward to advancing *PRISM's* mission as the leading forum for rigorous, cutting-edge scholarship and policy-focused research on irregular warfare, gray zone conflict, and strategic competition. This issue reflects the IWC's mission to advance understanding of irregular warfare and equip practitioners with ideas they can apply in real campaigns. The IWC connects scholars, operators, and policy-makers around the evolving character of irregular warfare and strategic competition—from gray-zone coercion and proxy conflict to cyber, lawfare, and information operations—and *PRISM* serves as its primary forum for that dialogue. Our goal is not only to analyze how adversaries wage irregular war, but also to help the United States and its allies and partners think creatively about doctrine and capabilities in a world where the boundaries between war and peace are increasingly blurred.

Irregular warfare has moved from the periphery of security studies to the center of twenty-first-century strategic competition. Great and middle powers now blend covert action, cyber operations, criminal networks, economic leverage, lawfare, and influence campaigns into integrated “gray war” strategies designed to erode rivals without triggering open

conflict. This spring 2026 issue of *PRISM* examines that shifting landscape from multiple angles: how states weaponize crime and agriculture; how cognitive warfare and lawfare reshape competition; how emerging technology, artificial intelligence (AI), and autonomous systems are reconfiguring command, ethics, and deterrence; and how air, space, cyber, and the electromagnetic spectrum are becoming contested maneuver spaces in their own right. Taken together, these seventeen contributions – fifteen articles and two book reviews – offer a multi-domain primer on irregular warfare in an era where the boundaries between war and peace, civilian and combatant, legal and illicit are increasingly porous.

We open the issue with Roberta Koleva and Dr. Atanas Rusev's “When States Go Rogue: Criminal Tools in Hybrid Warfare.” Drawing on the criminology of state crime and the post-Cold War evolution of organized crime, they show how contemporary regimes embed sanctions evasion, illicit trade, financial crime, and state capture into hybrid campaigns rather than treating them as aberrations. While investigating the distinct models by which China, Iran, and Russia blur the lines between state and illicit activity, they argue that the convergence of state, criminal, and corporate actors is a structural feature of modern politics rather than a deviation. Such models reflect a system in which “criminality is not a corruption of the state, but a corruption for the state.”

From the criminal underworld, we move to a vital but often overlooked strategic domain: agriculture. In “Agriculture as a Domain of Hybrid Warfare: China’s Strategy and U.S. Security Gaps,” Dr. Alicia Ellis and Sarah Shoer argue that agriculture should be treated as critical infrastructure given that it is a deliberate target and instrument of hybrid coercion. They document how the People’s Republic of China (PRC) is building upstream leverage through fertilizer dominance, ag-tech acquisitions, land purchases, and control of key logistics nodes, creating potential chokepoints in U.S. and global food systems. The article introduces an Agriculture Security (“AgSec”) framework that aims to protect “farm-to-fork infrastructure” from disruption, manipulation, or exploitation by adversaries and integrating agriculture into hybrid deterrence planning on par with other forms of critical infrastructure.

The third article, by Lt. Gen. (Ret.) Robert Schmidle, turns to the battle for perception and meaning itself. “Understanding Cognitive Warfare (CogWar): Beyond Information” seeks to answer how is CogWar different from information operations (IO), political warfare, propaganda, and other forms of non-kinetic warfare. Drawing on psychology, neuroscience, strategy, sociology, and post-modern philosophy, Schmidle argues that CogWar’s battlespace is over perceptions – both of enemy and friendly populations. As such it is a continuous, societal-level struggle in which adversaries seek to re-engineer moral forces, identity, and trust—often leveraging AI, social media, and narrative manipulation to generate cognitive dissonance and erode resilience. Unlike traditional IO, CogWar targets the social and cultural structures that produce “truth” in a society, blurring any meaningful distinction between wartime and peacetime competition.

If CogWar contests the mind, medical intelligence (MEDINT) contests the human body and

health systems that sustain combat power and legitimacy. In “Medical Intelligence in Support of Irregular Warfare,” 2LT Ryan M. Leone and colleagues examine the evolution and future of MEDINT as a critical enabler of irregular and gray-zone operations. They trace MEDINT from early epidemiological breakthroughs to contemporary conflicts in Ukraine, Syria, and counterterrorism campaigns, highlighting how intelligence on disease, medical infrastructure, and adversary health capabilities can both protect friendly forces and create exploitable vulnerabilities in enemy networks. The authors contend that MEDINT is a critical enabler for force protection and achieving operational objectives as current and future wars increasingly entail irregular tactics, decentralized operations, and contested communications environments. Integrating novel intelligence methods and new technologies with MEDINT will, they argue, help maintain advantage over an adversary.

Building on these conceptual and functional foundations, Lawrence Kuznar, Nathan Heath, and George Popp address the cultural underpinnings of strategy in “Strategic Culture – A Complex Model for a Complex Concept.” Revisiting decades of debate on whether strategic culture explains or merely contextualizes behavior, they utilize a complex-systems model built around identity, values, norms, and perceptive lenses. Their Strategic Culture System Model (SCSM) treats these elements as mutually reinforcing nodes that shape how states perceive threats, opportunities, and the utility of irregular tools, illustrated through a study of Russian strategic culture in the ongoing war in Ukraine. For practitioners, the payoff is an analytic framework, not based on cultural determinism, but one situated for adapting strategic culture to a particular context in a manner that helps anticipate red lines and develop potential responses in irregular competition.

G. Doug Davis, Michael Slobodchikoff, and Elizabeth Holley Dubose then provide a vivid case of

hybrid deception in “*Maskirovka* and the Olympics: The Russian Choice to Initiate Conflict During the Olympic Games.” They examine Russia’s pattern of timing operations in Georgia (2008), Crimea (2014), and Ukraine (2022) around Olympic Games, using the global media focus and the symbolism of peace to create a “fog of falsehood” that advances Russia’s geopolitical interests. Framing this practice within the Russian doctrine of *maskirovka* and reflexive control, the authors show how major international events can be exploited as strategic diversions, turning moments of global unity into windows of heightened vulnerability.

The middle portion of the issue focuses on China’s political warfare toolkit. Yenting Lin’s “Soft Power by Design: China’s United Front Strategy for Taiwan’s Civil Society in the Age of Irregular Warfare” dissects how Beijing uses United Front organizations, influencers, educational exchanges, religion, and social networks as part of a long-term campaign to shape how Taiwanese society understands the PRC, Taiwan, and reunification. Rather than overt coercion, the strategy relies on long-term socialization, particularly of youth, through seemingly apolitical content that normalizes PRC narratives and erodes trust in Taiwan’s democratic institutions by eroding trust, dividing society, and weakening confidence in democracy. Lin’s work underscores that Taiwan’s frontline is as much in classrooms, livestreams, and temples as it is in the Taiwan Strait.

Crispin Smith’s “Countering Hostile Chinese Lawfare: An Irregular Warfare-Based Approach” complements Lin by examining the PRC’s sophisticated use of law as a strategic weapon. He shows how Beijing leverages “legal warfare” to legitimize its own actions, constrain U.S. and allied operations, and shape international norms in areas such as the South China Sea, cyberspace, and on Taiwan’s status. Smith argues that lawfare is a central component of Chinese irregular doctrine, not a peripheral

legal issue, and advocates for an integrated counter-lawfare strategy rooted in irregular warfare thinking, joint interagency teams, and proactive narrative and legal engagement.

Robert Boudreau and James Johnsen then take us back to antiquity to illuminate a very modern dilemma in “From Saguntum to Taipei: The Hazards of Strategic Ambiguity.” Using Rome’s ambiguous posture toward Saguntum on the eve of the Second Punic War, they argue—through the lens of prospect theory—that ambiguity invites offense by forcing aggressors to weigh the risks of action against the risks of forgoing opportunity. They apply this insight to U.S. policy toward Taiwan, contending that continued strategic ambiguity may increase the likelihood of PRC miscalculation and thus they recommend that the U.S. move toward greater clarity about its commitments toward Taiwan.

Financial and technological infrastructures form a second major thread in the latter part of the issue. Kathleen Cassidy, Anne Walton, and Ian Conway’s “Mapping the BRICS Plus Cryptocurrency Ecosystem: Is the BRICS Plus Bloc Effectively Using Cryptocurrency to Avoid Sanctions?” investigates how Russia, the United Arab Emirates, and other BRICS Plus members are experimenting with cryptocurrencies, stablecoins, and alternative payment systems to erode U.S. sanctions leverage. Using blockchain forensics and equity-chain mapping, they trace how digital assets can support sanctions evasion and reduce BRICS Plus members reliance on Western financial systems, but they claim that the evidence is inconclusive that cryptocurrency is an effective tool to avoid sanctions.

In a companion piece, Ian Conway and Kathleen Cassidy’s “Equity Chain Mapping: Adapting Counter Threat Finance for Great Power Competition” retools Global War on Terrorism-era counter-threat finance (CTF) and counter-threat network (CTN) methods for state-level competition. They introduce equity chain mapping (ECM) as

a commercially driven methodology for unpacking clandestine ownership and control structures behind critical technologies—illustrated through a case study of autopilot software used in Russia’s Orlan-10 unmanned aerial vehicle (UAV) system. The article argues that integrating ECM with CTF/CTN doctrine can help identify corporate infrastructure that enables adversary military capabilities and guide more targeted sanctions and enforcement.

Bill DeMarco’s “Shadow Strategy: Air and Space Power in the Gray War” reframes air and space forces as tools of influence and disruption below the threshold of major combat. He distinguishes gray war from political and hybrid warfare, and argues that persistent intelligence, surveillance, and reconnaissance (ISR), attribution, and signaling from air and space can expose covert activities, impose reputational costs, and deter incremental aggression without having to fire a shot. He argues that this requires doctrinal and organizational shifts so that U.S. air and space power are optimized for persistent shaping, strategic messaging, and cognitive influence rather than only for traditional kinetic deterrence.

The final three articles confront the technological and ethical frontier of warfare. James Giordano and Elise Annett’s “Controlling Command: Is AI Capturing the Ethics of War?” examines how increasingly autonomous AI systems are used to achieve advantages in speed, precision, and operational scale, but also introduce unprecedented ethical, legal, and strategic challenges. To help counter these challenges, they argue that accountability must remain anchored in human decision-makers and propose a framework that enables ethical oversight, guidance, and use of military AI that maintains human values and agency “in and on the loop” of AI-enabled operations.

Nelson Godbolt, Craig Albert, Lance Hunter, and Jeffrey Morris extend the AI debate into the operational future in “Preparing for Future Wars:

Incongruent Beliefs on Autonomous Weapons.” They highlight a growing divergence between technological trajectories and political-ethical beliefs about lethal autonomous weapons systems (LAWS), noting that electronic warfare (EW) and contested communications may push militaries toward fully autonomous systems despite current norms. The article argues that serious conflict with peer adversaries could create powerful incentives to field LAWS before comprehensive treaties or ethical regimes are in place, and calls for urgent work on deterrence, doctrine, and governance in anticipation of “robot wars” or hybrid conflicts where LAWS feature prominently.

We close the article section with LTC Sean “Nick” Blas’ “Warfare in the Technology Arena: Cost-Imposition and Maneuver in the Electromagnetic Battlespace.” Using lessons from the ongoing Russia–Ukraine war, Blas treats the electromagnetic spectrum (EMS) as a maneuver space and explores how cost-imposition strategies and low-cost commercial technologies—such as high-altitude platforms—can help the United States regain advantage in a highly contested EMS environment. He argues that the U.S. needs to recognize the EMS as a critical battlespace and that understanding and practicing electromagnetic maneuver, both physical and non-physical, will be essential to sustaining joint all-domain operations under persistent jamming and cyber pressure.

Two book reviews round out the issue by situating these debates in the wider literature of future war and irregular campaigns. Dr. Robert J. Bunker’s review and “epochal change” critique of *Human, Machine, War: How the Mind-Tech Nexus Will Win Future Wars* engages an Air University Press anthology on the “mind-tech nexus,” praising its synthesis of neuroscience, AI, and command while challenging its assumptions about the nature and conduct of war in an era of autonomous systems and human–machine convergence. Bunker argues that

emerging technologies may represent an out-of-paradigm shift closer to civilizational change than to a routine revolution in military affairs (RMA), with implications for who—states, private military companies (PMCs), or augmented humans—will first realize the full potential of the mind-tech nexus.

Dr. Tom Searle's review of Mark Grdovic's memoir *Those Who Face Death: The Untold Story of Special Forces and the Iraqi Kurdish Resistance* then brings us back to the human level of irregular warfare, highlighting the often-overlooked role of battalion-level staff officers and Special Forces working alongside the *Peshmerga* in northern Iraq in 2003. Searle argues that Grdovic's candid account of staff work, transition moments between peace and war, and ethically fraught guidance offers indispensable material for professional military education (PME) and for understanding how irregular campaigns are planned, misplanned, and lived by those "who face death" on the ground.

Taken together, these contributions reflect *PRISM's* commitment, as the IWC's flagship journal, to bridging theory and practice in irregular warfare. They illustrate how today's contests are fought as much through financial networks, lawfare, narratives, infrastructure, and code as through kinetic engagements. They also underscore a common imperative: the United States and its allies and partners must adapt doctrine, capabilities, and ethical frameworks for a world in which state-proxy ecosystems, weaponized interdependence, cognitive warfare, and emerging technologies are not peripheral phenomena but the main battlegrounds of strategic competition.

DR. JOHN A. PENNELL
Editor-in-Chief

When States Go Rogue

Criminal Tools in Hybrid Warfare

By Roberta Koleva and Atanas Rusev

The concept of state crime has been extensively debated since the 1980s, encompassing a range of illegal, deviant, or harmful activities perpetrated by or with the complicity of state agencies.¹ By the early 21st century, scholars approached state crime through diverse theoretical frameworks, including analyses of structural contradictions within governance, the interplay between legality and legitimacy, and as an integral component of political and economic systems.² However, one such scholar—Friedrichs—cautioned that many existing frameworks were retrospectively focused on atrocities of the 20th century and advocated for a “prospective criminology” capable of anticipating and critically engaging with evolving forms of state criminality.³

Global events have reaffirmed the need for criminology to account for new and complex conceptualisations of state criminality. The Russian invasions of Ukraine in 2014 and then again in 2022 have been widely characterised not only as violations of international law but also as an example of hybrid warfare, where state crime is embedded as a geopolitical strategy.⁴ The Center for the Study of Democracy (CSD)’s studies over the years have illustrated Russia’s use of sanctions evasion, illicit trade, disinformation campaigns, and cyber warfare as part of a broader strategy of influence and destabilisation.⁵ Such developments complicate traditional definitions of state crime and accountability, particularly as third-party states, private entities, and transnational non-state actors play key roles in facilitating or resisting these practices. Simultaneously, this is not merely a theoretical debate but one with urgent practical

Atanas Rusev is the Security Program Director at the Center for the Study of Democracy (CSD). The Center is the first independent non-profit public policy institute in Bulgaria. After joining CSD in 2010, he has worked on a number of international research projects on crime and security, funded by the European Commission. His research focus is related to organized crime and in particular drug trafficking and drug markets, organized property crime, illicit trade in tobacco products, prostitution markets and human trafficking, organized VAT frauds, extortion, and loansharking. He is an author of various publications on corruption and organized crime, financing of organized crime, organized crime threat assessment and confiscation of criminal assets.

Roberta Koleva is a social anthropologist and an Analyst with CSD’s Security Program. Her work and research interests focus on the anthropology of post-socialism, political economy, nationalism studies, and urban anthropology, with an emphasis on Southeastern Europe and critical theory. At CSD she contributes to research on state-sponsored crime, threats to civil society in Bulgaria, and the rise of radicalization and far-right movements in the Western Balkans.

dimensions, increasingly recognised by key European institutions. Europol's latest Serious and Organised Crime Threat Assessment (SOCTA) report explicitly warns how state actors exploit criminal infrastructures and illicit economies as part of broader geopolitical strategies, signalling an institutional shift toward acknowledging the convergence of statecraft and organised crime. The geopolitical landscape of 2025 thus compels criminologists to rethink emerging forms of state criminality and their conceptualization.⁶

Structured in two main parts, bridging past and future, this article situates scholarly debates on state crime within the current geopolitical context, particularly concerning hybrid warfare, economic crime, and transnational illicit networks. The first section retrospectively analyzes the intellectual genealogy of state crime within criminology and related disciplines. It examines paradigmatic approaches – including harm-based models, human rights perspectives, and legalist and structural analyses – that have influenced and been influenced by rapid political and economic transformations of the 20th century. While foundational, these frameworks exhibit definitional ambiguities, methodological limitations, and neglected areas, prompting questions about their adequacy in capturing contemporary state criminality.

The second part takes a prospective turn to analyse what we term strategic state-sponsored criminality – a distinct assemblage of criminal practices that are coordinated, instrumentalized, and embedded within hybrid warfare. Drawing on current landscape – marked by Russia's weaponization of illicit networks (but also Iran's strategic use of cybercrime, China's state-backed economic coercion, etc.), we call for a rethinking of how we define, study, and address state criminality. Besides previous calls to anticipate future state crimes, the present moment demands a recalibration of criminological imagination. As the boundaries

between governance, legality, and criminality become increasingly porous, it is imperative to reconsider whether state crime remains an aberration in the international order or has instead become a structural feature of contemporary power relations.

TRACING THEORETICAL LEGACIES ON STATE CRIMINALITY: A RETROSPECTIVE LOOK

Dawn L. Rothe has convincingly argued that state crimes, such as genocides, state-sponsored terrorism, assassinations, etc., have resulted in more harm than conventional street crimes, yet have historically been understudied relative to traditional forms of criminality within criminology and criminal justice research.⁷ Early criminological thought, particularly in its positivist forms, focused on individual deviance, framing crime as a pathology of the working classes.⁸ For example, dominant theories by Lombroso positioned the state as a lawful authority, rendering crimes by those in positions of power, whether corporate executives or state actors almost unthinkable.⁹

By the 1950s, a growing number of criminologists began to question these assumptions. Major atrocities, from the Holocaust to the Rwandan Genocide, challenged the notion that crime was solely the domain of individuals acting outside the law. Cold War-era covert operations, state-backed coups, and extensive state surveillance apparatuses in both capitalist and socialist blocs further demonstrated that states could perpetrate vast, coordinated acts of harm while maintaining a veneer of legality. The neoliberal economic turn of the 1980s and 1990s added further complexity, as some state-led economic restructuring programs, often implemented through austerity measures and structural adjustment, resulted in widespread economic and social harm, such as inequality, loss

of social safety and security, etc. The emergence of global corporate networks and the proliferation of offshore zones led to expanding transnational organized crime networks and the obfuscation of ownership and perpetrator identification.

Coupled with financial crimes and deregulation policies that enabled corporate – political – state collusion or even state capture, these transformations raised critical questions about the blurred boundaries between harmful governance and state criminality.¹⁰ Furthermore, research by CSD has illustrated how in post-socialist contexts this turn introduced new dynamics of state-facilitated harm, as the privatization of public assets and the weakening of institutional oversight created fertile ground for **state capture**, in which private interests subvert public institutions for personal or political gain.¹¹ These processes highlight how contemporary state crime often manifests not only through overt acts of violence but also through the structural enabling of corruption, illicit trade, and the erosion of democratic accountability.

One of the first thinkers who marked a significant departure from mainstream criminology, Sutherland demonstrated that corporate crimes perpetrated by elites could be as harmful, if not more so than conventional street crimes.¹² However, as later scholars noted, even Sutherland’s pioneering work did not explicitly extend his critique to government institutions, even though corporate crime was often facilitated, ignored, or actively supported by the state.¹³ This omission highlighted the **persistent legalistic bias**, where crime was still conceptualized within the boundaries of existing legal frameworks rather than as a broader category of social harm – a problem that would later become central in definitional debates around state criminality.

A more radical shift in criminological thought emerged in the 1970s amid political unrest,

anti-war mobilisations, and increasing exposure to state abuses. Marxist, structuralist, and critical criminological perspectives challenged traditional understandings by arguing that crime is not an objective, legally defined phenomenon but a socially constructed category shaped by power relations, illustrating how **law itself is a political tool**, that enables selective enforcement on crime.¹⁴ A key intervention came with Foucault’s *Discipline and Punish*, which demonstrated how disciplinary power produces categories of criminality and deviance, legitimising state violence while criminalising resistance.¹⁵ This critique foregrounded the state’s monopoly over legality as a crucial site of contestation, exposing how legal definitions are mobilised to shield state actors from accountability while expanding criminalisation toward dissenting populations.

These debates eventually culminated in a significant turning point with Chambliss’ presidential address to the American Society of Criminology in 1989, where he directly called for the study of “**state-organized crime**.”¹⁶ Identifying various forms of state-organized crime, including state complicity in piracy, coups d’état, assassinations, domestic surveillance, financial fraud, arms trafficking to sanctioned countries, and the sponsorship of terrorist activities, his work emphasized that state crime should not be understood merely as individual corruption or abuse of power but as an organizational and structural phenomenon often embedded within the rational functions of governance itself. This intervention marked a crucial step in paving the way for new theoretical perspectives that accounted for state criminality as an enduring feature of modern governance.

This intellectual shift also posed new challenges: if state criminality was not simply a matter of individual misconduct but instead could be woven into the fabric of governance, what

analytical frameworks and criteria could capture its complexities, especially when states themselves controlled the legal apparatus that determined what counted as a crime? As scholars engaged with these emerging questions, the study of state crime increasingly became a battleground for new definitional debates, each offering different epistemological and methodological criteria for identifying state criminality. Michalowski outlined **three primary theoretical models that shape criminological discourse on state crime**: the juridical (legalistic) model, the conduct norms model, and the social harm model, which became central to understanding and contesting the boundaries of state criminality in the decades that followed.¹⁷

- One of the earliest frameworks for defining state crime has been **the legalist approach**, which views state crime as any act by state officials that violates domestic or international law. Chambliss was instrumental in advancing this view, identifying **state-organized crime** as acts “*defined by law as criminal and committed by state officials in the pursuit of their jobs as representatives of the state.*”¹⁸ In the 1990s, efforts to expand the model incorporated international human rights law through institutions like the ICC and ad hoc tribunals.¹⁹ Still, as Michalowski observed, legalist approaches remained limited by global power asymmetries, often targeting weaker states while protecting powerful ones.²⁰
- In response to the limitations of legalist definitions, scholars turned to the **conduct norm approach**, which argued that state crime should be defined by broader societal understandings of justice. This perspective emphasises human rights violations – such as torture, repression, and economic exploitation – as central to the definition of

state crime. Green and Ward built upon this framework, arguing that state crime should be conceptualized as acts of organizational deviance in which state officials or institutions pursue policies that systematically harm populations.²¹ The approach gained traction amid globalisation, as economic restructuring, corporate deregulation, and austerity measures were seen by many as **economic state crimes** due to their devastating social impact on social welfare systems in the Global South, despite being legal.²² The concept of “**crimes of globalization**” further extended this critique to supranational institutions complicit in structural violence.²³ However, while significantly expanding the scope of state crime beyond legal frameworks, this model was criticized due to its reliance on socially constructed definitions of deviance. As Michalowski noted, its reliance on socially constructed norms makes definitions of harm context-dependent and vulnerable to dominant geopolitical narratives, with selective recognition of state crimes.²⁴

- The **social harm approach** marked a further break from legalist and rights-based models, arguing that state crime should encompass any systemic harm caused by state policies, regardless of legality.²⁵ Influenced by Marxist and structural violence theories, it highlighted harms such as environmental degradation, economic dispossession, and militarization. Central to this framework was the concept of **state-corporate crime**, encompassing both state-initiated and state-facilitated harms – from war profiteering to corporate abuse.²⁶ This model gained traction after the 2008 financial crisis, where deregulation and state inaction enabled widespread corporate fraud and economic exploitation and in debates

on “ecocide,” pointing to state-led deforestation projects that displace indigenous populations for corporate gain.²⁷ However, while normatively and morally expansive, this model was also criticized for lacking enforceable mechanisms and objective standards for assessing harm, limiting its practical application.

Thus, as state scholarship moved forward towards the new century, the main challenge remained: *how can criminologists account for the layered and various complexities of state criminality while at the same time ensuring that such acts do not escape accountability?* These conceptual debates reflected a broader struggle to develop frameworks that account for power, structural violence, and global economic relations in response to the specific historical and geopolitical struggles of the times. It was the genocides of the late 20th century, the rapid rise of globalization, and the increasing collusion between state and corporate power that have all shaped criminological debates on how state crime should be understood and addressed. As **new forms of state crimes** emerge today, the question remains: are they still adequate for capturing the realities of contemporary state criminality?

STATE CRIMINALITY AND HYBRID WARFARE: TOWARDS A PROSPECTIVE APPROACH

If the dominant theoretical debates on criminality in the late 20th and early 21st centuries were shaped by large-scale atrocities – such as genocide, war crimes, authoritarian repression, and later, systemic human rights abuses, environmental degradation, and the erosion of public welfare under the guise of market rationality – today’s scholarly conversations are increasingly shifting toward more covert, deniable, and networked forms of state action. The rise of **hybrid warfare** has played a central role in

this shift.

Defined by Frank Hoffman as “any adversary that simultaneously and adaptively employs a fused mix of conventional weapons, irregular tactics, terrorism, and criminal behaviour,” and by NATO as a strategy that blends conventional, irregular, and cyber warfare with disinformation and economic coercion, hybrid warfare targets a society’s vulnerabilities across multiple domains to create confusion and strategic advantage.²⁸ While not a form of crime itself, **hybrid warfare constitutes the operational context in which new forms of state criminality unfold**. Unlike conventional warfare, which relies on direct military engagement, hybrid warfare enables state actors to simultaneously deploy legal, semi-legal and entirely illegal tactics, using proxies, cyber criminals, and criminal and financial networks to achieve strategic objectives while maintaining plausible deniability.

In this evolving context, state criminality is no longer confined to overt acts of violence or repression. Instead, it increasingly manifests through *covert, networked, and transborder aspects* – blurring the lines between state and non-state, legal and illegal, public and private spheres. Authoritarian states in particular have begun to *systematically weaponize and sponsor criminal networks*, embedding them into their foreign policy arsenals as tools of influence, disruption, and survival.²⁹ Such practices are increasingly central to how powers such as Russia, Iran, and China pursue advantage within the international system.³⁰ Particularly in the context of heightened global tensions following Russia’s 2014 and 2022 invasions of Ukraine, **the integration of transnational criminal actors into state strategies** has evolved into a deliberate and structured mode of warfare and governance, sometimes referred to as “organized crime as an instrument of statecraft.”³¹ This shift complicates inherited definitions of state crime and calls for a conceptual reorientation.

While recent literature has introduced a series of overlapping terms such as **geocriminality**, **state-organized crime**, **state-cybercrime**, **criminal statecraft**, etc., there is still no systematic theoretical framework akin to those developed for earlier forms of state criminality in the 20th century. Clarifying how these terms are used, what forms of criminality they encompass, and how they relate to or diverge from organized crime is a necessary step forward.

This section adopts a prospective approach. It first examines recent empirical cases from Russia, alongside comparative insights from Iran and China, to illustrate how such less theories of contemporary state criminality function within the context of hybrid warfare. It then reviews and assesses the current scholarly landscape, culminating in a working agenda proposal for a more systematic and analytically rigorous framework to capture a distinct category of contemporary state criminality what we would define as **strategic state-sponsored criminality** – the deliberate, coordinated use of criminal practices by states or with state consent, to achieve geopolitical, economic, or security objectives. Unlike historical state criminality, which often involved direct repression or corruption by officials within the domestic sphere, this emergent form is characterized by its transnational scope, covert operational style, and instrumental use of non-state actors. It is this distinct assemblage of features that warrants a rethinking of both theoretical and policy frameworks.

Comparative Models of Strategic State-Sponsored Criminality Today

Contemporary strategic state-sponsored criminality takes on diverse forms depending on the state's geopolitical ambitions, institutional structure, and tactical needs. While Russia, Iran, and China all engage in practices that strategically blur the lines between state and illicit activity, they do so through

slightly distinct models. These models – what we might term the militarized-criminal hybrid (Russia), the militia-criminal proxy model (Iran), and the corporate-criminal hybrid (China) – illustrate varying ways in which criminality is embedded into statecraft. Below, we trace these differences by examining each case in detail.

Russia: The Militarized-Criminal Hybrid

Russia represents perhaps the most well-documented case of a state that strategically deploys criminal networks and semi-legal actors to project influence and evade international legal repercussions. It exemplifies what is called a militarized-criminal hybrid: a governance structure where illicit actors are integral to statecraft, foreign policy, and warfare. The *Kremlin Playbook* series (2016–2025) has documented in detail how Russia operationalizes a **state capture model** – a systemic mode of governance in which economic, political, and media environments are reshaped to serve the interests of ruling elites and their strategic allies.³² This model involves the fusion of state and illicit networks, enabling the state to project influence beyond its borders while maintaining plausible deniability. While variations of state capture can be observed in other authoritarian contexts, including Iran and China, Russia's case stands out for the depth of integration between state institutions and proxy actors, combined with the ability to mask this integration within nominally legal, market-based, and democratic frameworks. This makes Russian state capture both structurally entrenched and uniquely deniable in the international arena.

As CSD and CSIS have illustrated, the Kremlin uses state capture as a model of domestic operation, and international influence, including the corrupt weaponisation of local ethnic warlords (Kadirov), private armies (Prigozhin), state enterprises (Gazprom), and organised crime.³³ Mark Galeotti similarly argues that the Kremlin has developed a

Table 1. Contemporary Models of Strategic State-Sponsored Criminality

Type of Activity	State Actor(s)	Mechanism	Description	Examples
Assassinations and targeted violence	Russia, Iran	Outsourced to proxies or intermediaries	Use of criminal or proxy actors to carry out killings or attacks on dissidents and defectors	Murder of Maxim Kuzminov in Spain (Russia); operations against opposition figures in Europe (Iran)
Cyber operations	Russia, Iran, China	State-directed or tolerated cyber actors	Cybercrime used for espionage, sabotage, and coercion, often through loosely affiliated criminal groups.	Sandworm and NotPetya (Russia); Albanian cyber attack (Iran); APT41 cyber-espionage (China)
Weapons smuggling	Russia, Iran	Proxy networks and covert logistics	Covert transfers of arms to militias or partner regimes through illicit channels	IRGC's Unit 190 shipments to Hezbollah; Wagner's arms deals in Africa
Sanctions evasion	Russia, Iran	Shell companies, crypto laundering	Circumvention of international sanctions using opaque financial networks	Russian smuggling via Turkey/UAE; Iranian ship-to-ship oil transfers
Illicit economic networks	Iran, Russia	Informal financial systems, trafficking	Use of narcotics, gems, oil, and informal value transfer systems to generate regime revenue	Crystal meth trade on the Iran-Iraq border; diamond smuggling via Hezbollah
Disinformation and subversive actions	Russia	Propaganda channels and cyber-influence tools	Information operations aimed at destabilizing foreign societies and discrediting democratic institutions.	RT/Sputnik disinformation; troll farms targeting Black Sea and Eastern Europe (CSD 2024)
Migration weaponization	Russia, Belarus	Use of smuggling networks and coercion	Facilitating or forcing irregular migration flows to create political instability in neighbouring states.	Belarus–Poland border crisis (2021–2022); Russia–Finland border incidents
Financial crime and money laundering	Russia, Iran	Crypto exchanges, fake enterprises	Laundering illicit proceeds through cryptocurrency and informal financial infrastructures	Bitzlato crypto laundering (Russia); hawala networks supporting Hezbollah
Use of private military companies	Russia	State-authorized private force with criminal roles	Deployment of private military actors for geopolitical, commercial, and violent ends	Wagner Group's role in Ukraine, Syria, and African conflicts
Use of ideological proxy militias	Iran	Militant groups aligned with regime ideology	Delegation of warfare and illicit operations to non-state actors with political and religious affiliations	Hezbollah in Lebanon/Syria; Houthis in Yemen; Shi'a militias in Iraq
Corporate espionage and IP theft	China	State-owned firms and corporate insiders	Theft of trade secrets and technology through legal firms acting as state agents	Hytera theft from Motorola; Linwei Ding AI theft case; Operation CuckooBees

Source: Center for the Study of Democracy (CSD).

“weaponized underworld,” integrating organized crime into its foreign policy toolkit with its use of criminal networks evolving from opportunistic collaborations in the post-Soviet era into a **coherent**

and deliberate method of hybrid warfare.³⁴

This shift has become especially visible following the full-scale invasion of Ukraine in 2022 when Western sanctions and diplomatic isolation pushed

the Russian regime to further blur the boundaries between state, para-state, and criminal actors, emerging as a critical case study for the evolving forms of state criminality of the current geopolitical landscape.

The roots of this relationship trace back to the Soviet period when the KGB used elements of the *vorovskoi mir* (the thieves' world) as informal collaborators and sources of intelligence. During the 1990s, amid the economic collapse and weakened state institutions, organized crime surged and often filled governance voids.³⁵ However, under Vladimir Putin, a former KGB officer, this relationship was restructured. Rather than attempting to dismantle organized crime, the state co-opted and subordinated it, transforming criminal groups into controllable auxiliaries of the regime. In what Galeotti describes as the transition from a "conscription state" to a "mobilization state," **criminal actors became embedded within Russia's geopolitical logic, tasked with fulfilling strategic functions in the grey zones of international politics.**³⁶

This co-optation has manifested across multiple domains. Since 2022, organized crime groups have taken on overtly geopolitical roles in support of Russia's war effort and broader foreign policy as well as in helping the Kremlin evade wide-ranging economic sanctions.³⁷ Türkiye sits as a transit hub for Russian energy and financial sanctions evasion enabled by private and organized criminal (OC) networks. **The Wagner Group** is perhaps the most prominent example of such an instrumentalized OC group: initially presented as a private military company (PMC), Wagner has conducted illicit mining operations, arms deals, and military interventions across Africa and the Middle East, finally filling in for the Russian army's most atrocious behavior in Ukraine. Its formal designation by the U.S. government as a transnational criminal organization in 2023 reflects its dual status as both

state proxy and criminal enterprise.³⁸ Similar roles have been well-documented for local warlords, such as Ramzan Kadirov, as well as Russian prisoners, sent to fight in Ukraine.

At the same time, organized crime has been instrumental in **helping Russia evade sanctions.** Smuggling networks and shell companies, particularly in jurisdictions such as Türkiye, Cyprus, the UAE, and Kazakhstan, have allowed for the continued flow of restricted goods – including microchips, military-grade electronics, and dual-use technologies – into Russia.³⁹ These grey-market logistics networks, often run by or in collaboration with criminal syndicates, play a vital role in sustaining the Russian defence industry under embargo conditions.⁴⁰ This illicit economic infrastructure functions not only with the tacit but with the explicit consent and direct sponsorship of the state, reinforcing a **logic of transactional sovereignty** – a system in which the rule of law is selectively applied according to the strategic needs of the state. In such a system, impunity is not guaranteed by legality but by utility. Criminal actors are permitted to operate freely so long as they serve the geopolitical objectives of the Kremlin. Loyalty, usefulness, and deniability become the currencies of protection, allowing criminal networks to flourish in exchange for strategic service. This dynamic marks a shift in Russian governance from fragmented post-Soviet corruption toward a model of state capture in which the state actively mobilizes illicit actors as integral components of its hybrid warfare arsenal.⁴¹

Financial crime has likewise become a key domain of collusion between the Russian state and its transborder criminal intermediaries. Cryptocurrency platforms such as Bitzlato – sanctioned by the U.S. in 2023, and before that HYDRA, sanctioned in 2022 – have been exposed as money laundering hubs facilitating the movement of illicit funds between Russia and criminal markets

abroad.⁴² These funds often serve dual purposes: financing covert operations and sustaining pro-Russian political actors in Europe, the Balkans, and the Global South. Russia has also actively used illicit gold trade in Türkiye to buy weaponry and dual use goods.⁴³

Cyber operations offer perhaps the clearest example of how the Kremlin has transformed cybercrime into a strategic asset. At least since the mid-2000s, Russian-speaking cybercriminals have operated under the informal patronage of state security services, particularly the FSB's Directorate K. These actors serve both profit-oriented and strategic functions, conducting ransomware campaigns, espionage, and sabotage. Groups such as Sandworm and Smokey Spider, closely linked to the GRU (Russia's military intelligence agency), have executed high-profile attacks including the NotPetya malware incident and repeated DDoS attacks on Ukraine's infrastructure.⁴⁴ According to the European Union Agency for Cybersecurity, such operations have intensified post-2022 and are often executed by actors who are technically independent but protected by the state as long as they target foreign systems.⁴⁵ This state-sanctioned impunity has fostered a "cybercrime ecosystem," where espionage, sabotage, and extortion merge into a single, state-tolerated and state-sponsored threat environment.⁴⁶

Russia has also turned to transnational organized criminal networks as a means of plugging the gaps created by the expulsion of more than 400 Russian diplomats and suspected intelligence agents from Europe since the war began. In countries like Poland, Spain, and Estonia, Russian security services have reportedly relied on **local criminal actors** for surveillance, smuggling, and targeted violence. The assassination of defector Maxim Kuzminov in Spain, for example, is widely believed to have been subcontracted to criminal intermediaries, allowing the Kremlin plausible

deniability while maintaining operational reach.⁴⁷ Beyond Europe, Russian **criminal networks form part of a transnational diaspora** that Moscow can tap into for political interference, money laundering, and targeted coercion. Ethnically diverse groups such as the Georgian Kutaisi clan and remnants of the Shulaya crew in the U.S. have reportedly maintained ties to Russian state interests, making them susceptible to pressure or recruitment. Similar tactics have allowed Russia to claim global reach, as evidenced by its presence in Africa and in Latin America, despite significant resources being committed in Ukraine.⁴⁸

Central components of Russia's hybrid warfare strategy also feature **disinformation and propaganda**. As CSD research has illustrated, these disinformation operations are integral to Russia's geopolitical tactics, targeting societal cohesion, democratic institutions, and public opinion, particularly in regions like Eastern Europe and the Black Sea area.⁴⁹ Such propaganda campaigns intensified significantly following Russia's full-scale invasion of Ukraine in 2022, highlighting their strategic importance as tools of hybrid warfare intended to disrupt decision-making and maintain plausible deniability for direct state involvement.

Finally, Russia has increasingly weaponized **migration flows as a tool of destabilization**. By collaborating with people-smuggling networks, Russian authorities have facilitated irregular migration into Finland and other EU border states, deliberately exacerbating domestic tensions within those countries. This tactic mirrors Belarus's strategy during the 2021–2022 border crisis and reflects an emerging pattern of criminalized border warfare.⁵⁰

Iran: The Militia-Criminal Proxy Model

Iran has developed an elaborate, and much better documented in time, model along similar patterns of state-criminal engagement as Russia,

weaponising illicit markets to pursue strategic goals and circumvent global constraints. However, its model also employed some distinctive features, that we suggest understanding as a militia-criminal proxy model, shaped by its revolutionary ideology, geopolitical isolation, and regional ambitions. Rather than fully institutionalizing criminality within state structures, the Iranian state operates primarily through ideologically aligned non-state actors, paramilitary units, and illicit economic networks. As detailed in a 2024 report by the Global Initiative Against Transnational Organized Crime, Tehran has built extensive networks of criminal proxies and state-aligned enterprises to enhance its asymmetric warfare capabilities.⁵¹ Iran's regime relies heavily on such illicit partnerships to carry out assassinations, abductions, cyber-attacks, weapons smuggling, and sanctions evasion.⁵² Many of these activities are outsourced to criminal networks or ideologically aligned non-state actors, affording the state a degree of plausible deniability while advancing its geopolitical interests.

For example, the Islamic Revolutionary Guard Corps (IRGC), particularly its Quds Force, oversees extensive smuggling and arms trafficking operations, often conducted through proxy and partner networks. A specialized IRGC unit, known as Unit 190, has been linked to covert weapons deliveries to Hezbollah and the Houthis.⁵³ These operations typically rely on intermediaries – including shell companies, criminal logistics facilitators, and covert maritime supply chains – allowing Iran to distance itself from direct attribution. Iran's broader strategy to circumvent international sanctions depends on complex oil smuggling networks facilitated by offshore entities, ship-to-ship oil transfers, and fraudulent documentation across jurisdictions including the UAE, Russia, China, and Türkiye.⁵⁴

In addition, Iran has cultivated relationships with transnational criminal enterprises, such as

the so-called Dubai super-cartel, which helped facilitate drug trafficking and money laundering through Europe and the Middle East.⁵⁵ Iran-linked traffickers and militias have also played a key role in the production and smuggling of crystal meth across the Iran-Iraq border, turning drug profits into hard currency as a response to renewed U.S. sanctions.⁵⁶ The report further highlights how Iran leverages Hezbollah's global logistical and financial infrastructure, such as hawala systems, money exchanges, and diamond smuggling, to launder funds and finance terrorism.⁵⁷ Similar patterns have been observed in Syria, particularly during and after the collapse of formal governance structures under Assad, where Iranian-linked actors reportedly used smuggling and illicit trade to consolidate power and secure revenue streams.⁵⁸

Crucially, Moscow and Tehran increasingly collaborate: Russia has imported and locally produced Iranian Shahed (Geran-2/3) drones for its Ukraine war effort, using the same covert finance and logistics systems long perfected by Iran to bypass sanctions.⁵⁹ Analysts note that the Kremlin has studied and adopted Iranian oil-shipping and payment-laundering techniques, establishing joint “sanctions-evasion corridors” that move crude and dual-use goods through the Caspian Sea, Persian Gulf, and International North-South Transport Corridor (INSTC) route.⁶⁰

Iran's cyber strategy similarly blends state power with criminal networks. It operates a decentralized cyber apparatus composed of criminal hackers, hacktivists, and academic contractors, all loosely coordinated by the Ministry of Intelligence or the IRGC.⁶¹ These actors have been implicated in attacks across Europe and North America, including the targeting of NATO allies with significant digital vulnerability, such as Albania in retaliation against support for the exiled Mojahedin-e-Khalq (MEK).⁶² More recently, in May 2024, Sweden's security service reported that the Iranian government

was using criminal networks in Sweden ‘to carry out violent acts against other states, groups and individuals.’⁶³

China: The Corporate-Criminal Hybrid

China, while operating through less overtly criminalized networks and relying on information suppression and strict international image control, has similarly been accused of fusing state strategy with illicit and coercive economic tactics. Chinese state-backed entities have engaged in widespread intellectual property theft and cyber-espionage campaigns targeting Western companies and institutions. These operations often rely on **legitimate private firms or state-affiliated commercial entities** that are covertly instrumentalized by the Chinese state to carry out strategic objectives. This tactic serves to obfuscate the state’s role and complicate attribution, effectively transforming corporate actors into tools of foreign policy.⁶⁴ Although not criminal organizations in the conventional sense, they are used to conduct illicit or coercive activities (e.g., intellectual property theft and cyber-espionage) under the guise of legality, thereby blurring the line between corporate enterprise and statecraft.

One notable recent case involved the 2024 U.S. indictment of Linwei Ding, a Chinese national working at Google, who allegedly stole trade secrets related to artificial intelligence (AI) to benefit Chinese firms and state interests.⁶⁵ In another high-profile example, Chinese telecommunications giant Hytera pleaded guilty in 2025 to conspiring to steal digital mobile radio technology from Motorola Solutions, highlighting long-term efforts to acquire key communications technology through illicit means.⁶⁶ China’s cyber-espionage capabilities have also been linked to coordinated state-backed groups such as APT41 (also known as “Double Dragon”), which has conducted extensive operations against targets in healthcare, telecommunications, and

software industries. APT41 was charged in 2020 by the U.S. Department of Justice for infiltrating over 100 companies worldwide.⁶⁷ Similar investigations, like Operation CuckooBees, revealed that hundreds of gigabytes of sensitive corporate data were exfiltrated – such IP theft campaigns align with Beijing’s industrial policy goals as articulated in *Made in China 2025*.⁶⁸

The Limits of Existing Frameworks: What Have We Missed?

The cases of Russia, Iran, and China underscore a fundamental transformation in contemporary state criminality: a shift from overt acts of violence and political repression to covert, networked, and hybrid forms.⁶⁹ In this new landscape, state crime is characterized by *sophisticated layers of plausible deniability, indirect operational strategies, and instrumental use of non-state actors*. Contemporary state criminality incorporates the strategic deployment of transnational criminal networks, cyber operations, economic manipulation, and disinformation campaigns, all calibrated to serve geopolitical objectives and often under the broader rubric of hybrid warfare. States like Russia have normalized the use of organized criminal networks abroad, cyber criminals, and PMCs to carry out influence operations, espionage, sabotage, and ransomware attacks with minimal direct attribution. These networks are relied upon not only for kinetic operations but also for economic crimes such as sanctions evasion, money laundering and economic coercion.

While classical criminological literature has developed robust frameworks for analyzing state crime, these recent developments expose some of their limitations. Chambliss’ concept of state-organized crime provides perhaps the closest parallel, particularly with his extensive examples of foreign intelligence’s historical utilization of criminal networks, including drug

Table 2. Types of State-Crime Relationships

Dimension	Russia	Iran	China
State-Crime Relationship	Institutionalized symbiosis (state capture): Criminal actors integrated into statecraft and hybrid warfare; strategic co-optation.	Proxy model: Criminal and ideological non-state actors used for deniable asymmetric warfare.	Corporate-state fusion: Legal entities and firms used to carry out illicit state objectives under the guise of legitimacy.
Historical Trajectory	From Soviet-era intelligence collaboration with criminals → post-Soviet criminal state consolidation under Putin.	From revolutionary networks (IRGC) → expanded under sanctions into transnational criminal proxies.	From cyber and economic espionage → institutional embedding of corporate actors in strategic missions.
Key Actors	Wagner Group, vorovskoi mir, cybercriminals (Sandworm, Smokey Spider), shell companies.	IRGC (esp. Quds Force), Unit 190, Hezbollah, regional militias, cyber-hacktivists.	State-owned or affiliated firms (e.g., Hytera), APT groups (APT41), academic and corporate actors.
Use of Illicit Markets	Sanctions evasion, arms and resource smuggling, grey-market logistics, drug trafficking, cybercrime.	Arms trafficking, oil smuggling, crystal meth trade, global hawala networks, Hezbollah financing.	Intellectual property theft, cyber-espionage, illicit tech transfers via front companies.
Cyber Strategy	State-sanctioned cybercrime ecosystem; ransomware, sabotage, surveillance.	Decentralized cyber units under IRGC/Intelligence Ministry; retaliatory attacks, espionage.	Corporate-supported cyber-espionage and data theft with direct industrial goals.
Deniability Strategy	Criminal intermediaries blur attribution; legal impunity in exchange for loyalty.	Outsourcing to ideologically aligned groups for plausible deniability.	Legal firms operate under normal cover; illicit behaviour hidden within formal legality.
Geopolitical Objectives	Undermining Western influence, circumventing sanctions, sustaining the war effort (esp. Ukraine).	Regional influence (Lebanon, Iraq, Yemen), resisting Western sanctions, asymmetric deterrence.	Strategic technological superiority, global economic positioning, long-term industrial policy goals.
Model of Criminality	Militarized-criminal hybrid	Militia-criminal hybrid	Corporate-criminal hybrid
Type of Warfare	Full-spectrum hybrid warfare, including kinetic and non-kinetic operations.	Asymmetric warfare with emphasis on covert and proxy interventions.	Economic and informational warfare embedded in formal systems.

Source: Center for the Study of Democracy (CSD).

traffickers, during the Cold War. Chambliss frames such practices within the context of structural contradictions inherent in capitalist states, whereby states face the inherent tension between maintaining

legitimacy through adherence to laws and morality and pursuing capital accumulation and geopolitical dominance, often by illicit means. Similarly, Green and Ward have demonstrated that powerful

political and economic actors are frequently entangled in, rather than opposed to, organized crime networks.⁷⁰ In popular literature, especially when it comes to Russia's transformation, this is often labelled a "mafia state." However, to classify Russia merely through the lens of organized crime is reductive. What emerges instead is a form of state crime that is more structured, instrumental, and geopolitically strategic. CSD has conceptualized such systemic entanglement under the notion of *state capture*—a process in which private or illicit interests infiltrate, dominate, and repurpose state institutions for their own benefit.⁷¹ In the Russian case, this extends beyond domestic governance: today's use of proxies by states like Russia reflects a deeply institutionalized partnership, in which criminal actors are embedded within broader "statecraft" and hybrid warfare strategies.⁷² This integration positions criminal actors as permanent, instrumental assets within state power rather than occasional disposable tools.

Moreover, as seen in the different cases, states deploy a spectrum of actors – private firms, proxies, cyber groups – to achieve deniable, transnational influence. This assemblage of practice – PMCs (Wagner–Russia), ideological militias (Hezbollah–Iran), and state-owned corporations (Hytera–China) – points to **differentiated forms of state–crime convergence** and to **different diapasons of plausible deniability**. Understanding these convergences also raises institutional questions: **who has or should have the remit to investigate strategic state-sponsored crime? And how?** Traditional criminal justice institutions often lack the mandate or jurisdiction to address crimes perpetrated through or by states. In addition, in most cases, they are greatly outmatched in terms of human and other resources compared to the perpetrator states.

The legalist framework – which defines state crime as the violation of domestic or international law – makes it difficult to use in cases where states

manipulate or circumvent legal mechanisms to shield illicit activity. As Lavorgna has argued, for example, cyber affordances – i.e., the features of digital technologies that enable and constrain actions – have **reshaped the relationship between states and organized crime**.⁷³ While state-organized crime, as described by Chambliss, has historically involved smuggling, political assassinations, espionage, and corruption, cyber affordances provide new opportunities for states to engage in criminal activities with **less accountability and greater anonymity** in ways that **do not clearly violate existing legal statutes, yet produce deep structural harm**. Thus, cyberspace blurs the lines between legality and illegality, making it difficult to categorize certain state cyber activities as crimes under **existing legal frameworks**.

Similarly, Russia's use of shell companies, cryptocurrencies, and sanctions evasion networks illustrates the difficulty of applying legalist frameworks to activities that exploit legal loopholes rather than openly contravene laws. China's state-sponsored cyber-espionage and Iran's illicit arms and oil networks operate in murky transnational zones that are only partially regulated.

These challenges also expose the limitations of the conduct norms approach, which relies on violations of broadly accepted moral standards. In an increasingly multipolar world, where norms themselves are contested, actions such as election interference or information manipulation **lack the universal condemnation** required for this framework to be analytically effective and risk relativism or ineffectiveness. The social harm approach offers a broader lens, expanding the notion of state crime to include legally sanctioned but materially damaging actions. It draws attention to the cumulative and often invisible effects of state policy – structural inequality, economic violence, environmental degradation. However, this approach also struggles with precision and operationalization.

Table 3. Classical approaches to state crime and their limitations

Approach	Key Features	Recognized Crimes	Blind Spots (Challenges in Hybrid Warfare)
Legalistic	Defines state crime as acts violating national or international law.	War crimes, smuggling, piracy, genocide, human rights violations, corruption.	Ignores legal grey zones; struggles with cybercrime, disinformation, and covert operations via proxies.
Conduct Norm	Focuses on violations of widely accepted social norms and human rights.	State repression, political violence, environmental destruction.	Subjective standards; weak enforcement; hard to apply in contested global contexts or to hidden influence tactics.
Social Harm	Expands crime to include state actions causing systemic harm, regardless of legality.	Economic exploitation, austerity, structural violence, corporate-state collusion.	Hard to define and measure harm; lacks clear legal tools; vague on digital harms and financial crimes like sanctions evasion.

Source: Center for the Study of Democracy (CSD).

How can one quantify the long-term harm of digital surveillance, algorithmic manipulation, or financial destabilization via cybercrime? Without clear thresholds or mechanisms for accountability, the social harm perspective may be normatively powerful but analytically diffuse.

These limitations point to the need for a forward-looking transnational, multi-disciplinary approach – one that anticipates the strategic use of legal, technological, and financial infrastructures by states to pursue geopolitical aims through covert or semi-legal means. Ultimately, state crime, particularly when it operates through proxies, corporate channels, or covert alliances, demands analytical frameworks that recognize the very **erosion of traditional analytical boundaries between legal and illegal**, state and criminal, formal and informal.

Addressing this blurred terrain is not just an important conceptual task but a political and institutional imperative for future harm-assessment framework, as used by Europol and academic criminologists, to identify **high-risk criminal**

ecosystems. Such an approach must integrate the use of digital platforms for espionage and manipulation, the financial opacity afforded by cryptocurrencies and offshore banking, and the systematic use of criminal networks as instruments of state policy, and for transnational actors for broader geopolitical goals. Although **contemporary scholarship has not yet developed a consistent and systematic theoretical approach** that integrates all these characteristics of contemporary state criminality, some authors have engaged with different aspects of the problem, proposing new concepts or directions to grasp state criminality's evolving nature.

New Directions to Understanding Strategic State-Sponsored Criminality

Lavorgna advances the concept of *state-cybercrime* which encompasses **illegal or harmful cyber activities conducted for the benefit of a state**.⁷⁴ She emphasizes that while cybercrime has been extensively studied in relation to individual or organizational actors, the intersection of

cyber affordances and state criminality remains underexplored.⁷⁵ Lavorgna proposes a **threefold typology of state-cybercrimes**: cyberattacks (such as hacking and cyberespionage), cybercontrol (including surveillance and censorship), and cyberdeceit (such as disinformation and propaganda). Each of these categories involves distinct actors and mechanisms, often operating in ways that evade clear legal or normative categorization. Crucially, Lavorgna challenges the tendency to subsume state-cybercrime under traditional definitions of state-organized crime. Unlike conventional organized crime, which typically revolves around profit motives and the social embeddedness of non-state actors, state-cybercrime operates in a fluid digital environment with blurred boundaries between state and non-state actors. In many cases, states outsource operations to proxies – such as hacker collectives or private tech firms—while retaining plausible deniability. This ambiguity complicates both attribution and regulation and **highlights the limitations of applying traditional organized crime labels**, which may instead serve to justify expansive surveillance regimes.

While classical scholarship tends to treat organized crime as a profit-seeking, anti-state phenomenon, critical research suggests that many authoritarian governments now **conscript illicit networks into their core state functions**. CSD frames this evolution through its **state-capture model**, which highlights how political elites, oligarchs, and criminal entrepreneurs “lock in” public institutions and regulatory levers to advance both private enrichment and geopolitical strategy.⁷⁶ The *Kremlin Playbook* series deepens this insight by showing how Russia’s intelligence services broker partnerships with private intermediaries and organized-crime groups to evade sanctions, launder capital, and conduct influence operations across Europe and Türkiye.⁷⁷ CSD’s brief on **Illicit**

Financial Flows in the Balkans and the Black Sea estimates that more than USD 30 billion a year now moves through such hybrid channels, sustaining both corruption at home and Kremlin leverage abroad.⁷⁸

These findings dovetail with Galeotti’s analysis of a **hybrid Russian governance model**, where criminal networks operate as extensions of the security apparatus – an arrangement fostered by Western sanctions and diplomatic isolation. Far from operating independently, these networks now function as extensions of the security apparatus. While Russia does not fit neatly into the model of a “mafia state,” the Putin regime has moved toward a hybrid model, where criminal groups are integral to the operational architecture of the state.⁷⁹ This institutionalized criminal nexus reflects the pressures of Western sanctions and diplomatic isolation, which have pushed the Kremlin to rely more heavily on illicit networks for economic and strategic resilience. These developments are not unique to Russia. China’s use of cyber-mercenaries and Iran’s reliance on proxy groups for illicit financing suggest that hybrid state-criminal structures are becoming globally normalized.

One of the most analytically complex challenges is the **intersection between state-sponsored crime and transnational organized crime**. The emerging but still developing concept of “**geocriminality**” offers a lens through which to analyze this transnational entanglement between states and organized crime with a particular focus on geopolitical goals. Geocriminality refers to the **systematic instrumentalization of illicit actors and criminal economies by states as tools for influence beyond their borders**.⁸⁰ Rather than a series of isolated collaborations, this framework captures a strategic and durable alignment between state interests and criminal infrastructures transnationally. From the smuggling corridors of the Caucasus and the Balkans to the dark web marketplaces

and encrypted financial platforms of East Asia, states are increasingly cultivating, managing, and directing criminal networks to project power, bypass sanctions, destabilize rivals, and extract value from global systems. As the concept suggests, criminal actors are geographically positioned, politically activated, and infrastructurally embedded within broader geopolitical strategies. These forms of criminal outsourcing complicate attribution and accountability, especially within a global order defined by technological opacity and fragmented legal regimes.

Harm assessment has also been partially addressed. The main problem in understanding the convergence of covert action, organized crime, and irregular warfare, and therefore developing adequate countering mechanisms, as Magda Long argues, is the **fragmented and compartmentalized nature of existing analytical and institutional frameworks**.⁸¹ Traditional approaches tend to separate **national security, intelligence, law enforcement, and criminology** into distinct domains, making it difficult to grasp how these elements function together in practice. This siloed thinking obscures the ways in which states deliberately blur the lines between legal and illegal, civilian and military, domestic and international, in order to exploit criminal networks for strategic gain. Moreover, the covert and deniable nature of these operations – often hidden behind proxies, front organizations, and plausible deniability – makes it challenging to trace accountability or fully comprehend the scale of state involvement.

Complementing these theoretical contributions, Shima D. Keene introduces the idea of *silent partnerships*, referring to covert and functional alliances between states and organized crime or irregular armed actors.⁸² Far from being symptomatic of state weakness, these partnerships are deliberate arrangements that serve to outsource violence, maintain control over contested spaces,

and evade legal constraints, complicating the traditional understandings of sovereignty and legitimacy. Most importantly, this challenges the conventional state-centric theoretical models of sovereignty and security, advocating for a more nuanced understanding of how power operates in hybrid political orders. In this line of thought, Keene calls for acknowledging the role of non-state actors not just as threats to state authority, but as integral to how many states function and exert control. Her analysis advocates for **a strategic-operational intelligence framework** that integrates social network analysis, financial intelligence, and understanding of relationship dynamics to identify vulnerabilities within these partnerships. This can directly have a reflection in harm-assessment frameworks in policy and academic analysis on contemporary conflict, governance, and global security **that account for the interdependence or “silent partnerships” of state and non-state, legal and illegal spheres.**

Across these contributions, several analytical convergences emerge: 1) the strategic use of proxies to sustain deniability; 2) the embedding of criminal infrastructures within state and corporate operations; and 3) the inadequacy of traditional models to account for hybrid, covert, and transnational modalities of power. What emerges is not a breakdown of state authority, but its mutation – a shift toward decentralized, networked, and deniable forms of coercive influence.

CONCLUSION: AN AGENDA FOR NEW CONCEPTUAL DIRECTIONS

In light of the preceding analysis, it becomes imperative to conceptualize a new framework that captures the specificities of contemporary state criminality as it unfolds within the infrastructure of twenty-first-century hybrid warfare and geopolitical transformation. While numerous concepts have proliferated in recent years, there

is a need to identify the critical dimensions any reconceptualization must encompass to better grasp the evolving entanglements of state and criminality.

At the heart of this revised conceptualization lies a recognition of the **convergence of state, criminal, and corporate actors** within the broader infrastructures of contemporary governance and war. There is a need for a shift in theoretical focus towards the deliberate, coordinated use of criminal practices by states – or with their direct consent, tacit approval, or strategic tolerance – to achieve geopolitical, economic, or security objectives. These practices, tentatively labelled as **strategic state-sponsored criminality** reflect a systemic logic of governance in which criminality is not a corruption of the state, but a corruption for the state – an extension of its strategic capacities. States deploy a variety of actors – militias, cyber proxies, private companies, smugglers, and money launderers – as modular instruments within transnational assemblages of power projection, especially hybrid warfare.

Crucially, such forms of strategic state-sponsored criminality are characterized by *intentionality* and *coordination*. Unlike the “black swan” events often associated with rogue elements or bureaucratic overreach, these practices are not accidental or peripheral, but carefully embedded in state strategies, often operating through *formalized relationships with intermediaries and organized networks*. This coordination can take the form of integrated logistics between state agencies and transnational smuggling rings, shared technological infrastructures between intelligence services and hacker collectives, or sanctioned laundering operations between shell companies and national banks. In each case, the state leverages criminal methods not as a deviation from governance but as an extension of it, operating within a logic of calculated utility. In **the ultimate case of state capture**, these features become embedded in the state governance and function automatically, to ensure

alignment between state and organized crime goals. As *de facto* state capture systems are then touted as models of international development, state capture in other countries becomes a vulnerability through which foreign influence is channeled.

Another defining feature is *instrumentality*. The criminal activities in question are not ends in themselves, as in classical organized crime, where profit is the primary motivator, but are instead means to broader (geo-)political and strategic goals. Whether it is undermining foreign electoral processes through disinformation campaigns, sustaining embargoed war efforts through illicit trade, or extracting advanced technological capabilities through cyber-theft, the criminal acts are subordinated to geopolitical logic. This quality distinguishes strategic state-sponsored criminality from both traditional state repression and criminal enterprises: it is rational, flexible, and goal-oriented, often responding dynamically to shifts in the international system.

Equally important is *transnationality*. These operations are rarely only confined within national borders. In fact, one of their most important aspects, that needs to be considered when thinking about harm-assessment, is that they exploit **the fragmentation of global legal jurisdictions**, the **opacity of financial systems**, and the **decentralized affordances of digital infrastructures**. States operating in this mode intentionally exploit these fault lines: offshoring illicit profits through global shell networks, using foreign-based actors to preserve plausible deniability, or carrying out cyberattacks through layered proxy infrastructures that blur attribution. The international scale of these actions not only complicates accountability but challenges the very foundations of sovereignty, legality, and enforcement upon which conventional criminological frameworks are built.

In this sense, another crucial aspect of strategic state-sponsored criminality is that it allows a certain

level of *plausible deniability*: the ability to project force, disrupt rivals, or bypass sanctions while **preserving a facade of legality or non-involvement**. Whether in the form of Russian cyberattacks conducted by loosely affiliated hacker collectives, Iranian assassinations outsourced to criminal syndicates, or Chinese intellectual property theft carried out via state-affiliated corporate actors, deniability becomes the architecture through which the illicit is operationalized by the state.

This perspective also demands a reconceptualization of the state – not as a bounded legal entity inherently distinct from crime, but as a *networked actor* capable of managing, instrumentalizing, and strategically directing criminal infrastructures to achieve its political and geopolitical objectives. Rather than merely embedding within illicit networks, such states – often authoritarian or semi-authoritarian – use their institutional apparatuses and resources to **exert control over, co-opt, or collaborate with criminal actors**. In this configuration, criminal groups can function as extensions of state security services or proxies in the pursuit of state interests. This is governance not solely through the monopoly of violence, but through the calculated orchestration of criminal economies, often masked by plausible deniability and intermediated by semi-legal or extra-legal actors. It challenges the assumption that criminality necessarily undermines state authority, suggesting instead that certain regimes can consolidate power and enhance their strategic reach precisely by **fusing state governance with illegality**.

Thus, such a conceptual model compels a shift in both criminological and geopolitical analysis. It calls for a cross-disciplinary approach and methodologies that **bridge cyber studies, political economy, international relations, and critical legal studies**. Cyber studies, for instance, can trace the technical infrastructure and digital tools used in state-sanctioned cyber operations.

Political economy helps us follow the financial and logistical chains that enable illicit flows of capital and goods. International relations provide a framework for understanding how these criminal tactics are deployed to project power and destabilize rivals. Critical legal studies can reveal how states manipulate or selectively enforce laws to shield themselves and criminalize others.

Each of these fields offers necessary insights, but only when brought into conversation with one another can we develop a more nuanced understanding of **how modern states govern through crime**. Similarly, such an agenda would also necessitate rethinking investigative and regulatory institutions: the actors best suited to investigate and counteract this phenomenon – intelligence agencies, cyber units, financial regulators, organized crime agencies, and transnational legal bodies – are usually organized vertically and separately, each focused on a more narrowly defined domain or jurisdiction. The challenge, then, is not merely to theorize this form of criminality but to **build new institutional architectures capable of addressing** it with the same level of strategic sophistication.

Ultimately, the challenge ahead is twofold: conceptual and political. Conceptually, we must continue moving towards models that do not assume crime as a deviation from state order and recognize how criminality is being reconstituted as a means of statecraft. Politically, we must confront the implications of a world in which the erosion of legality has become a strategic logic at the heart of certain state regimes. It seems that studying these developments is not anymore only a criminological imperative, but more a **matter of global democratic security**. A future-oriented criminology must therefore be interdisciplinary, institutionally agile, and attuned to the ways in which digital, financial, and logistical infrastructures are reprogrammed by states to serve covert objectives. **PRISM**

Notes

¹ Green, P., and Ward, T., *State Crime: Governments, Violence and Corruption*, London: Pluto Press, 2004.; Rothe, D. L., and Friedrichs, D. O., “The state of the criminology of crimes of the state,” *Social Justice*, 33(1 (103)), 2006, pp. 147–161.

² W. Chambliss. “State-Organized Crime,” *Criminology*, 27(2), 1989, pp. 183–208.; Friedrichs, D. O., *Trusted Criminals*, Boston, MA: Cengage Learning, 2009.; Michalowski, R. J., and Kramer, R. C., *State-Corporate Crime: Wrongdoing at the Intersection of Business and Government*, New Brunswick, NJ: Rutgers University Press, 2006.

³ D. Friedrichs. *Trusted Criminals: White Collar Crime in Contemporary Society*, 4th ed., Belmont, CA: Wadsworth, 2010.

⁴ Council on Foreign Relations, *How Russia's invasion of Ukraine violates international law*, Council on Foreign Relations, 2022.; Conley, H. A. et al., *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe*, Washington, DC: Center for Strategic and International Studies (CSIS), 2016.; Galeotti, M., *Gangsters at War: Russia's Use of Organized Crime as an Instrument of Statecraft*, Global Initiative Against Transnational Organized Crime, 2024.

⁵ M. Vladimirov, et al., *The Kremlin Playbook in Türkiye: Geoeconomics Unfolded*, Sofia: Center for the Study of Democracy, 2025.; Center for the Study of Democracy (CSD), *Illicit Financial Flows and Strategic Corruption*, Policy Brief No. 157, Sofia: CSD, April 2025.; Vladimirov, M., Orejarena, G., and Osipova, D., *Global Reach: The Kremlin Playbook in Latin America*, Sofia: Center for the Study of Democracy, 2024.; Conley et al., *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe*, Washington, DC: CSIS, 2016.; Lavorgna, A., “Unpacking the political-criminal nexus in state-cybercrimes: a macro-level typology,” *Trends in Organized Crime*, 2023, pp. 1–20.

⁶ Europol, *EU Serious and Organised Crime Threat Assessment (SOCTA) 2025: The changing DNA of serious and organised crime*, European Union Agency for Law Enforcement Cooperation, 2025, pp. 14–15.

⁷ D. Rothe, *State Criminality: The Crime of All Crimes*, Lanham, MD: Lexington Books, 2009.

⁸ M. E. Wolfgang, “Pioneers in Criminology: Cesare Lombroso (1825–1909),” *Journal of Criminal Law, Criminology, and Police Science*, Vol. 52, 361, 1961.

⁹ M. E. Wolfgang, “Pioneers in Criminology: Cesare Lombroso (1825–1909),” *Journal of Criminal Law, Criminology, and Police Science*, Vol. 52, 361, 1961.

¹⁰ Michalowski, and Kramer (eds.), *State-Corporate Crime*, New Brunswick, NJ: Rutgers University Press, 2006.

¹¹ Center for the Study of Democracy (CSD) , *State Capture Unplugged: Countering administrative and political corruption in Bulgaria*, Sofia: CSD, 2016.

¹² E. Sutherland, “White Collar Crime”, *Social Forces*, Vol. 28, Issue 2, NY: Dryden Press, December 1949, pp. 215–216.

¹³ Friedrichs, *Trusted Criminals*, 4th ed., Belmont, CA: Wadsworth, 2010, p. 73.

¹⁴ Quinney, R., *Class, State and Crime: On the Theory and Practice of Criminal Justice*, New York: David McKay, 1977.; Chambliss, W., and Seidman, R., *Law, Order, Power*, Boston: Addison-Wesley, 1971.; Michalowski, R., *Order, Law and Crime*, New York: Random House, 1985.

¹⁵ M. Foucault, *Discipline and Punish: The Birth of the Prison*, 2nd ed., translated by A. Sheridan, New York: Vintage Books, 1995 (original work published 1975).

¹⁶ W. Chambliss, “State-Organized Crime”, *Criminology*, 27(2), 1989, pp. 183–208.

¹⁷ R. Michalowski, “In search of ‘state and crime’ in state crime studies,” In *State Crime in the Global Age*, Cullompton: Willan, 2013, pp. 13–30.

¹⁸ Chambliss, “State-Organized Crime”, *Criminology*, 27(2), 1989, pp. 183–208.

¹⁹ W. Chambliss, “Commentary by William Chambliss,” *Society of Social Problems Newsletter*, 26 (2), 1995.

²⁰ Michalowski, “In search of ‘state and crime’ in state crime studies,” In *State Crime in the Global Age*, Cullompton: Willan, 2013, p.18.

²¹ Green, and Ward, *State Crime: Governments, Violence and Corruption*, London: Pluto Press, 2004.

²² Rothe, *State Criminality: The Crime of All Crimes*, Lanham, MD: Lexington Books, 2009.; Friedrichs, *Trusted Criminals*, 4th ed., Belmont, CA: Wadsworth, 2010.

²³ Friedrichs, D., and J. Friedrichs, “The World Bank and Crimes of Globalization: A Case Study”, *Social Justice*, Vol. 29, 2002, pp. 13–36.; Harvey, D., *The New Imperialism*, New York: Oxford University Press, 2003.

²⁴ Michalowski, *Order, Law and Crime*, NY: Random House, 1985.

²⁵ Michalowski, *Order, Law and Crime*, NY: Random House, 1985.; Hillyard, P. et al.(eds.), *Beyond Criminology: Taking Harm Seriously*, London: Pluto Press, 2004.

²⁶ Michalowski, and Kramer, *State-Corporate Crime*, New Brunswick, NJ: Rutgers University Press, 2006.

- ²⁷ S. Tombs, “State-Corporate Symbiosis in the Production of Crime and Harm,” *State Crime Journal*, Vol. 1(2), 2012, pp. 170–195.; Lynch, M. J., Fegadel, A., and Long, M. A., “Green Criminology and State-Corporate Crime: The Ecocide-Genocide Nexus with Examples from Nigeria,” In *The Genocide-Ecocide Nexus*, London: Routledge, 2022, pp. 81–101.
- ²⁸ F. G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Arlington, VA: Potomac Institute for Policy Studies, 2007.; North Atlantic Treaty Organization (NATO), *Countering hybrid threats*, NATO, 2024.
- ²⁹ W. A. Qureshi, “The Rise of Hybrid Warfare,” *Notre Dame Journal of International & Comparative Law*, Vol. 10, Iss. 2, Art. 5, 2020.
- ³⁰ See for example: Conley et al., *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe*, Washington, DC: CSIS, 2016; Lavorgna, A., “Unpacking the political-criminal nexus in state-cybercrimes: a macro-level typology,” *Trends in Organized Crime*, 2023, pp. 1–20; Mailey, J. R., *Iran’s criminal statecraft: How Tehran weaponizes illicit markets*, Global Initiative Against Transnational Organized Crime, 2024; Galeotti, *Gangsters at War*, Geneva: GI-TOC, 2024.
- ³¹ Galeotti, *Gangsters at War*, Geneva: GI-TOC, 2024
- ³² Conley et al., *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe*, Washington, DC: CSIS, 2016.; Conley, H. A. et al., *The Kremlin Playbook 2: The Enablers*, Washington, DC: Center for the Study of Democracy (CSD) and Center for Strategic and International Studies (CSIS), 2019.; Vladimirov, Orejarena, and Osipova, *Global Reach: The Kremlin Playbook in Latin America*, Sofia: CSD, 2024; Vladimirov et al., *The Kremlin Playbook in Türkiye*, Sofia: CSD, 2025.
- ³³ Center for the Study of Democracy, *State Capture Unplugged*, Sofia: CSD, 2016.
- ³⁴ Galeotti, *Gangsters at War*, Geneva: GI-TOC, 2024.
- ³⁵ McLaren, R., Clemente Fito, E., and A. Rusev, *Shadow Fusions: The Convergence of Criminal Networks and the Russian State*, Sofia: Center for the Study of Democracy, 2025.
- ³⁶ Galeotti, *Gangsters at War*, Geneva: GI-TOC, 2024, pp. 6-8.
- ³⁷ Center for the Study of Democracy, *Illicit Financial Flows and Strategic Corruption*, Policy Brief No. 157, Sofia: CSD, April 2025.; Vladimirov et al., *The Kremlin Playbook in Türkiye*, Sofia: CSD, 2025.
- ³⁸ U.S. Department of the Treasury, *Treasury Sanctions Russian Proxy Wagner Group as a Transnational Criminal Organization*, 2023.
- ³⁹ M. Oliver, “Russia Suspected of Smuggling EU Fridges to Strip for Weapon Parts,” *The Times*, 7 November 2022.; James, B., et al., *Silicon Lifeline: Western Electronics at the Heart of Russia’s War Machine*, London: RUSI, 2022.; Vladimirov, Orejarena, and Osipova, *Global Reach: The Kremlin Playbook in Latin America*, Sofia: CSD, 2024; Vladimirov et al., *The Kremlin Playbook in Türkiye*, Sofia: CSD, 2025.; Center for the Study of Democracy, *State Capture Unplugged*, Sofia: CSD, 2016.
- ⁴⁰ Bilousova, O., et al., *Challenges of Export Controls Enforcement: How Russia Continues to Import Components for Its Military Production*, Yermak-McFaul International Working Group on Russia, 2024.
- ⁴¹ Center for the Study of Democracy, *State Capture Unplugged*, Sofia: CSD, 2016.; Conley et al., *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe*, Washington, DC: CSIS, 2016.; Galeotti, *Gangsters at War*, Geneva: GI-TOC, 2024, p. 8, pp. 20-22, p.43.
- ⁴² FinCEN, “FinCEN Identifies Virtual Currency Exchange Bitzlato as a “Primary Money Laundering Concern” in Connection with Russian Illicit Finance,” 18 January 2023.
- ⁴³ Vladimirov, Orejarena, and Osipova, *Global Reach: The Kremlin Playbook in Latin America*, Sofia: CSD, 2024; Vladimirov et al., *The Kremlin Playbook in Türkiye*, Sofia: CSD, 2025.
- ⁴⁴ Galeotti, *Gangsters at War*, Geneva: GI-TOC, 2024, pp. 25-27.; Lella, I. et al. (eds.), *ENISA Threat Landscape 2023*, ENISA, 2023.
- ⁴⁵ Lella, I. et al. (eds.), *ENISA Threat Landscape 2023*, ENISA, 2023.
- ⁴⁶ National Cyber Security Centre, *Ransomware, extortion and the cyber crime ecosystem*, NCSC and NCA, 11 September 2023.
- ⁴⁷ Galeotti, *Gangsters at War*, Geneva: GI-TOC, 2024, p. 15.
- ⁴⁸ Vladimirov, Orejarena, and Osipova, *Global Reach: The Kremlin Playbook in Latin America*, Sofia: CSD, 2024.
- ⁴⁹ Novosiolova, T., and G. Georgiev, *Countering hybrid warfare in the Black Sea region: Strengthening Institutional Frameworks for Protection and Resilience*, Sofia: Center for the Study of Democracy (CSD), 2024.
- ⁵⁰ K. M. Greenhill, “When Migrants Become Weapons: The Long History and Worrying Future of a Coercive Tactic,” *Foreign Affairs*, March/April 2022. (Accessible via MIT Center for International Studies)
- ⁵¹ Mailey, *Iran’s criminal statecraft: How Tehran weaponizes illicit markets*, GI-TOC, 2024.
- ⁵² Mailey, *Iran’s criminal statecraft: How Tehran weaponizes illicit markets*, GI-TOC, 2024, pp. 1-2, pp. 4-8.

⁵³ While Hezbollah is a major political party in Lebanon and has been described by some scholars and supporters as a resistance movement, it is also officially designated—either in whole or in part—as a terrorist organization by at least 26 countries as of October 2020, including the U.S., the EU, and most Western states. This contested status underscores Hezbollah’s hybrid nature: it operates simultaneously as a state-aligned proxy, a political actor with institutional power, and a non-state entity engaged in organized crime and transnational violence. Additionally, the U.S. relisted the Iranian-backed Houthis as a foreign terrorist organization (FTO) in March 2025.

⁵⁴ Mailey, *Iran’s criminal statecraft: How Tehran weaponizes illicit markets*, GI-TOC, 2024, pp. 6-7.

⁵⁵ Mailey, *Iran’s criminal statecraft: How Tehran weaponizes illicit markets*, GI-TOC, 2024, p. 9, p. 14.

⁵⁶ Mailey, *Iran’s criminal statecraft: How Tehran weaponizes illicit markets*, GI-TOC, 2024, pp. 20-21.

⁵⁷ Mailey, *Iran’s criminal statecraft: How Tehran weaponizes illicit markets*, GI-TOC, 2024, p. 7, pp. 12-14.

⁵⁸ Morris, L., and Mekhennet, S., *Syria seeks to sever last Iran-linked networks for smuggling arms and cash*, Washington Post, 12 April 2025.

^{59W} Reinsch, “The Story of Sanctions,” CSIS, 17 March 2025.

⁶⁰ United Against Nuclear Iran, *Tehran’s Ties with Beijing and Moscow*, NY: United Against Nuclear Iran, 2023.

⁶¹ Mailey, *Iran’s criminal statecraft: How Tehran weaponizes illicit markets*, GI-TOC, 2024, pp. 9-11.

⁶² Mailey, *Iran’s criminal statecraft: How Tehran weaponizes illicit markets*, GI-TOC, 2024, p. 4.

⁶³ Swedish Security Service, “Iran is using criminal networks in Sweden,” Säkerhetspolisen, 30 May 2024.

⁶⁴ F. Nabeel, “The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age,” *Journal of Contemporary Studies*, vol. VII, no. 1, 2018, pp. 94–96.; Clarke, R. A., and Knake, R. K., *Cyber War: The Next Threat to National Security and What to Do About It*, New York: Ecco, 2010.

⁶⁵ U.S. Department of Justice, “Chinese National Residing in California Arrested for Theft of Artificial Intelligence-Related Trade Secrets from Google,” 6 March 2024.

⁶⁶ U.S. Attorney’s Office, Northern District of Illinois, “Chinese Telecommunications Company Pleads Guilty to Conspiring to Steal Technology from Illinois-Based Motorola Solutions,” 14 January 2025.

⁶⁷ C. Cimpanu, “US charges five hackers part of Chinese state-sponsored group APT41,” *ZDNet*, 16 September 2020.

^{68B} Jensen, “How the Chinese Communist Party Uses Cyber-Espionage to Undermine the American Economy,” CSIS, 19 October 2023.

⁶⁹ Conley et al., *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe*, Washington, DC: CSIS, 2016.; Conley, H. A. et al., *The Kremlin Playbook 2: The Enablers*, Washington, DC: CSIS, 2019.

⁷⁰ Green, and Ward, *State Crime: Governments, Violence and Corruption*, London: Pluto Press, 2004.

⁷¹ Center for the Study of Democracy, *State Capture Unplugged*, Sofia: CSD, 2016.

⁷² Galeotti, *Gangsters at War*, Geneva: GI-TOC, 2024.

⁷³ A. Lavorgna, “Unpacking the PoliticalCriminal Nexus in StateCybercrimes: A MacroLevel Typology,” *Trends in Organized Crime*, 2023.

⁷⁴ Lavorgna, *Unpacking the PoliticalCriminal Nexus in StateCybercrimes: A MacroLevel Typology, Trends in Organized Crime*, 2023.

⁷⁵ Rusev, A., and T. Comunale, *Cybercrime and Businesses: A closer look at reporting behaviour, associated costs and incident management in Bulgaria, the Netherlands and Spain*, Sofia: Center for the Study of Democracy (CSD), 2023.

⁷⁶ Center for the Study of Democracy, *State Capture Unplugged*, Sofia: CSD, 2016.; Stoyanov, A., Gerganov, A., and Yalamov, T., *State Capture Assessment Diagnostics*, Sofia: Center for the Study of Democracy, 2019.

⁷⁷ Vladimirov et al., *The Kremlin Playbook in Türkiye*, Sofia: CSD, 2025.

⁷⁸ Center for the Study of Democracy, *Illicit Financial Flows and Strategic Corruption*, Policy Brief No. 157, Sofia: CSD, April 2025.

⁷⁹ Galeotti, *Gangsters at War*, Geneva: GI-TOC, 2024.; Varese, F., “Is Sicily the Future of Russia? Private Protection and the Rise of the Russian Mafia,” *European Journal of Sociology / Archives Européennes de Sociologie*, 35(2), 1994, pp. 224–258.

⁸⁰ Global Initiative Against Transnational Organized Crime, *Geocriminality*, Geneva: GI-TOC, 2024.

⁸¹ Magda Long, “Shadows of Power Beneath the Threshold: Where Covert Action, Organized Crime and Irregular Warfare Converge,” *Intelligence and National Security*, 40(1), 87–113, 2025.

⁸² S. Keene, *Silent Partners: Organized Crime, Irregular Groups, and NationStates*, Carlisle, PA: U.S. Army War College Press, Strategic Studies Institute, 2018.

Agriculture as a Domain of Hybrid Warfare

China's Strategy and U.S. Security Gaps

Dr. Alicia Ellis and Sarah Shoer

Hybrid warfare has become a defining feature of 21st-century strategic competition, pushing conflict into the gray zone below open war.¹ The North Atlantic Treaty Organization (NATO) and the U.S. Department of War (DoW) recognize its potency, and the People's Republic of China (PRC) operationalizes it through the “Three Warfares” doctrine, merging cyber, economic, legal, and information tools across multiple domains.² Yet agriculture remains virtually absent from U.S. hybrid threat assessments, despite serving as a foundational pillar of economic stability and public legitimacy. While analysts have examined vulnerabilities in energy, finance, and telecom, agriculture is largely relegated to the margins, framed in terms of public health or market dynamics rather than national security.

This neglect comes at a cost. From Cold War grain diplomacy to Russia's 2022 fertilizer embargo, agriculture has long been deployed as an instrument of coercion. Today, the PRC is quietly building upstream influence through land acquisition, systemic agricultural technology (agtech) ownership, and control over crop inputs, creating chokepoints that could be weaponized under crisis. To address this, we propose the Agriculture Security (AgSec) framework, which elevates agriculture to the policy space presently occupied by cyber and energy security. This review synthesizes evidence of U.S. vulnerabilities and PRC strategies and

Dr. Alicia Ellis is an IWC Researcher, an Assistant Teaching Professor, and Director of the M.A. in Global Security program at Arizona State University (ASU). A former Air Force officer with deployments in support of Operation Enduring Freedom and Operation Iraqi Freedom, she also served as a Presidential Management Fellow (PMF) at the Departments of Treasury and State. Her research focuses on the role of agriculture in competitive statecraft and supply chain security. Dr. Ellis holds a PhD from Arizona State University.

Sarah Shoer is an IWC Researcher, a Program Manager at ASU's Office of University Affairs, and the Managing Editor of *Inter Populum: The Journal of Irregular Warfare and Special Operations*. Before joining ASU, she held public diplomacy roles at several embassies in Washington, D.C. She holds a Master's degree in Global Security from ASU, where her research on the Wagner Group was published in *Inter Populum*, and a Bachelor's degree from Colby College.

offers practical policy and research approaches to integrate agriculture into national hybrid-warfare doctrine and allied deterrence planning.

AGRICULTURE AS CRITICAL INFRASTRUCTURE

Understanding agriculture as critical infrastructure begins with recognizing its centrality to both U.S. economic power and global stability. As the world's leading agricultural exporter by total value in 2023, the United States accounted for roughly 31% of all global corn exports, 35% of soybeans, and 15% of wheat, supplying major food-importing nations across Asia, Europe, and Africa.³ Corn and soybeans are especially significant, as they underpin global livestock feed and food processing industries. Recognizing this, the Department of Homeland Security (DHS) designates agriculture as one of sixteen critical infrastructure sectors.⁴ Yet, this recognition has not translated into operational planning: agriculture remains largely absent from integrated threat assessments, even as the system grows more digitized, globalized, and vulnerable to coercion.

Modern U.S. agriculture operates on a just-in-time model that prioritizes efficiency but leaves little margin for disruption.⁵ Precision farming technologies, automated irrigation systems, commodity logistics, and processing all depend on seamless access to critical inputs and continuous data flows.⁶ DHS' 2021 *Threats to Food and Agriculture Resources* (TFAR) report warned that this efficiency introduces compounding vulnerabilities, especially when interdependencies with energy, water, transportation, and cyber systems are not fully mapped or protected.⁷ Recent crises validated this concern: during the COVID-19 pandemic and the 2022 global shipping bottlenecks, even short-term delays in receiving key parts or fertilizers led to planting setbacks and price spikes.⁸ A 2023 industry survey by Willis Towers Watson found that 73% of food and

agriculture companies reported higher-than-expected supply chain losses over the prior two years, citing the pandemic, war in Ukraine, and export controls as factors.⁹ A 2021 MITRE network analysis further underscored fragility: the disruption of just five major U.S. meat processing facilities could trigger nationwide failures, undermining not only the economy but also social trust in government responses.¹⁰

The war in Ukraine highlighted the global cascading effects of disruptions to agricultural inputs. Russia's temporary fertilizer export bans, combined with its cutoff of natural gas to Europe, curtailed the production of ammonia, a key ingredient in manufacturing nitrogen fertilizers. Although the United States produces a significant share of its nitrogen-based fertilizers, imports still account for nearly 20% of total fertilizer use.¹¹ The sudden shortfall in 2022 rocked global markets and left farmers in the U.S. Southwest unable to secure fertilizer during a critical planting window. Producers were forced either to delay planting—absorbing soaring costs and yield losses—or not plant at all. By March 2022, prices for anhydrous ammonia, urea, and nitrogen solutions spiked up to 184% over the prior year.¹² While markets later corrected, three problems remain: agriculture cannot absorb delays without yield loss, sanction exemptions on Russian fertilizer continue to channel export revenue into Moscow's war economy, and the episode exposed a structural vulnerability nested deep in U.S. agrifood systems.¹³

Vulnerability is magnified by foreign dominance of agricultural inputs. Russia, Belarus, and China lead in synthetic fertilizers, particularly phosphates and potash.¹⁴ Beijing has repeatedly restricted exports, most recently in 2021 and 2024, framing the measures as domestic stabilization but effectively tightening global supply.¹⁵ At the same time, China has actively worked to reduce its reliance on U.S. agricultural exports by diversifying sources of food imports by ramping up purchases from Brazil and

Argentina and investing in South American logistics and production infrastructure.¹⁶

This dual approach (tightening global supply while diversifying its own) allows China to absorb shocks while competitors face volatility, reinforcing its leverage over supply chains. This strategy reflects a broader pattern in the PRC's hybrid strategy: measures that can be justified as domestic policy but also serve as tools of influence in the international system. Recognizing fertilizer's value as both a commodity and a coercive tool, the PRC has steadily expanded its global footprint in fertilizer production, warehousing, and logistics infrastructure through its Belt and Road Initiative (BRI).¹⁷ These projects embed Chinese state-linked firms into the supply chains of critical agricultural inputs across Africa, South Asia, and the Middle East, creating future chokepoints that can be leveraged in times of geopolitical tension. Russia, too, has pursued fertilizer dominance, using military force to control Syria's phosphate mines and extend influence over European markets.¹⁸

Beyond traditional fertilizers and chemicals, U.S. agriculture increasingly depends on precision technologies. GPS-guided tractors, drone-enabled crop monitoring, and AI-based yield forecasting rely on semiconductors, sensors, and software systems sourced largely from East Asia, leaving them susceptible to disruption or surveillance. Yet this digitization has outpaced investment in cybersecurity, leaving the sector "behind the curve" compared to other critical infrastructure sectors due to a focus on safety and efficiency rather than threat mitigation.¹⁹ Many farms and agribusinesses have minimal cyber protections, making them vulnerable to ransomware, data theft, or service interruptions.²⁰ At DEF CON 29 in 2021, researchers exposed software flaws in John Deere and Case IH equipment that allowed remote manipulation of GPS-guided tractors and harvesters.²¹ In April 2022, the FBI warned that ransomware actors were increasingly likely to

strike agricultural cooperatives during planting and harvest seasons, a risk starkly illustrated by recent cyberattacks on food processing firms.²²

THE PRC'S HYBRID STRATEGY AGAINST U.S. AGRICULTURE

Adversarial espionage, theft, and sabotage against the U.S. agriculture sector are often framed as commercially motivated or as acts of geoeconomic competition. Yet the pattern of target selection suggests something more strategic: adversaries are mapping and probing points of systemic vulnerability that could be exploited in crisis. Among them, the PRC stands out for adopting a hybrid warfare posture toward agriculture, using legal, economic, cyber, and biotechnological tools to operate below the threshold of armed conflict. Its systematic focus on upstream assets, such as seed genetics, fertilizer production, and agricultural technology platforms, reflects a deliberate strategy to embed influence at the foundation of food production. This pattern reveals not only recognition of agriculture's strategic value but also a growing willingness to hold food systems at risk in future geopolitical disputes.

Foreign Ownership & Infrastructure Access

Chinese entities have significantly expanded their footprint in the U.S. agricultural sector through land acquisitions, corporate takeovers, and infrastructure investments. At its peak in 2021, Chinese investors had control of approximately 384,000 acres of U.S. farmland, a dramatic increase from just 13,720 acres in 2010.²³ Chinese acquisitions are set apart by their proximity to critical infrastructure and opaque ownership structures, which often evade federal oversight under current U.S. reporting laws.²⁴ In 2021, the Fufeng Group, a Chinese fermentation company, purchased 370 acres near Grand Forks Air Force Base in North Dakota, a major site for U.S. intelligence, surveillance, and

reconnaissance (ISR) operations. Though marketed as a corn mill project, the facility's proximity to the base sounded alarm bells across the national security community. In 2023, the U.S. Air Force formally concluded that the project posed a "significant threat to national security," which led the city to terminate the development agreement.²⁵ In 2021, Chinese businessman Sun Guangxin acquired about 130,000 acres of ranch land in Val Verde County, Texas, near Laughlin Air Force Base, with plans to build the Blue Hills wind farm project.²⁶ U.S. officials grew alarmed that the turbines and grid access could allow for interference or spying on Air Force training flights, and Texas eventually responded by passing a 2021 law barring adversary states from critical infrastructure projects, which effectively blocked the wind farm.²⁷

Beyond U.S. borders, China's approach to land acquisition reflects deeper concerns about its long-term food and water security. Faced with limited arable land, rapid urbanization, and worsening water scarcity, Beijing has increasingly looked abroad to secure the agricultural resources it needs. These global land deals serve as a form of strategic insurance. According to a 2022 report by the U.S.-China Economic and Security Review Commission, this model enables China to "own" production capacity rather than depend on trade, a strategy that favors control over interdependence.²⁸ While this may enhance China's long-term food resilience, it also raises serious concerns for host nations. When foreign powers control local farmland and water resources, communities risk losing decision-making power over their own food systems, potentially making them dependent on external actors for basic sustenance.

Chinese corporate acquisitions also have strategic implications, particularly when they intersect with core components of the U.S. food supply chain. In 2013, China's WH Group acquired Smithfield Foods for \$4.7 billion (\$7.1 billion, including

assumed debt), transferring 146,000 acres of U.S. farmland and full ownership of a vertically integrated company—one that controls approximately one quarter of U.S. hog production, processing, packaging, and distribution.²⁹ This gave the PRC direct access to every stage of the American pork supply chain. While this type of consolidation mirrors trends seen in large U.S. firms like Kroger and Tyson, the implications of foreign ownership are distinct. Following the acquisition, Smithfield cancelled contracts with American grain cooperatives and began sourcing corn directly from U.S. farmers, reducing reliance on domestic intermediaries and reshaping operations to better serve China's food security priorities.³⁰

During China's African Swine Fever crisis from 2018 to 2020, the country experienced a significant loss in pork production, estimated at 27.9 million metric tons. This shortfall led to a surge in pork imports, with the United States (notably, Smithfield) exporting record volumes of pork to China and essentially providing Beijing with food security insurance.³¹ Simultaneously, the COVID-19 pandemic caused disruptions in U.S. meat processing plants, leading to domestic meat shortages and empty grocery store shelves at home. In April 2020, the U.S. exported a record 129,000 tons of pork to China, even as U.S. consumers faced supply shortages.³² This exposed a serious bottleneck at a critical stage of production, but more importantly, how easily control over essential food supply chains can be transferred.

In 2024, the China Oil and Foodstuffs Corporation (COFCO), a Chinese state-owned food processing holding company and the PRC's largest food processor, manufacturer, and trader, acquired majority ownership of a major grain terminal in Cahokia, Illinois. The terminal's location along the Mississippi River and its capacity to move massive quantities of grain make it a critical chokepoint in U.S. grain exports.³³ This provides the PRC with

potential insight into commodity flows and pricing, and, in crisis scenarios, the means to disrupt logistics in ways that benefit foreign supply chains. The U.S.-China Economic and Security Review Commission warned that Chinese ownership or control of port infrastructure may allow the Chinese government to “monitor or manipulate critical export routes,” posing risks to U.S. domestic logistics and global trade flows.³⁴

Control over upstream agricultural inputs, such as seed genetics, agrichemicals, and biotech, is critical because these components shape the productivity and resilience of the entire food system. Innovations in genetically modified (GM) seeds, crop protection technologies, and precision farming tools not only affect crop yields and input costs but also what is grown, how it’s grown, and who benefits from it. As a result, influence over upstream inputs has a ripple effect throughout the food supply system. In 2017, ChemChina, a Chinese state-owned enterprise, acquired Syngenta for \$43 billion, bringing one of the world’s largest agrochemical and seed companies under Beijing’s influence. Though headquartered in Switzerland, Syngenta’s sprawling U.S. operations, including biotech R&D, seed production, and chemical manufacturing, now operate under a Chinese state-owned umbrella.³⁵ Economically, this gives China access to proprietary U.S. agricultural technology, including GM seed traits and crop protection systems that are essential to U.S. food production and export competitiveness. Strategically, it raises concerns about supply chain integrity, intellectual property (IP) security, and long-term control over foundational inputs in U.S. agriculture. If geopolitical tensions escalate, upstream leverage over seeds and agrochemicals could become a chokepoint, impacting domestic crop production and food system resilience.

National security experts warn that these types of acquisitions enable quiet consolidation of influence through legal means. The U.S.-China

Economic and Security Review Commission notes that current oversight mechanisms, like the Agricultural Foreign Investment Disclosure Act (AFIDA), are outdated and lack enforcement mechanisms.³⁶ There is no requirement to identify controlling interests hidden behind shell corporations or monitor how land is used post-acquisition.³⁷ This creates significant blind spots that adversaries could exploit for long-term strategic positioning.

Supply Chain Leverage and Input Dependency

The U.S. agriculture sector relies on key foreign-manufactured inputs, including fertilizers, pesticides, seeds, and machinery, much of which comes from the PRC. China dominates global fertilizer production, especially phosphates and nitrogen. In July 2021, facing rising domestic prices and potential shortages, Beijing imposed an export ban on phosphate fertilizers to secure domestic supply. This restriction, lasting into mid-2022, dramatically reduced global phosphate availability and contributed to record-high fertilizer prices worldwide.³⁸ Again in 2024, China’s Ministry of Commerce restricted fertilizer exports under the guise of domestic stabilization, but the timing raised questions over whether input dependencies could be leveraged during geopolitical disputes.³⁹

China also has overwhelming dominance in herbicides and fungicides, namely glyphosate, the world’s most widely used herbicide. In 2024, an estimated 99% of glyphosate used in the United States was sourced from China, despite limited domestic production.⁴⁰ Beijing is also a major supplier of other pesticide active ingredients (AIs) such as paraquat, atrazine intermediates, and pyrethroids, which are vital for weed control in crops like corn and soybeans. Chinese suppliers furnished 100% of U.S. atrazine and 85% of glufosinate imports in 2024. In aggregate, China supplied more than half of all herbicide AIs globally, underscoring how the U.S. is

tied to Chinese upstream inputs at multiple points of production.⁴¹

China is likewise a pivotal producer of urea, the most widely used nitrogen fertilizer. Synthesized from ammonia and carbon dioxide, urea is central to yields in corn, wheat, and other staples, and China accounts for roughly one-third of global output.⁴² Because nitrogen is the primary yield driver in most row crops, shocks to urea supply or price transmit quickly to planting decisions, farm margins, and downstream food prices. Although the United States sources most of its urea from Canada, Qatar, Algeria, Russia, and Saudi Arabia, Chinese export decisions ripple through global markets. When Beijing restricted urea exports in 2021, prices surged worldwide; across restrictions eased in mid-2025, Chinese urea exports spiked more than 600 percent year-over-year, once again reshaping availability and costs. Even without direct reliance, U.S. producers face higher fertilizer costs whenever China tightens or loosens supply, proving Beijing's role as a global price-setter.

Beyond fertilizers and chemicals, U.S. agriculture increasingly depends on precision technologies. GPS-guided tractors, drone-enabled crop monitoring, and AI-based yield forecasting rely on semiconductors, sensors, and circuit boards sourced largely from East Asia, including China. This reliance introduces significant vulnerabilities. Disruptions from cyberattacks, geopolitical tensions, export restrictions, or supply chain sabotage can ripple across planting and harvest cycles. Even minor delays in equipment parts can compromise narrow planting windows, reduce yields, and impact logistics. With agriculture's tight seasonal schedules, these chokepoints can be exploited in a crisis, essentially turning technological interdependence into a strategic liability with consequences for food security and market stability.

Market Manipulation and Economic Coercion

The PRC also leverages demand-side market power in agricultural trade. China is consistently the largest buyer of U.S. soybeans and corn; during the U.S.-China trade war (2018-2019), Beijing's withdrawal from U.S. purchases crashed prices and targeted politically sensitive farm states to pressure U.S. policymakers.⁴³ Although subsidies and alternative markets blunted some damage, the episode exposed a structural vulnerability in U.S. agriculture: overdependence on specific foreign buyers can be exploited for geopolitical leverage. While this is the flip side of supply-chain control, it shows that China can use its market power in agricultural trade as leverage. Experts have warned that increased Chinese ownership across the U.S. food supply chain could give Beijing "undue leverage," enabling it to distort markets or pressure U.S. suppliers by favoring Chinese-owned intermediaries.⁴⁴

Cyberattacks and Digital Espionage

Many agtech platforms operate in regulatory gray zones, where commercially available tools, such as AI-powered yield models, can be repurposed to surveil or manipulate U.S. agricultural outputs. The dominance of Chinese agtech firms in the U.S. drone market introduces additional risk. Chinese companies such as DJI and XAG now provide around 70% of agricultural unmanned aerial vehicles (UAVs) used in crop spraying, field surveillance, and data collection across American farmlands.⁴⁵ These drones are often connected via cloud infrastructure and managed remotely, which poses data integrity, espionage, and firmware manipulation risks.⁴⁶ Knowledge of U.S. crop yields and locations could for example allow the PRC to target U.S. food production in a conflict through cyberattacks on precision ag systems or by sabotaging seed and chemical supply to specific regions.

However, despite mounting concerns, U.S. regulatory frameworks remain fragmented, and there is no requirement to ensure data generated by agricultural drones is stored securely or redomestically. In 2024, the Cybersecurity and Infrastructure Security Agency (CISA) blacklisted DJI drones due to national security risks and issued guidance warning that “foreign-manufactured UAS pose serious threats to critical infrastructure sectors, including food and agriculture.”⁴⁷

There have been several recorded instances of major PRC-linked cyberattacks on U.S. agriculture firms. In 2015-2016, Chinese cyber actors associated with the firm Boyusec (APT3) breached Trimble Inc., a U.S. company known for its GPS technologies widely used in precision agriculture. The hackers exfiltrated proprietary designs and positioning data for advanced farming applications.⁴⁸ In 2022, the Chinese-linked group APT41 orchestrated one of the clearest known examples of a state-linked cyber attack targeting U.S. agricultural systems. By exploiting a zero-day vulnerability in USAHerds, a software platform used by more than a dozen U.S. states for managing livestock health, tracking disease outbreaks, and coordinating biosecurity responses, APT41 showed that agriculture-specific systems are not outside the scope of cyber targets.⁴⁹ The breach provided access to sensitive information on animal populations, movement patterns, and outbreak response infrastructure.

Intellectual Property (IP) Theft and Research & Development (R&D) Sabotage

Chinese actors have repeatedly targeted U.S. agricultural research and development (R&D) in a strategic effort to acquire high-value IP, especially in the areas of GM seed technology and precision agriculture software. In 2016, Robert Mo (legal name: Mo Hailong), Director of International Business for the Beijing Dabeinong Technology Group (DBN Group), a Chinese agricultural

conglomerate, targeted multiple test fields across Iowa and Illinois and attempted to smuggle elite inbred seeds to reverse-engineer hybrid corn lines in China.⁵⁰ A less publicized but equally significant case involved Weiqiang Zhang, a rice breeder at Ventria Bioscience, convicted in 2018 in Kansas for stealing hundreds of genetically modified rice seeds engineered for pharmaceutical applications. Zhang, who conspired with a Chinese crop research institute, was later intercepted by U.S. customs.⁵¹ In 2022, in another high-profile case, Xiang Haitao pleaded guilty to stealing a proprietary agricultural algorithm known as the “Nutrient Optimizer” from the Climate Corporation, a subsidiary of Monsanto, an internationally based company doing business in St. Louis, Missouri. The software uses machine learning to optimize fertilizer and seed application, an advanced system at the heart of modern precision farming. Haitao attempted to transfer the data back to China while working for the Chinese Academy of Sciences’ Institute of Soil Science.⁵²

These incidents reflect a broader trend in which state-backed or state-aligned actors look to accelerate China’s agricultural competitiveness by circumventing R&D timelines. So far, the primary objective appears to be commercial. But the implications are far more serious than economic espionage alone. Economically, such theft undermines U.S. agricultural competitiveness by eroding the innovation edge that sustains America’s productivity and net-export status in global food markets. Strategically, adversaries could potentially weaponize the stolen IP, especially genetic blueprints or agronomic algorithms.

Biothreats and Synthetic Bio Risks

Stolen genetic material from U.S. crops, particularly GM seeds, is at risk of being used for strategic sabotage. While China’s main interest in acquiring GM seeds to date has been to improve its own domestic crop yields, the dual-use nature of agricultural bio-

technology introduces the potential for adversaries to weaponize these assets.⁵³ Experts warn that these genetic blueprints could be reverse-engineered to introduce harmful modifications.⁵⁴ A researcher from the Chinese Academy of Sciences has openly acknowledged the ease with which GM traits can be reverse-engineered, noting that “an important feature of genetically modified technology is that reverse engineering is very easy to accomplish.”⁵⁵ The Chinese government has traditionally expressed skepticism toward importing GM crops from the West, but its scientific and defense communities have increasingly recognized the strategic utility of agricultural biotechnology.⁵⁶ Jiang Gaoming, a professor at the Chinese Academy of Sciences, made this clear in an open letter urging China’s GMO scientists to align their work with national defense imperatives: “Friends, GMO experts, your wisdom should be aimed at the enemy, not your own.”⁵⁷

Unlike conventional bioterrorism targeting human health, agricultural biothreats operate more subtly through crop degradation, pest introduction, or genetic contamination, which can trigger snowballing economic and environmental consequences. The U.S.-China Economic and Security Review Commission explicitly warned that GM seeds could be genetically altered to create blights or pathogens capable of targeting U.S. crops.⁵⁸ These warnings echo earlier findings from the National Defense University, which in 2011 identified the dual-use nature of synthetic biology as a potential avenue for biological warfare.⁵⁹ In addition to plant pathogens, rapidly spreading animal diseases, such as African Swine Fever or avian influenza, also pose a major threat to food security, especially given how concentrated and industrialized U.S. livestock production is.⁶⁰ However, recent U.S. biodefense strategy documents, including the 2023 Department of Defense Biodefense Posture Review, prioritize human health and military readiness over agricultural biotechnology as a potential vector for biothreats.⁶¹

Recent biosecurity incidents involving the PRC illustrate how threats to U.S. agriculture can span from low-cost, seemingly innocuous tactics to more deliberate and dangerous forms of biological aggression. In July 2020, thousands of Americans reported receiving mysterious seed packages in the mail with Chinese postage. The U.S. Department of Agriculture (USDA) and state agriculture officials urged recipients not to plant the seeds, warning they could be invasive species, carry plant pathogens, or disrupt native ecosystems. By early 2021, the USDA had collected over 20,000 seed packets and identified more than 100 distinct plant species, including noxious weeds and known agricultural pests.⁶² While initially believed to be a prank or e-commerce mishap, a March 2025 New York Times investigation revealed that similar unsolicited seed packages were still arriving in the U.S. as recently as 2024.⁶³

In June 2025, the threat of agricultural bioterrorism became even more concrete with two high-profile incidents highlighting critical gaps in U.S. biosecurity. Federal authorities arrested two Chinese nationals for conspiring to smuggle *Fusarium graminearum*, a dangerous fungal pathogen capable of devastating cereal crops, into a University of Michigan laboratory without proper permits.⁶⁴ *Fusarium graminearum*, which causes “head blight,” attacks wheat, barley, maize, and rice, and produces toxins that can harm both human and animal health, leading to liver disease, vomiting, and reproductive issues.⁶⁵ Just one week later, a separate case emerged in which another Chinese researcher was accused of illegally shipping worm-related biological materials into the U.S., concealing the specimens inside books destined for the same university.⁶⁶ Although no attack occurred, these incidents show how state-enabled agroterrorism is no longer a distant or hypothetical threat. The smuggling of biological agents points to a growing willingness to exploit biosecurity gaps for strategic advantage. When combined with foreign ownership

of key agribusiness assets and upstream control over chemical inputs and seed technologies, they reveal several potential entry points into the U.S. agriculture system.

GAPS IN POLICY AND SCHOLARSHIP

U.S. policy has long acknowledged agriculture as critical infrastructure, but only in narrow, hazard-based terms. It has been slow to recognize agriculture as a contested domain within hybrid warfare, where adversaries deliberately exploit food systems through cyber, bio, or economic coercion. Foundational authorities, such as Homeland Security Presidential Directive 9 (2004) and the Securing Our Agriculture and Food Act (2017), tasked DHS with coordinating the defense of the Food and Agriculture Sector. Subsequent initiatives, including the National Agriculture and Food Defense Strategy (2015, 2019) and the Food Safety Modernization Act (2011), emphasized resilience in the face of contamination or natural disasters.⁶⁷ Similarly, the National Infrastructure Protection Plan (2013) and the Food and Agriculture Sector-Specific Plan (2015) recognized agriculture's critical infrastructure status but framed threats largely in terms of traditional hazards.⁶⁸ This hazard-centric posture meant that adversarial exploitation of agriculture, through cyber intrusions, biotechnology manipulation, or foreign investment, remained outside the scope of national security planning. More recent policies show incremental change. National Security Memorandum-16 (2022) and National Security Memorandum-22 (2024) reaffirmed agriculture's critical role and designated USDA and Health and Human Services (HHS) as co-Sector Risk Management Agencies (SRMAs).⁶⁹ Yet these were modest steps, confirming existing responsibilities without embedding agriculture into broader deterrence or hybrid threat frameworks.

A more substantial shift came in 2025 with USDA's National Farm Security Action Plan (NFSA), the first initiative to explicitly frame agriculture as a national security priority.⁷⁰ The NFSA laid out a seven-part strategy to secure farmland, strengthen supply chain resilience, enhance research protections, and safeguard plant and animal health. It introduced significant reforms to the Agricultural Foreign Investment Disclosure Act, including higher penalties for noncompliance, stricter disclosure rules, and closer coordination with the Committee on Foreign Investment in the United States (CFIUS) on foreign land purchases. It also launched a publicly accessible map of foreign landownership and a reporting portal for suspicious investment activity. These measures marked meaningful progress by embedding security considerations into a domain that had long been treated as primarily economic.

At the same time, the NFSA underscored how slow U.S. policy has been to adapt. It addresses risks that had accumulated for more than a decade, but its scope remained narrow: heavily weighted toward land ownership and transparency while cyber vulnerabilities, biotechnology risks, and hybrid threat scenarios were left underdeveloped. Most critically, the NFSA stopped short of embedding agriculture into the nation's broader deterrence posture alongside sectors such as semiconductors, energy, or telecommunications. In this sense, the NFSA was a significant step forward but still a reactive and incomplete strategy for defending agriculture in the context of great-power competition.

Cybersecurity policies further underscore these gaps. Until recently, national cyber strategies paid little attention to agriculture. The bipartisan Farm and Food Cybersecurity Act (2024-2025) was a stop-gap effort, directing USDA and DHS to assess sector vulnerabilities and run annual threat exercises.⁷¹ In parallel, CISA conducted a national-level cyber wargame in 2024, Cyber Storm IX, the first national-level cyber wargame to designate the Food and

Agriculture sector as the primary impacted sector, highlighting how late agriculture was to be included in federal cyber planning.⁷² The 2023 launch of the Food and Agriculture-ISAC also provided a new platform for industry threat sharing.⁷³ Yet neither the 2023 National Cybersecurity Strategy nor CISA's 2022 "Shields Up" campaign explicitly prioritized agriculture, even after the 2021 ransomware attack on JBS temporarily shut down U.S. meatpacking plants and disrupted nearly one-fifth of national beef production, in a clear demonstration of how cyber extortion could paralyze critical food infrastructure.⁷⁴ Taken together, recent legislative, wargaming, and industry initiatives represent progress, but they remain piecemeal and reactive. No permanent framework integrates agriculture into national cyber deterrence, continuity planning, or sector-wide resilience.

Biosecurity policy, particularly in the agricultural domain, remains incomplete. The National Biodefense Strategy (2018, updated 2022) acknowledges agro-terrorism but does not anticipate state-sponsored biological attacks on crops or livestock.⁷⁵ Oversight remains fragmented across USDA, DHS, HHS/FDA, and state agencies, with no single entity positioned to coordinate defenses against hybrid campaigns that span biological, cyber, and economic vectors. The DHS Threats to Food and Agriculture Resources (TFAR) report (2021) highlighted these weaknesses, calling attention to insufficient biosurveillance, the absence of sector-wide cyber incident reporting, and the lack of a trained agricultural defense workforce.⁷⁶ The National Security Commission on Emerging Biotechnology (NSCEB), established in the FY22 NDAA, added further warning in its 2025 final report: the United States lacks a coordinated biotechnology strategy and is falling behind China, which has treated biotech as a strategic priority for two decades. The Commission urged treating biological data as a strategic resource, expanding

biosafety and biosecurity tools, and using national security authorities to protect U.S. innovation. Yet these recommendations remain broad, focused on medicine, defense, and biomanufacturing, with little operational attention to agriculture.⁷⁷ This gap is significant: agricultural biotechnology, from GM seeds to animal genetics, is already a high-value target, and adversaries such as China have demonstrated the capability and intent to exploit it through IP theft and data acquisition.

The academic literature has similarly been slow to treat agriculture as a deliberate target in hybrid warfare. While hybrid warfare and gray-zone conflict studies have expanded over the past decade, agriculture is rarely analyzed as a deliberate target or tool of coercion. Most scholarship focuses on information, energy, or finance, with extensive work on cyberattacks against power grids or elections but little on grain distribution systems or livestock platforms. Russia's war in Ukraine offered a vivid case study of food disruption as a weapon. Some analysts have asked whether similar strategies could be weaponized against the United States. Lt. Col. Karl Scheuerman's 2023 *Joint Force Quarterly* essay drew parallels between Russia's targeting of Ukraine's grain infrastructure and potential vulnerabilities in U.S. wheat systems, urging policy shifts such as a national grain reserve and stronger cyber-bio defenses.⁷⁸ Apart from a 2022 U.S.-China Economic and Security Review Commission report on Chinese agricultural investment, however, little work has synthesized Beijing's economic coercion, cyber capabilities, and biotechnology ambitions in the agricultural domain.

This lack of attention is reinforced by complacency. Policymakers and academics have treated the U.S. food supply as secure by default, likely due to the United States' long-standing status as a net exporter of agricultural goods. Abundance has created the assumption that food security threats are problems of fragile states or conflict zones, not

of the United States itself. As a result, research and policy attention have often focused on how the U.S. can feed the world, rather than how adversaries might target our own agri-food systems. In reality, advanced agrifood systems rest on fragile foundations. Just-in-time logistics, globalized supply chains, and foreign-sourced critical inputs introduce compounding risks that could be exploited in a crisis. The COVID-19 pandemic and ensuing supply chain disruptions were the first major stress test: empty shelves, processing plant shut-downs, and export bottlenecks made clear that even surplus-producing nations are not immune to disruption.

TOWARD AN AGRICULTURE SECURITY FRAMEWORK

Agriculture is politically salient in ways that make it an especially attractive target for hybrid coercion. Disruptions to food systems are felt immediately by households, communities, and electoral constituencies, giving them a visibility and emotional weight that attacks on military or government assets often lack. This creates opportunities for adversaries, most notably the PRC, to manipulate public opinion and indirectly pressure U.S. policymakers. At a time when interdependence, consolidation, and digitization magnify systemic risks, treating agriculture as peripheral to national security has left the United States reliant on thin scholarship and reactive policies.

Bridging the gaps in policy and scholarship requires a conceptual framework for understanding agriculture as a domain of security in its own right. We define this framework as agriculture security (AgSec): the protection of farm-to-fork infrastructure, including inputs, production, processing, logistics, and data, from deliberate disruption, manipulation, or exploitation by state and non-state actors. Whereas food security research emphasizes access and availability, AgSec focuses

on the infrastructures and processes that sustain those outcomes. This distinction is key to bringing agriculture into deterrence and resilience planning. Agriculture's designation as critical infrastructure has not, to date, translated into its integration within hybrid warfare planning. Adversaries such as the PRC have already shown how food systems can be pressured indirectly through cyberattacks, foreign investment, market manipulation, and biotechnology theft. Adding AgSec to the security lexicon provides a framework to capture these activities as deliberate coercive tactics rather than peripheral economic events. This shift matters: it gives policymakers a shared language for identifying agriculture as a contested domain; it allows analysts to anticipate how hybrid threats might converge on food systems; and it guides investment toward resilience measures on par with those in semiconductors, energy, and critical minerals.

Operationalizing AgSec requires tools that can both identify vulnerable nodes and test institutional responses. CARVER and CARVER+Shock, military vulnerability assessment tools that have long been used in food defense at the facility level, should be adapted to agricultural systems at the national scale. CARVER evaluates nodes across six attributes: Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability. CARVER+Shock adds a seventh dimension, capturing the combined health, economic, and psychological impacts of disruption. These tools have already been applied in practice in the food and agriculture sector but have been exclusively confined to the facility and product level. Expanding CARVER to the national scale across fertilizer supply chains, export terminals, and precision-agriculture platforms would allow policymakers to generate a ranked index of systemic vulnerabilities, prioritize resilience investments, and compare risks across subsectors and regions. In this way, CARVER evolves from a narrow food defense tool

into an instrument of hybrid deterrence. However, the traditional CARVER model alone is insufficient for mapping today's agricultural ecosystem, where interdependencies generate overlapping and non-linear effects. Future research should build on this foundation—leveraging advances in AI—to develop complex systems modeling tools that capture second-, third-, and higher-order consequences of both friendly and adversary actions.

Where CARVER identifies vulnerabilities, wargaming tests how institutions respond when those vulnerabilities are exploited. In agriculture security, wargames can serve three complementary purposes: for policymakers, they provide a rehearsal space for crisis coordination and decision-making; for scholars, they generate empirical data on threat perception, resource allocation, and institutional blind spots; and for industry, they stress-test continuity plans and expose asymmetries in data-sharing with government. Agriculture-focused wargames should simulate a range of hybrid disruptions, from cyber intrusions into precision-agriculture systems, to export bans that restrict fertilizer supply, to bio-threats against livestock and crops. Unlike one-off exercises, a sustained corpus of AgSec wargaming would build a dataset over time, inform theory building on how hybrid threats exploit civilian infrastructure, and deliver decision-support tools that strengthen deterrence and resilience alike.

Finally, alliances must embed agriculture into their strategies to sustain both resilience and deterrence. For decades, U.S. agricultural surpluses have underpinned alliance stability—from sustaining victory in WWII to anchoring the Marshall Plan and Food for Peace, food power has long been a source of U.S. economic strength and a decisive instrument of statecraft. Today, however, that foundation is eroding. Brazil's rise in soybean exports and Russia's growing dominance in wheat already challenge U.S. leadership, leaving partners more vulnerable to coercion through food supply. The PRC,

which has already weaponized trade through export controls, punitive tariffs, and fertilizer restrictions, is deliberately positioning itself to undermine U.S. agricultural leadership. Its campaign of economic punishment against Australia after Canberra called for an independent COVID-19 investigation targeted wine, barley, beef, and other farm exports—illustrating the speed and severity of coercion when food becomes a pressure point, while demonstrating how U.S. producers benefited in the short term from redirected demand.⁷⁹ Similarly, during ongoing U.S.-China trade tensions, Beijing has treated American farmers as bargaining chips, cutting off soybean imports to impose political and economic costs. These cases show agriculture is not a hypothetical target for economic coercion; it is already a recurring tool in Beijing's playbook.

As U.S. dominance erodes and competitors like Brazil, Russia, and China gain ground, the risk is not only the loss of economic primacy but the handover of strategic leverage to geopolitical rivals. Preventing that outcome requires treating agriculture as a core element of national power, on par with semiconductors, energy, and critical minerals. To prevent this, agriculture must be elevated within frameworks such as AUKUS, the Quad, and NATO. Practical steps include joint risk-mapping of key choke-points, scenario-based wargaming to stress-test responses, and trade agreements that explicitly align economic and security interests. Policy measures should also extend alliance structures to secure food and agricultural inputs alongside advanced tech, defense, and energy, with built-in rapid response mechanisms when a partner is targeted by coercive measures.

Closing these gaps is all the more urgent because the consequences of disruption extend far beyond the United States and its closest allies. As one of the world's leading exporters, the United States stabilizes both commercial markets and international food aid. A major disruption—whether

from cyberattacks, biothreats, or geopolitical choke-points—would not only harm U.S. producers and consumers but also destabilize food markets around the globe. In regions already struggling with hunger and instability, a breakdown in U.S. exports could intensify humanitarian crises, fuel political unrest, and spark conflict. The resilience of U.S. agriculture is not merely a domestic concern; it is a global imperative. Agriculture must no longer be treated as peripheral to national security but as one of its cornerstones: an essential pillar of international stability whose disruption would reverberate far beyond America's borders. **PRISM**

Notes

¹U.S. Department of War (DoW). *2026 National Defense Strategy of the United States of America*. Washington, DC: DoW, 2026. <https://media.defense.gov/2026/Jan/23/2003864773/-1/-1/0/2026-NATIONAL-DEFENSE-STRATEGY.PDF>.

²NATO Strategic Communications Centre of Excellence. *Hybrid Threats and Hybrid Warfare*. NATO, 2024. https://www.nato.int/nato_static_fl2014/assets/pdf/2024/7/pdf/241007-hybrid-threats-and-hybrid-warfare.pdf; Department of Defense. *2022 National Defense Strategy of the United States of America*. Washington, D.C.: Department of Defense, 2022; Peter Mattis, “China’s ‘Three Warfares’ in Perspective,” *War on the Rocks*, January 30, 2018, <https://warontherocks.com/2018/01/chinas-three-warfares-perspective/>.

³U.S. Department of Agriculture, Foreign Agricultural Service, *2023 U.S. Agricultural Export Yearbook*, May 14, 2024, <https://www.fas.usda.gov/data/2023-us-agricultural-export-yearbook>.

⁴Cybersecurity and Infrastructure Security Agency (CISA), “Food and Agriculture Sector,” accessed April 9, 2025, <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/food-and-agriculture-sector>.

⁵Johanna Yang and Maria Riofrio, “Cybercriminals Targeting U.S. Food and Agriculture Sector Now More Than Ever,” *Foundation for Defense of Democracies*, February 13, 2025, <https://www.fdd.org/analysis/2025/02/13/cybercriminals-targeting-u-s-food-and-agriculture-sector-now-more-than-ever/>.

⁶U.S. Government Accountability Office, *Precision Agriculture: Benefits and Challenges for Technology Adoption and Use*, GAO-24-105962 (Washington, D.C.: U.S. Government Accountability Office, 2024), <https://www.gao.gov/products/gao-24-105962>.

⁷Department of Homeland Security. *Threats to Food and Agriculture Resources*. Washington, DC: Department of Homeland Security, 2021, https://www.dhs.gov/sites/default/files/publications/threats_to_food_and_agriculture_resources.pdf.

⁸U.S. International Trade Commission, “The Impact of the COVID-19 Pandemic on Freight Transportation Services and U.S. Merchandise Imports,” *Shifts in U.S. Merchandise Trade, 2020*, November 2021, https://www.usitc.gov/research_and_analysis/tradeshifts/2020/special_topic.html.

⁹U.S. Government Accountability Office, *Precision Agriculture: Benefits and Challenges for Technology Adoption and Use*, GAO-24-105962 (Washington, DC: U.S. Government Accountability Office, January 2024), <https://www.gao.gov/products/gao-24-105962>.

¹⁰MITRE Corporation. *U.S. Food Supply Chain Security: A Network Analysis*. McLean, VA: MITRE Corporation, 2021, <https://www.mitre.org/sites/default/files/2021-10/pr-21-1826-us-food-supply-chain-security-a-network-analysis.pdf>.

¹¹U.S. Department of Agriculture, Foreign Agricultural Service, *Impacts and Repercussions of Price Increases on the Global Fertilizer Market*, September 2022, <https://www.fas.usda.gov/data/impacts-and-repercussions-price-increases-global-fertilizer-market>.

¹²USDA Economic Research Service, “Most Fertilizer Prices Increased from February to March 2022,” *Charts of Note*, May 16, 2022, <https://www.ers.usda.gov/data-products/charts-of-note/chart-detail/?chartId=111221>.

¹³Vladimir Soldatkin and Katya Golubkova, “Kremlin’s Fertilizer Cash Stream Is a Blind Spot in EU Sanctions,” *Reuters*, March 14, 2025, <https://www.reuters.com/markets/commodities/kremlins-fertilizer-cash-stream-is-blind-spot-eu-sanctions-vladimirov-2025-03-14/>; U.S. Department of the Treasury, Office of Foreign Assets Control, “Russia Sanctions: Agricultural Commodities, Fertilizer, and Medicine,” updated guidance, <https://ofac.treasury.gov>.

¹⁴Kee, Jennifer, Lila Cardell, and Yacob Abrehe Zereyesus, “Global Fertilizer Market Challenged by Russia’s Invasion of Ukraine,” *Amber Waves*, U.S. Department of Agriculture, Economic Research Service, September 18, 2023, <https://www.ers.usda.gov/amber-waves/2023/september/global-fertilizer-market-challenged-by-russia-s-invasion-of-ukraine>.

¹⁵ National Development and Reform Commission (NDRC), *National Development and Reform Commission*, <https://en.ndrc.gov.cn/>.

¹⁶ China 2023 Soybean Imports From Brazil Rise 29%, US Share Shrinks,” *UkrAgroConsult*, January 23, 2024, <https://ukragroconsult.com/en/news/china-2023-soybean-imports-from-brazil-rise-29-us-share-shrinks>.

¹⁷ Tortajada, Cecilia, and Hongzhou Zhang. “When Food Meets BRI: China’s Emerging Food Silk Road.” *Global Food Security* 29 (2021): 100518, <https://doi.org/10.1016/j.gfs.2021.100518>.

¹⁸ Al-Allaf, Azzam and Salam Said, *Russian Investment in Syrian Phosphate: Opportunities and Challenges*, Policy Briefs 2021/04, Middle East Directions (MED), Wartime and Post-Conflict in Syria (Florence: European University Institute, 2021), <https://hdl.handle.net/1814/69882>.

¹⁹ Ali Dehghantaha, “Cyber-attacks a Growing Threat to Farm, Food Security, Warn U of G Researchers,” *University of Guelph News*, August 17, 2022, <https://news.uoguelph.ca/2022/08/cyber-attacks-a-growing-threat-to-farm-food-security-warn-u-of-g-researchers/>.

²⁰ Adebunmi Okechukwu Adewusi, Njideka Rita Chiekezie, and Nsiong Louis Eyo-Udo, “Cybersecurity in Precision Agriculture: Protecting Data Integrity and Privacy,” *International Journal of Applied Research in Social Sciences* 5, no. 10 (December 2023): 693–708, <https://fepl.com/index.php/ijarss/article/view/1482/1725>.

²¹ Paul Roberts, “DEF CON: Security Holes in Deere, Case IH Shine Spotlight on Agriculture Cyber Risk,” *The Security Ledger*, August 8, 2021, <https://securityledger.com/2021/08/def-con-security-holes-in-deere-case-ih-shine-spotlight-on-agriculture-cyber-risk/>.

²² Federal Bureau of Investigation, “Ransomware Attacks on Agricultural Cooperatives Potentially Timed to Critical Seasons,” Private Industry Notification 20220420-001, April 20, 2022, <https://www.ic3.gov/CSA/2022/220420-2.pdf>; Aishwarya Nair, “JBS Says It Paid \$11 Million Ransom After Cyberattack,” *Reuters*, June 9, 2021, <https://www.reuters.com/technology/jbs-paid-11-mln-response-ransomware-attack-2021-06-09/>.

²³ U.S.-China Economic and Security Review Commission, *2022 Annual Report to Congress*, November 2022, <https://www.uscc.gov/annual-report/2022-annual-report-congress>.

²⁴ U.S.-China Economic and Security Review Commission, “China’s Interests in U.S. Agriculture: Augmenting Food Security through Investment Abroad,” May 26, 2022, [https://www.uscc.gov/sites/default/files/2022-05/Chinas Interests in U.S. Agriculture.pdf](https://www.uscc.gov/sites/default/files/2022-05/Chinas%20Interests%20in%20U.S.%20Agriculture.pdf).

²⁵ Steve Karnowski, “Air Force Opposes Chinese-Owned Corn Plant for North Dakota,” *AP News*, January 31, 2023, <https://apnews.com/article/politics-north-dakota-state-government-kevin-cramer-doug-burgum-china-9345443132364783ba3f94e34352f0c2>.

²⁶ John Cornyn, “Cornyn Urges DoD to Block Chinese Wind Farm Near Laughlin AFB,” *Senator John Cornyn*, July 16, 2024, <https://www.cornyn.senate.gov/news/cornyn-urges-dod-to-block-chinese-wind-farm-near-laughlin-afb/>.

²⁷ John Hyatt, “Exclusive: Inside a Chinese Billionaire’s Bizarre Maneuvers to Save His Texas Land,” *Forbes*, May 26, 2023, <https://www.forbes.com/sites/johnhyatt/2023/05/26/exclusive-inside-a-chinese-billionaires-bizarre-maneuvers-to-save-his-texas-land/>.

²⁸ U.S.-China Economic and Security Review Commission, “China’s Interests in U.S. Agriculture: Augmenting Food Security through Investment Abroad,” May 26, 2022, [https://www.uscc.gov/sites/default/files/2022-05/Chinas Interests in U.S. Agriculture.pdf](https://www.uscc.gov/sites/default/files/2022-05/Chinas%20Interests%20in%20U.S.%20Agriculture.pdf).

²⁹ Renee Wilde, “American Soil Is Increasingly Foreign Owned,” *The Land Report*, September 28, 2019, <https://landreport.com/american-soil-is-increasingly-foreign-owned>.

³⁰ Michael Hirtzer, “Pork Giant Smithfield Skips Middlemen in Grain Supply Chain,” *Reuters*, December 30, 2016, <https://www.reuters.com/article/world/uk/pork-giant-smithfield-skips-middlemen-in-grain-supply-chain-idUSKBN14J0DB>.

³¹ U.S.-China Economic and Security Review Commission, *2022 Annual Report to Congress*, November 2022, <https://www.uscc.gov/annual-report/2022-annual-report-congress>.

³² Fadel Allassan, “U.S. Meatpackers Exported Record Amount of Pork to China While Warning About Supply Shortages,” *Axios*, June 16, 2020, <https://www.axios.com/2020/06/16/meatpackers-pork-china-coronavirus>.

³³ “COFCO Takes Over Mississippi River Terminal,” *Great American Crop*, June 27, 2024, <https://www.greatamericancrop.com/news-resources/article/2024/06/27/cofco-takes-over-miss-river-terminal>.

³⁴ U.S.-China Economic and Security Review Commission, *2024 Report to Congress: Executive Summary and Recommendations*, November 2024, [https://www.uscc.gov/sites/default/files/2024-11/2024 Executive Summary.pdf](https://www.uscc.gov/sites/default/files/2024-11/2024%20Executive%20Summary.pdf).

³⁵ Fitch Ratings, “China National Chemical Corporation Limited,” May 29, 2020, <https://www.fitchratings.com/research/corporate-finance/china-national-chemical-corporation-limited-29-05-2020>; U.S.-China Economic and Security Review Commission, *2022 Annual Report to Congress*, November 2022, <https://www.uscc.gov/annual-report/2022-annual-report-congress>.

³⁶ U.S.-China Economic and Security Review Commission, “China’s Interests in U.S. Agriculture: Augmenting Food Security through Investment Abroad,” May 26, 2022, https://www.uscc.gov/sites/default/files/2022-05/Chinas_Interests_in_U.S._Agriculture.pdf.

³⁷ U.S.-China Economic and Security Review Commission, “China’s Interests in U.S. Agriculture: Augmenting Food Security through Investment Abroad,” May 26, 2022, https://www.uscc.gov/sites/default/files/2022-05/Chinas_Interests_in_U.S._Agriculture.pdf.

³⁸ Kee, Jennifer, Lila Cardell, and Yacob Abrehe Zereyesus, “Global Fertilizer Market Challenged by Russia’s Invasion of Ukraine,” *Amber Waves*, U.S. Department of Agriculture, Economic Research Service, September 18, 2023, <https://www.ers.usda.gov/amber-waves/2023/september/global-fertilizer-market-challenged-by-russia-s-invasion-of-ukraine>.

³⁹ Aya Adachi, “PRC Fertilizer Export Controls Provoke Derisking Abroad,” *China Brief* 24, no. 19 (October 4, 2024), <https://jamestown.org/program/prc-fertilizer-export-controls-provoke-derisking-abroad/>.

⁴⁰ Farmers Business Network, 2025 USA Ag Chem Price Transparency Report, Farmers Business Network, 2025, accessed September 9, 2025, <https://go.fbn.com/rs/197-HFR-752/images/2025%20USA%20Ag%20Chem%20Price%20Transparency%20Report.pdf>.

⁴¹ Farmers Business Network, 2025 USA Ag Chem Price Transparency Report, Farmers Business Network, 2025, accessed September 9, 2025, <https://go.fbn.com/rs/197-HFR-752/images/2025%20USA%20Ag%20Chem%20Price%20Transparency%20Report.pdf>.

⁴² Julia Santolin, Oliver Christopher Larsen, Albrecht Fritze, Bing Xue, Zheng Yang, and Vera Susanne Rotter, “Reaching China’s Fertilizer Reduction Goals through Nitrogen and Phosphorus Recovery: A Substance Flow Analysis Case Study,” *Journal of Material Cycles and Waste Management* 26 (2024): 3650-3664, <https://doi.org/10.1007/s10163-024-02067-6>.

⁴³ Kim, Sung Eun and Yotam Margalit, “Tariffs as Electoral Weapons: The Political Geography of the US–China Trade War,” *International Organization* 75, no. 1 (Winter 2021): 1–38, <https://doi.org/10.1017/S0020818320000612>.

⁴⁴ U.S.-China Economic and Security Review Commission, “China’s Interests in U.S. Agriculture: Augmenting Food Security through Investment Abroad,” May 26, 2022, https://www.uscc.gov/sites/default/files/2022-05/Chinas_Interests_in_U.S._Agriculture.pdf.

⁴⁵ Oliver Morrison, “The Ultimate Trojan Horse? US Drone Makers Up in Arms About Chinese Industry Advancement,” *AgTechNavigator*, April 8, 2024, <https://www.agtechnavigator.com/Article/2024/04/08/The-ultimate-Trojan-Horse-US-drone-makers-up-in-arms-about-Chinese-industry-advancement/>.

⁴⁶ Mohd. Hasan Ali Hasan and Md. Rabiul Islam, “Cyberthreats and Security Measures in Drone-Assisted Agriculture,” *Electronics* 14, no. 1 (2025): 149, <https://doi.org/10.3390/electronics14010149>.

⁴⁷ Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI), *Cybersecurity Guidance: Chinese-Manufactured UAS*, January 17, 2024, <https://www.cisa.gov/sites/default/files/2024-01/Cybersecurity%20Guidance%20Chinese-Manufactured%20UAS.pdf>.

⁴⁸ Office of Public Affairs, U.S. Department of Justice, “U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage,” November 27, 2017, <https://www.justice.gov/archives/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations>.

⁴⁹ Mandiant, “Does This Look Infected? A Summary of APT41 Targeting U.S. State Governments,” *Google Cloud Blog*, March 8, 2022, <https://cloud.google.com/blog/topics/threat-intelligence/apt41-us-state-governments/>.

⁵⁰ Federal Bureau of Investigation, “Protecting Vital Assets: Pilfering of Corn Seeds Illustrates Intellectual Property Theft,” December 19, 2016, <https://www.fbi.gov/news/stories/sentencing-in-corn-seed-intellectual-property-theft-case>.

⁵¹ U.S. Department of Justice, Office of Public Affairs, “Kansas Agricultural Scientist Convicted in Theft of Engineered Rice,” February 16, 2017, <https://www.justice.gov/archives/opa/pr/kansas-agricultural-scientist-convicted-theft-engineered-rice>.

⁵² U.S. Department of Justice, “Chinese National Sentenced for Economic Espionage Conspiracy,” news release, April 7, 2022, <https://www.justice.gov/archives/opa/pr/chinese-national-sentenced-economic-espionage-conspiracy>.

⁵³ Jerry Warner, James Ramsbotham, Ewelina Tunia, and James J. Valdes, *DTP-082: Analysis of the Threat of Genetically Modified Organisms for Biological Warfare*, Defense Technology Paper, National Defense University Press, May 2011, <https://ndupress.ndu.edu/Media/News/Article/1229164/dtp-082-analysis-of-the-threat-of-genetically-modified-organisms-for-biological/>.

⁵⁴ U.S.-China Economic and Security Review Commission, “China’s Interests in U.S. Agriculture: Augmenting Food Security through Investment Abroad,” May 26, 2022, [https://www.uscc.gov/sites/default/files/2022-05/Chinas Interests in U.S. Agriculture.pdf](https://www.uscc.gov/sites/default/files/2022-05/Chinas%20Interests%20in%20U.S.%20Agriculture.pdf).

⁵⁵ *Chinese Science Journal*, “Experts from the Chinese Academy of Sciences Comment on the ‘Conspiracy Theory: It is the Imagination of the Layman that is Technically Not True,’” January 23, 2017, <https://tech.sina.cn/d/qy/2017-01-23/detail-ixfzuswq3301796.d.html>.

⁵⁶ U.S.-China Economic and Security Review Commission, “China’s Interests in U.S. Agriculture: Augmenting Food Security through Investment Abroad,” May 26, 2022, <https://www.uscc.gov/sites/default/files/2022-05/Chinas Interests in U.S. Agriculture.pdf>.

⁵⁷ Jiang Gaoming, “Are Biological Weapons an Exaggeration?,” *Aisixiang*, January 12, 2018, <https://tech.sina.cn/d/qy/2017-01-23/detail-ixfzuswq3301796.d.html>.

⁵⁸ U.S.-China Economic and Security Review Commission, “China’s Interests in U.S. Agriculture: Augmenting Food Security through Investment Abroad,” May 26, 2022, <https://www.uscc.gov/sites/default/files/2022-05/Chinas Interests in U.S. Agriculture.pdf>.

⁵⁹ Warner, Jerry, James Ramsbotham, Ewelina Tunia, and James J. Valdes, *DTP-082: Analysis of the Threat of Genetically Modified Organisms for Biological Warfare*, Defense Technology Paper, National Defense University Press, May 2011, <https://ndupress.ndu.edu/Media/News/Article/1229164/dtp-082-analysis-of-the-threat-of-genetically-modified-organisms-for-biological/>.

⁶⁰ U.S. Department of Agriculture, Animal and Plant Health Inspection Service, *United States National Animal Health Surveillance System: 2017 Surveillance Activity Report* (Washington, DC: USDA APHIS, November 2018), <https://www.aphis.usda.gov/sites/default/files/nahss-annual-report.pdf>.

⁶¹ Department of Defense, *2023 Biodefense Posture Review*, August 2023, [https://media.defense.gov/2023/Aug/17/2003282337/-1/-1/2023 BIODEFENSE POSTURE REVIEW.PDF](https://media.defense.gov/2023/Aug/17/2003282337/-1/-1/2023%20BIODEFENSE%20POSTURE%20REVIEW.PDF).

⁶² Waller, Allyson, “27 States Issue Warnings About Seed Packets From China,” *The New York Times*, July 26, 2020, <https://www.nytimes.com/2020/07/26/us/seeds-from-china-mail.html>.

⁶³ Shear, Michael D. and Katie Rogers, “Invasive Seeds Scam Tied to China Raises Concerns,” *New York Times*, March 31, 2025, <https://www.nytimes.com/2025/03/31/us/invasive-seeds-scam-china.html>.

⁶⁴ U.S. Department of Justice, U.S. Attorney’s Office, Eastern District of Michigan, *Chinese Nationals Charged with Conspiracy and Smuggling a Dangerous Biological Pathogen into the U.S. for Their Work at a University of Michigan Laboratory*, press release, June 3, 2025, <https://www.justice.gov/usao-edmi/pr/chinese-nationals-charged-conspiracy-and-smuggling-dangerous-biological-pathogen-us>.

⁶⁵ American Phytopathological Society, New Toxin Facilitates Disease Infection and Spread in Wheat, press release, July 13, 2023, APSNet Newsroom, <https://www.apsnet.org/about/newsroom/releases/Pages/NXtrichothecenes.aspx>.

⁶⁶ NBC News, “Another Chinese Researcher Accused of Smuggling Biological Material to University of Michigan via Books,” NBC News (online), June 10, 2025, <https://www.nbcnews.com/world/asia/another-chinese-researcher-accused-smuggling-biological-material-rcna211963>.

⁶⁷ National Agriculture and Food Defense Strategy (NAFDS): <https://www.fda.gov/food/food-defense-tools-educational-materials/nationalagriculture-and-food-defense-strategy-nafds>; *FDA Food Safety Modernization Act*, Public Law 111–353, U.S. Statutes at Large 124 (2011): 3885–3968, <https://www.congress.gov/111/plaws/publ353/PLAW-111publ353.pdf>.

⁶⁸ U.S. Department of Homeland Security, *National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: U.S. Department of Homeland Security, 2013), <https://www.cisa.gov/sites/default/files/2022-11/national-infrastructure-protection-plan-2013-508.pdf>; U.S. Department of Homeland Security, *Food and Agriculture Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan* (Washington, D.C.: U.S. Department of Homeland Security, 2015), <https://www.cisa.gov/sites/default/files/publications/nipp-ssp-food-ag-2015-508.pdf>.

⁶⁹ The White House, *Fact Sheet: Biden-Harris Administration Releases National Security Memorandum to Strengthen the Security and Resilience of U.S. Food and Agriculture*, November 10, 2022, <https://irp.fas.org/offdocs/nsm/nsm-16-fs.pdf>; The White House, *National Security Memorandum on Critical Infrastructure Security and Resilience*, April 30, 2024, <https://irp.fas.org/offdocs/nsm/nsm-22.pdf>.

⁷⁰ U.S. Department of Agriculture, National Farm Security Action Plan (Washington, DC: U.S. Department of Agriculture, 2025), <https://www.usda.gov/sites/default/files/documents/farm-security-nat-sec.pdf>.

⁷¹ U.S. Congress, Senate, *Farm and Food Cybersecurity Act of 2024*, S.3661, 118th Cong., 2nd sess., introduced in Senate January 25, 2024, <https://www.congress.gov/bill/118th-congress/senate-bill/3661>.

⁷² Cybersecurity and Infrastructure Security Agency. *Cyber Storm IX After-Action Report*. October 2024. https://www.cisa.gov/sites/default/files/2024-10/Cyber%20Storm%20IX%20After-Action%20Report%20v00%2020241001_508.pdf.

⁷³ Food and Agriculture-Information Sharing and Analysis Center (Food and Ag-ISAC), *Cybersecurity Guide for the Food and Agriculture Sector* (Washington, DC: U.S. Department of Agriculture, 2023), https://www.fsis.usda.gov/sites/default/files/media_file/documents/Food_and_Ag-ISAC_Cybersecurity_Guide.pdf.

⁷⁴ U.S. White House, Office of the National Cyber Director, National Cybersecurity Strategy (Washington, DC: The White House, March 2, 2023), <https://bidenwhitehouse.archives.gov/oncd/national-cybersecurity-strategy/>; Cybersecurity & Infrastructure Security Agency (CISA), Shields Up, CISA, <https://www.cisa.gov/shields-up>; HackersHub, “JBS Foods Ransomware Attack: Cybersecurity Breach 2021,” HackersHub (website), June 2023, accessed September 9, 2025, <https://hackershuh.com/incidents/jbs-foods-ransomware-attack-cybersecurity-breach-2021>.

⁷⁵ Executive Office of the President of the United States, *National Biodefense Strategy and Implementation Plan for Countering Biological Threats, Enhancing Pandemic Preparedness, and Achieving Global Health Security* (Washington, DC: White House, October 2022), <https://www.whitehouse.gov/wp-content/uploads/2022/10/National-Biodefense-Strategy-and-Implementation-Plan-Final.pdf>.

⁷⁶ Department of Homeland Security. *Threats to Food and Agriculture Resources*. Washington, DC: Department of Homeland Security, 2021, https://www.dhs.gov/sites/default/files/publications/threats_to_food_and_agriculture_resources.pdf.

⁷⁷ U.S. Congress, *Congressional Research Service*, National Security Commission on Emerging Biotechnology: Final Report and Options for Congress, CRS Report IN12546 (2025), <https://www.congress.gov/crs-product/IN12546>.

⁷⁸ Karl A. Scheuerman, “Weaponizing Wheat: How Strategic Competition With Russia Could Threaten American Food Security,” *Joint Force Quarterly* 111 (4th Quarter 2023): 34–49, . https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-111/jfq-111_34-49_Scheuerman.pdf?ver=wNMywVo9xMndDtrU07ybA%3d%3d.

⁷⁹ Georgia Edmonstone, “China’s Trade Restrictions on Australian Exports,” United States Studies Centre, April 2, 2024, <https://www.usss.edu.au/chinas-trade-restrictions-on-australian-exports>.

Understanding Cognitive Warfare Beyond Information

By Dr. Robert Schmidle, Lieutenant General (Retired, USMC)

This paper is the result of a new research project funded by the Irregular Warfare Center (IWC) within the U.S. Department of War (DOW). The purpose of the project is to answer the question: “What is cognitive warfare (CogWar) and how is it different from information operations (IO), Political Warfare, propaganda, and other forms of non-kinetic warfare?”

Answering this question is important because CogWar lies at the foundation of 21st century IO in the irregular warfare (IW) sphere and the other domains of warfare like air, land, sea, and space, and that it is the key to victory—particularly victory without conventional war.¹ The ‘domain’ of CogWar takes as its battlespace the human cognitive functions of perception and creation of beliefs. The fight in this battlespace is for the perceptions of both enemy and friendly populations. It differs, for example, from IO in that IO is a fight for the data (and information) itself, while CogWar is a fight for the context and perceptions that give meaning to that information and data.²

Cognitive warfare prioritizes not data but the *meaning* of data. The question in CogWar becomes not “what data is noticed by people?” but “how does data lead to certain meaningful constructions by people, regardless of whether or not they are conscious of that data?”³ There is emerging research by scholars, security coalitions, and alliances that suggests that CogWar today, though as old as war itself in its foundations, is a new and potentially more effective form of warfare in achieving strategic goals.⁴ It uses the psychological weapons of fear, anxiety, and suspicion to weaken an adversary’s will to fight, while at the same time hardening the will of the friendly populations to continue the conflict.⁵

Dr. Robert Schmidle is a retired U.S. Marine Corps Lieutenant General and a noted scholar in cognitive warfare, cyber conflict, and strategy. One of his final senior postings was as Deputy Commander of U.S. Cyber Command, where he helped stand up and lead large-scale cyber operations across the U.S. Department of Defense. He previously held key leadership roles shaping national defense strategy, force design, and resource allocation. He is currently a Professor of Practice and University Advisor at Arizona State University, researching and teaching on cyber security and emerging technologies.

METHODOLOGY

To address the question, “What is Cognitive Warfare?” the author employed a modified Delphi method to engage experts in fields related to the study. The Delphi method is a group-based process for eliciting and aggregating opinions on a topic with the goal of exploring the existence of consensus or divergence among a generally diverse group of handpicked experts.⁶ Although the Delphi method usually includes anonymity, participants agreed to have their names disclosed to each other and in this publication, as there were neither security issues, professional reputation issues, nor perceived bias issues at stake.

Each selected expert was a subject matter expert on different aspects of CogWar, including psychology, neuroscience, intelligence, military strategy, and sociology.⁷ The objective of the workshop was to develop a practical framework for analyzing and codifying the concept of CogWar.

Each of the participants was required to give a presentation addressing the question “What is Cognitive Warfare?” from their perspective and within their particular academic discipline and background. The speaker’s agenda was arranged so that the presentations began with a focus on individual cognition and then transitioned to focusing on ever larger group cognition.

The following section of this paper is an exploration of the current literature on CogWar, as highlighted in the workshop. The literature review is followed by a synthesis of the major themes and discussions from the workshop conducted in the Arizona State University (ASU) facility in Washington, D.C. in May 2025. The final part of this paper elaborates on the evolution of CogWar, to its present-day challenges and opportunities. Throughout, there is continued exploration and articulation of the concept of CogWar in the context of current and emerging technologies, particularly

artificial intelligence (AI), neuroscience, and cyber. Additionally, trends in postmodern philosophy are incorporated and applied to our understanding of CogWar – both offensive actions and defensive mitigations. Lastly, the implications of CogWar for DOW are identified.

LITERATURE REVIEW

Defining the Terms

The three main points of consideration discussed in this section include: 1) deconstructing the expression to understand better what is meant by the words “cognitive” and “war” separately and when used together; 2) concluding that CogWar is a continuous struggle —there is no time of “peace” in a CogWar; and 3) understanding the logic of CogWar as a “societal war,” which plays to the moral forces that enable and support the will of a people to struggle and resist, or alternately, to surrender.

The topic of CogWar is best examined by first deconstructing the term to understand better the meanings of the words “cognitive” and “war,” separately and together. To begin, human cognition is a continuous process, not a discrete snapshot in time of a particular activity. Cognition is a process grounded in the cultural and social situation in which a person lives. In other words, an individual comes to understand their world through processes defined by socially constructed structures such as language.⁸ These cognitive processes are defined by the American Psychological Association (APA) as including “all forms of knowing and awareness, such as perceiving, conceiving, remembering, reasoning, judging, imagining, and problem solving.”⁹

Since these processes have a cultural and social foundation, research suggests that cognition could be different in type, if not in kind, depending on language, genetics, and so forth.¹⁰ However, research also shows that the primary determinant of the

beliefs and biases of the cognitive processing is the social order in which one lives.¹¹ Therefore, an effective CogWar campaign would target the social and cultural structures (and biases) that, in turn, create the understanding one has about the data used, for example, in making decisions. These social and cultural structures are also where power is dispersed throughout a society. It is dispersed at all levels, not just at the higher levels of political or economic leadership. The targets of an effective CogWar campaign are the perceptions the adversary holds as “true,” not simply the data that generally conforms to those perceptions. Those perceptions change by challenging the way power is distributed through a culture’s social norms and everyday practices. The People’s Republic of China’s (PRC) Social Credit System is an example of this strategy in practice, where individuals are ranked or scored based on their alignment with the economic and political policies of the Chinese government.¹²

Following this definition of cognition, the next step is to define the word “war.” The best way to define war is to start with Clausewitz since his magnum opus, *On War* (1832), is referenced in all professional military education (PME) in the United States. Clausewitz defines war as follows: “War is nothing but a duel on a larger scale”—a physical contest between people, each using force to compel our enemy to do our will.¹³ He does, however, differentiate between contests between individuals who are fighting (such as wrestling) and those between nations engaged in combat (war).

Importantly, while Clausewitz focuses on the use of physical force to compel an enemy, he acknowledges the overarching importance of the “moral forces” in war. Those moral forces are inseparable from the cognitive processes that created and then revealed them through actions. Clausewitz claims that “. . . the moral forces are amongst the most important subjects. . . they fasten themselves with the greatest affinity onto the

Will which puts in motion and guides the whole mass of powers, uniting with it as it were in one stream because this is a moral force itself.”¹⁴ These moral forces are what motivate the will of both the adversary and friendly sources of power and therefore become targets in CogWar.

It is also important to consider the following fundamental differences between CogWar (perception control) and conventional war (physical destruction). The first thing to keep in mind is that CogWar challenges the traditional strategic/tactical divide that grips contemporary thinking about the way of war. For example, in reviewing U.S. military operations since the end of World War Two (WWII), it is apparent that there has been a continued effort (albeit generally unsuccessful) to achieve strategic goals through the primary use of tactical military actions. Unfortunately, by privileging tactical actions, those actions are elevated to the level of strategy—a level at which tactics are increasingly irrelevant to the strategic outcomes of a conflict. It must be remembered that CogWar is fundamentally strategic, with a societal focus and impact, as opposed to being tactical, with a military focus and impact. Although the execution of CogWar may appear to be tactical in nature—IO, propaganda, etc.—those effects, to be relevant to an overall campaign, must be measurable in terms of a strategic (i.e., societal) impact.

The second consideration is that CogWar is a continuous struggle—there is no time of “peace.” This concept is dialectically opposed to combat in a conventional conflict, which, at least in principle, alternates between times of peace. Peace, in the context of relations between nation-states, has generally been considered the norm and war considered the aberration. CogWar challenges this characterization by inverting that paradigm—war now becomes the normal order of affairs and peace, the temporal aberration. This is important because of the way it changes the mindset of the belligerents. In other

words—CogWar is a continuous engagement toward achieving leverageable advantage—there is never a time of peace, except in the minds of those eternal optimists hoping for a Westphalian conclusion.

Third, the logic of CogWar as a societal war plays to the moral forces that enable and support the will to struggle and resist; it is indeed the society, the people of a country, whose will sustains and continues the fight, resulting in either victory or defeat. Lastly, the link among CogWar, technology, and language determine why CogWar is a unique and still emerging concept today. Military operations executed in any of the traditional warfighting domains are guided by extant cognitive processes, which in turn are defined by the social and cultural context in which those processes occur. Any operational decisions made in war necessarily result from processes in the cognitive domain and drive operations in all other domains of air, land, sea, space and cyber.

COGNITION AS A PROCESS

Cognitive processes have a cultural and social foundation. Research suggests that cognitive function and process differ between cultures such as those that exhibit independent social orientation versus those societies with interdependent social orientations. Varnum, Grossman, Kitayama, and Nisbet posit that Westerners and East Asians could also differ in cognitive tendencies due to linguistic, genetic, and cultural differences other than social orientation.¹⁵ However, they emphasize that social orientation is the primary determinant of cognitive processing type. This sets an important precedent for CogWar. It suggests that the most efficient and successful CogWar campaigns would be specifically tailored for target audiences based upon their cultural and societal characteristics at a macro and micro level.

CLAUSEWITZ ON COGNITIVE WARFARE

In *On War*, Clausewitz states that “. . . It would be an obvious fallacy to imagine war between civilized peoples as resulting merely from a rational act on the part of their governments and to conceive of war as gradually ridding itself of passion, so that in the end one would never really need to use the physical impact of the fighting forces.”¹⁶ Clausewitz is emphasizing that war results from emotional not rational acts on the part of the belligerents. Cognitive warfare by its very nature, targets those (emotional) passions in order to create the desired perceptions in a target population.

In *Clausewitzian Theory of War in The Age of Cognitive Warfare*, Brittain-Hale examines the Ukrainian Ministry of Defense’s (UMOD) use of social media influence operations through a Clausewitzian lens. Hale examines the relevancy of Clausewitzian theory to modern CogWar while positing the necessity for a “redefinition,” “expansion,” and “re-evaluation.”¹⁷ She subsequently applies the Clausewitzian model to CogWar for examination. Hale suggests that violence, although traditionally viewed as a physical act, should similarly be applied to “aggressive tactics that assault perceptions and beliefs.” She also notes that Clausewitz’s notion of “chance” illustrates the unpredictable and fluid nature of warfare. “Reason” (also from Clausewitz) on the other hand, demonstrates the calculated nature of the deployment of social media campaigns to achieve a political end.¹⁸ Hale states that “The extension of Clausewitz’s battlefield into the cognitive domain reflects a significant evolution in military strategy. It underscores the need for a holistic approach to conflict, considering the power of information and public perception as critical components of modern warfare.”¹⁹ Hale continues drawing parallels between the traditional application of Clausewitzian theory to kinetic warfare and

its contemporary relevance to the modern digital age. Cognitive warfare in theory, if not in practice, is better understood through the lens of the Clausewitzian model of war.

In comparison, David Pappalardo's *Win the War Before the War? A French Perspective on Cognitive Warfare*, cites Clausewitz as the supporting rationale for the idea that the battlefield has always included the cognitive domain and that modern cyber and technological capabilities have only "increased the magnitude" and "exacerbated competition."²⁰ Pappalardo states that three observations inform the CogWar approach to strategic thinking; that war has always implied a dialectic of wills and intelligences; that strategy is "a science of the other;" and that information is a weapon that offers a strategic advantage.²¹

COGNITIVE WAR IN THE 21ST CENTURY

Some have argued that CogWar is nothing new, that it has been employed for centuries.²² To an extent that is correct, because it is humans who make the decisions to go to war and then make the decisions on how to execute that war. However, there are factors today that make CogWar more effective, more dangerous, and potentially more intrusive in the lives of a target population than a conventional war. Importantly, CogWar is executed in 360 degrees; it is never just focused on the adversary.

Cognitive War today is different in these fundamental ways:

- First, communication and propagation technologies (Internet) enable a societal (strategic) focus that was heretofore only possible at a local (tactical) level. The Internet has had an unmistakable and unarguable impact on the transmission of data, the presentation and manipulation of data and the creation and alteration of discrete context, which gave

meaning to that data. Should the poster of such data have the knowledge, skill and good fortune to reach virality, it might be possible to reach thousands, if not millions, of people instantly and simultaneously. It also enables the more extreme beliefs in threat nations and diffused local groups to have an outsized voice and influence on the perceptions and actions of a given population.

- Second, the rapid and continuous maturing and evolution of AI enables the immediate creation and use of computational propaganda to boost a weaponized narrative.²³ Computational propaganda is the use of automated social media accounts and algorithms to enable media manipulation that pushes false information into mass awareness.²⁴ For example, generative AI could instantly target individuals with a tailored narrative designed to cause them to make decisions that they think are in their own best interest, when in fact those decisions enable their enemy's strategic goals.
- Third, advances in neuroscience that can mechanically, biologically, and chemically alter the human brain.²⁵ Neuroscience and mind-tech advancements are on the verge of fundamentally changing the interplay of chemical, biological, and environmental factors that create human consciousness and affect the process of cognition.²⁶
- Fourth, the influence of post-modern philosophy. While the influence of postmodernism may not be as obvious as that of the Internet, AI, or neuroscience, it nonetheless has a significant impact on modern CogWar and will be examined in more depth in this research paper.

Of these four factors that make CogWar different today, only the third, neuroscience and fourth, postmodernism, have had limited exposure

to a wider audience. The following part of this paper explains in more detail the influences of neuroscience and postmodernism on our current understanding of CogWar.

Neuroscience and mind-tech advancements are fundamentally changing CogWar, which has predominantly relied on thinking errors and cognitive distortions to change the perceptions of a target audience. Now, neuroscience is expanding the domains of CogWar by the modernization and use of pharmacological agents, microbial agents, organic toxins, and neurotechnology that can chemically, biologically, and mechanically modify functions of the human brain.²⁷

There is growing interest and investment by a number of nations in the application of neurocognitive approaches towards warfare, intelligence, and national security (WINS).²⁸ Biological and chemical weapons have historically been used for their profound physical effects of harm and death. However, current developments in neurocognitive science and mind-tech offers a wider range of non-lethal possibilities that allow for the covert manipulation of neurocognitive (and emotional) states and resulting behaviors of the target.

The neurosciences entail a convergent set of disciplines, inclusive of genetic and synthetic biology that can be focused on modifying neural structures and functions involved in cognitive, emotional and behavior functions. Thus, advancements in gene editing pose a new challenge in the future of CogWar. Gene editing through advancements in Clustered Regularly Interspaced Short Palindromic Repeats (CRISPR) enables relatively facile engineering of novel bioagents that may evade detection or attribution.²⁹ Dr. James Giordano, author of *Battlescape Brain: Engaging Neuroscience in Defense Operations*, raises concerns that current regulatory instruments such as the Biological and Toxin Weapons Convention (BTWC) and Chemical Weapons Convention (CWC) lack the ability to

constrain these technologies to their originally stated uses.³⁰ Non-state and malicious actors can operate by proxy outside of regulated channels creating dangerous and effective weaponizable agents.

Current research in nanoparticulate technologies provides a sobering glimpse of the future of CogWar. Nanotechnologies exist at the atomic or molecular level and, in a weaponizable form, have the ability to disrupt brain processes and affect the network properties of the brain.³¹ Existing nanotechnology applications range from the ability to attack specific tissues to the delivery of nanoparticles via the olfactory system in order to remotely control organisms.³² Nanotechnology will likely have an increasing role in CogWar as countries including China, Germany, Russia, United Kingdom, and the United States continue to fund nanotechnology research for its dual or direct military use.³³

CogWar continues to adapt and shift to the existing technology environment. As continued research in neurotechnology expands, CogWar will naturally incorporate advancements in technology to enhance its efficacy. Today, our understanding of CogWar differs from the past through its expanding use of modern neuroscience to yield more dynamic and measurable outcomes in changing perceptions and consequent actions within a target population.

POSTMODERNISM

The other major influence on our current thinking about CogWar is the intellectual and cultural movement known as Postmodernism, which began to emerge in the early 20th Century after World War One (WWI). It took many forms but of interest is the way the movement challenged conventional, objective views on knowledge and truth. The beginnings of this movement can be traced to the physicists. Einstein introduced the idea that the perspective of the observer would have an impact on the way the object being observed was inter-

preted.³⁴ Then Heisenberg postulated that the mere act of measuring would change the behavior of the system being observed (at least at the sub-atomic level).³⁵ Furthermore, Heisenberg argued that one could not be certain about the behavior of those systems, which exhibited exceptions to the prevailing Newtonian view about the logic and predictability of the universe.³⁶

These scientific theories informed the thinking of some philosophers and led them to argue that the world around us is socially constructed—by our perceptions and beliefs. In particular, Wittgenstein famously said that the “Limits of my language are the limits of my world.”³⁷ This means that the language I use to describe my world actually creates and limits what I can know of that world. He wasn’t talking about empirical things like mountains or scientific things like diseases. He was referring to human behaviors. Wittgenstein believed that knowledge was created through the social interactions of people in local moral orders and through the medium of language.³⁸ In other words, language doesn’t simply reflect the world around us, it creates our understanding of it. This concept marks a significant change from past views. Previous philosophers, such as Descartes, had argued that cognition was an internal, individual process. Now, the postmodern philosophers were arguing that cognition was an external, group process, which was shaped by culture and language.

A more recent postmodern philosopher, Michel Foucault would take that concept a step further. He proposed that within the process of cognition the origin of truth wasn’t outside power but rather it was produced by power.³⁹ He said that each society has its “regime of truth” which contains the types of discourses that it uses to distinguish between true and false statements.⁴⁰ This suggests that the expression “speaking truth to power” is a misnomer because “truth” is created

within those structures of power and not something discoverable outside of that context. Relating this notion to the previous discussion on cognition, it is evident that cognition is not a process focused on discovering some elusive universal and eternal truth. Rather, cognition is a process, which uncovers any number of possible truths. Truth(s), it seems are created and based on differing group and or individual perspectives. Those perspectives, in turn, give meaning to the events experienced by an individual or group. Importantly, Foucault was not referring to empirical or scientific truths – for example, “that is a mountain,” or “AIDS is a deadly disease.” Rather, he was referring to what counts as true in the interpretation of data—for example, arguments over empirical data by claiming to possess “alternative facts.”

According to Foucault, “Truth’ is linked in a circular relation to systems of power which produce and sustain it. . .”⁴¹ The implications for our understanding of CogWar are consequential because Foucault’s influence has extended into all regimes of current thought. The expressions, “follow the science,” “fake news,” or “facts matter” are examples of different truths that were created in different power structures. Following this line of thought, there exists an inherent relativity in the production of truth that makes it easier to dismiss empirical science and create and live in one’s own alternate reality. The creation of this alternate reality is where the effects of CogWar are amplified. If a country’s population is already conditioned to doubt their country’s political institutions and scientific research, it is easy to see how much more vulnerable they are to a concerted CogWar campaign. Especially since that campaign necessarily magnifies their doubts and exacerbates existing societal divisions.

In effect CogWar challenges the beliefs that a target population holds as true. Highlighting the conflict between what is seen as true by individuals

and groups and what they are told is true (by extant powers) creates what is known as cognitive dissonance, which is the psychological angst that comes from holding conflicting beliefs.⁴² In an attempt to reduce this angst, an individual or group will question seemingly empirical truths in an effort to minimize the conflict with the ‘truths’ created by other existing power structures. Widespread cognitive dissonance sets the stage for effective execution of CogWar against vulnerable populations.

In addition to the post-modern philosophers, there was, in the late 20th Century, a burgeoning movement in social psychology coalescing around the idea of Positioning Theory.⁴³ Positioning Theory focuses on how individuals are positioned (and position themselves) within conversations, narratives, and social situations, and how these positionings shape their rights, duties, and understanding of their world.⁴⁴ It is the concept of shaping narratives that is of interest in deepening our understanding of CogWar. This is because one of the most common methods of executing CogWar is by influencing narrative construction in both the friendly and enemy societies.

In line with our previous discussion, we see that these narratives are constructed first at the society level (inter-psychological) and then at the individual level (intra-psychological).⁴⁵ For example, *Russia Today*, an international TV channel, has developed and refined strategies for using conspiracy theories in international politics, especially targeting people in the United States and other relatively open societies.⁴⁶ The conspiracies propagated by *Russia Today* find their way into narratives shared by even mainstream groups in those countries including conspiracies that claim 9/11 didn’t happen or that it was a government coverup. The continuation of debunked conspiracies shows the power of narrative in shaping perceptions through the movement from the inter-psychological to the intra-psychological.⁴⁷

WHAT IS COGNITIVE WARFARE?

To form an understanding of contemporary schools of thought on CogWar, this section explores its existing definitions. Cognitive warfare is a contemporary term with mainstream adoption in the U.S. military in 2017.⁴⁸ Prior works such as *Command Dysfunction: Minding the Cognitive War* (1996) sought to expand on the cognitive components of Command-and-Control Warfare (C2W) but lacked the incorporation of modern neuroscience and technological advancements which have created this still nascent concept.⁴⁹

A recent NATO article defines CogWar as “the activities conducted in synchronization with other instruments of power, to affect attitudes and behaviors by influencing, protecting, and/or disrupting individual and group cognitions to gain an advantage.”⁵⁰ In Nikoula and McMahon describe CogWar as “the use of the means of action that a state or an influential group makes to manipulate the spontaneous mechanisms of the cognition of an enemy or its people, in order to weaken, penetrate, influence, or even subdue or destroy it.”⁵¹

In *Win the War Before the War? A French Perspective on Cognitive Warfare*, Pappalardo refers to CogWar as “a multidisciplinary approach combining social sciences and new technologies to directly alter the mechanisms of understanding and decision-making in order to destabilize or paralyze an adversary.”⁵²

In *The Cognitive Warfare Concept*, Claverie and du Cluzel, define CogWar as an “unconventional form of warfare that uses cyber tools to alter enemy cognitive processes, exploit mental biases or reflexive thinking, and provoke thought distortions, influence decision-making and hinder actions, with negative effects, both at the individual and collective levels.”⁵³

In *Cognitive Warfare: The New Battlefield Exploiting Our Brains*, Claverie defines CogWar as “at the very least a field of research—and probably a way of contributing to the preparation and conduct of war or hostile action—implemented by state or non-state actors. It covers operations aimed at distorting, preventing or annihilating the adversary’s thought processes, situational awareness and decision-making capacity, using a scientific approach and technological, and in particular digital, means.”⁵⁴

In *Cognitive Warfare: The Human Mind as the New Battlefield*, Marjanović and Smiljanić developed a well-researched definition of CogWar using some of the aforementioned works as a basis. In their 2025 published work, the authors define it as “the deliberate use of psychological, informational, and technological tactics to manipulate the cognitive processes of individuals, groups, and societies, such as perception, emotions, beliefs, and decision-making. Targeting the human mind seeks to weaken, influence, or destabilize the intended audience by undermining trust, cohesion, and autonomy, often without relying on physical force.”⁵⁵

In *Towards a Definition of Cognitive Warfare*, Morelle, Marion, Cegarra, and Andre define CogWar as “an emerging concept aiming to weaken the enemy in order to gain a tactical or strategic advantage, in the military, economics, gaming, sports and other fields. It encompasses various operations carried out against the human mind, targeting both individual and collective cognition and decision-making.”⁵⁶ Their citation builds upon the previous definitions of Claverie and du Cluzel.

In *The Changing Character of Warfare: Cognitive Warfare or 21st Century Subversion*, Dr. Frank Hoffman defines CogWar as “the application of targeted and tailored messages and nonviolent methods used against decision-makers or a population to influence, dislocate or paralyze governments, military leaders, and civil society in order to gain

a positional advantage in the cognitive domain or gain desired political and informational outcomes by dissuasion or subversion.”⁵⁷

Differences and Distinctions from Other Terms

Perhaps the most complete attempt at a taxonomy of CogWar and its relation to other terms such as information warfare and psychological warfare comes from Ibrahim, Rhode, and Daseking. In *A Systematic Review of Cognitive and Psychological Warfare*, the authors provide a thorough review of the definitions and relational context of CogWar, information warfare, and psychological warfare by applying Lasswell’s “model of communications.” Their well-researched and thoughtful paper offers clarity — “Cognitive Warfare is a more expanded concept of psychological warfare. Psychological warfare focuses on the perceptions, thoughts, and feelings of human agents to affect the psychology of human actors. Cognitive warfare is a concept that has evolved a step beyond psychological warfare, focusing on the occupation of human cognition to ultimately impact human acts.”⁵⁸

In this exploration of the extant literature it is apparent that there is a need to continue to evaluate the terminology and taxonomy of CogWar. In *Cognitive Warfare: Beyond Dominance, Maneuvers, and Information*, Pripoe-Șerbănescu makes a bold case that the term CogWar itself may be a misnomer. Pripoe-Șerbănescu posits that cognition is “only a fraction of mental activity, subordinated to other higher psychological processes, all definitions centered around the word cognition are at least partial, if not misleading.” He continues to assert this claim by stating that “escaping from the cognitive spell is essential to catch up with the enemy’s refined knowledge and efficiency in informational-psychological warfare.”⁵⁹

Pripoe-Șerbănescu offers another approach based on Friston’s active inference theory and Solms’

theory on consciousness to provide a more accurate reflection of the complexities of CogWar.⁶⁰ He offers the novel interpretation of CogWar as “all forms of influence that are purposely designed to alter the precision optimization mechanism.” This model breaks from the theoretical cognitivist view, where individuals passively receive external stimuli, to a new model that focuses more on the inference process and the targets active generation of hypotheses and predictions based on “affects and mental fantasies.”⁶¹ This follows the claims made earlier in this article about the power of social context in creating perceptions and therefore, meaning in the world.

Pripoea-Şerbănescu’s claims of the enemy’s more advanced understanding of CogWar is supported by Takagi in *New Tech, New Concepts: China’s Plans for AI and Cognitive Warfare*. Takagi refers to the PRC’s development of the term “intelligentized warfare.” China has made clear that the goal of this intelligentized warfare is to control the enemy’s will through intelligence dominance and using AI to directly control decision makers and citizens.⁶²

In summarizing the current state of research on the definition of CogWar, and its relation to other forms of non-kinetic warfare, three distinct schools of thought dominate in describing CogWar, including that it is:

- an entirely new form of warfare, separate and apart from information and psychological operations of the past,
- a new term used to encapsulate multiple existing domains of non-kinetic warfare, and
- itself a subset of a higher taxonomy of psychological warfare.

EVOLUTION AND DOMAINS OF COGWAR

Cognitive warfare has existed throughout human history in various forms and functions. Its character has changed with the advent of new technologies and social systems that catalyze the core concepts of deception, disruption, and manipulation. The following section seeks to contextualize modern CogWar, characterized by civilization’s rapid expansion and interconnectedness through the various industrial and technological revolutions of the 20th and 21st centuries.

Beginning with Clack and Johnson, in *The World Information War: Western Resilience, Campaigning, and Cognitive Effects*, they form a succinct characterization of the historical context of CogWar. Clack and Johnson note Sun Tzu’s famous principle of subduing the enemy without fighting as a demonstration of “supreme excellence.”⁶³ They reference Machiavelli’s use of “men who are discontented and desirous for change...to open the way for the invasion of their country and to render its conquest easy.”⁶⁴ Clack and Johnson also reference Clausewitz’s description of “direct political repercussions, that are designed in the first place to disrupt the opposing alliance, or paralyze it, that gain us new allies, favorably affect the political scene.”⁶⁵

Research suggests that CogWar is a “historical descendant” of the term psychological warfare. In *A Systematic Review of Cognitive and Psychological Warfare*, the authors lay out Sun Tzu’s overarching concepts of stratagem, Fuller’s 1920 conception of the term psychological warfare, the term information warfare’s 1966 adoption by the U.S. military, and the subsequent mainstream adoption of the term CogWar circa 2017.⁶⁶

Cognitive warfare takes place across many domains and battlefields. It changes with the advent of new technologies and adapts to naturally

occurring cultural and societal shifts. Its overall intent is to manipulate, compel, and fracture the human psyche of perception by whatever means available. The future of CogWar will be defined by the rapid expansion of artificial intelligence technologies and creation of new disruptive technologies that could further exploit the human mind. In the *Handbook of the Future of Warfare* Coker states, “most technologies that will dominate life have not yet been invented and that the technologies we are already using will only continue to be useful through constant upgrades.”⁶⁷ New technologies such as AI will enhance the generation of information operations through leveraging its computing power to formulate individualized target packages.⁶⁸ It is easy to see how these technologies could be used for the continuous exploitation of the asymmetry between democracies and authoritarian regimes.⁶⁹

Information Operations

The battle for information and its subsequent use in information operations campaigns is an original form of CogWar. Methods of communication such as music, newspapers, radio, digital advertisements, and news media throughout history have been used for the purposes of cognitive manipulation and control. The battle for information in CogWar consists of not only controlling the dissemination of information (both externally and internally) but also falsifying and fabricating information through information operations campaigns. The goal of information operations is to distract, demoralize, discredit, deceive, divide, deny, dislocate expectations, and destroy from within.⁷⁰

In *Active Measures: The Secret History of Disinformation and Political Warfare*, Thomas Rid makes three arguments. First, that disinformation campaigns are an attack on a liberal political system that entrusts its truths to “custodians of factual authority;” second, that after WWII the West maintained equivalence to its Eastern counterparts in the

pace of disinformation campaigns for only 10 years; and third, that the digital revolution fundamentally altered disinformation campaigns by making them cheaper, quicker, more reactive, and less risky.⁷¹

Rid provides an extensive review of information operations and propaganda campaigns with a focus on Soviet/Russian tactics and methodologies. The term active measures, or *aktivnye meropriyatiya*, originated from Soviet/Russian influence operations dating back to the 1920s.⁷² Those influence operations during the Cold War were designed to achieve the end states of a CogWar campaign, i.e., the downfall of an adversary government.

PSYCHOLOGICAL OPERATIONS

Psychological warfare is defined as “the deliberate utilization of communication strategies, encompassing both online and offline mediums, orchestrated by predominantly anonymous actors to manipulate and destabilize primarily unspecified recipients, both in times of warfare and peace.”⁷³ The three central effects of psychological warfare are: influencing the enemy’s cognitive processes, influencing the enemy’s behavior, and influencing friendly cognitive processes and behaviors.⁷⁴

In *Cognitive Centric Warfare: Modelling Indirect Approach in Future Warfare*, Takagi speaks on the battle of wills and psychological disposition of the enemy. Takagi reminds us that cognition is a fundamental aspect of victory and defeat. The enemy must recognize that “he or she has lost the war” as a requirement for an end to war.⁷⁵ He points out that with the exception of societies like the Carthaginians, very rarely are enemy populations completely eradicated.⁷⁶ There exists a necessary determination by both parties to accept the outcome as defeat or victory and move forward into new phases of political discourse or acceptance. This follows Sun Tzu’s philosophy of preserving the enemy’s resources for future exploitation and use. The outcome of a CogWar campaign would be to subjugate

the enemy combatants and have them conform to the new world order of their defeat.

One extreme example of this is the story of Kanji Tsuda Onoda, a Japanese soldier who evaded capture and maintained his orders of resistance for thirty years in the Philippine jungle after WWII. Onoda's orders were simple, remain and resist at all costs until relieved. Onoda refused countless attempts by Japanese and Philippine officials to convince him that the war was over. Japanese delegates made contact on several occasions with photos and letters from family pleading for Onoda to come home. Onoda was convinced these were fake. It would not be until 1974 that Onoda's former commanding officer would personally travel to the jungles of Lubang to officially relieve him.⁷⁷ As illustrated by Onoda's extreme example, victory and defeat are ultimately determined in the cognitive domain.

Cyber Operations

In *Aspects of Cognitive Warfare*, Matthias Wasinger states that "Cyberspace has essentially facilitated the creation of a more potentially transparent human society. Digitalization and the everyday use of cyberspace have turned this virtual domain into a place of actual consequence, a diplomatic tool, an economic factor, a military effector and a social space satisfying the human need for social connectivity. . . ."⁷⁸ This signals a shift in social dynamics that suggests that ownership of influence and connectivity in the digital realm could possibly hold more value than geography and actual, physical property. The long-term impact of Cryptocurrency, such as Bitcoin, will provide insight into the influence and feasibility of this shift in social dynamics.

One of the courses of action in a CogWar would focus on the exploitation and control of mass communication techniques such as social media, data, and cyber-information with the goal of interfering with the mind and its ability to interpret

neurological stimuli.⁷⁹ Cognitive warfare in the cyber realm differs from other, more traditional forms of cyber warfare that target the hardware and software of digital infrastructure. Cognitive warfare in cyberspace stands to control and manipulate information and other stimuli to target individuals and groups to alter their perceptions of events occurring or about to occur in the world. In other words, in a CogWar, cyber will play a major role in creating the context that a target audience uses in making sense of the available data about an adversary's intent and conduct.

Artificial Intelligence

The information and research regarding AI's role in CogWar is limited and mainly futuristic in nature. Even more advanced forms of AI could achieve human-like reasoning, such as Artificial General Intelligence (AGI) and Artificial Superintelligence (ASI), may not have significant impacts for the next 20 years, according to Christopher Coker in *Thinking About the Future of Warfare*.⁸⁰ The most likely case for AI's role in CogWar for the immediate future is one that focuses on leveraging modern computing to mine data in "algorithmic cognitive warfare," generating large amounts of fake video and imagery and managing bot armies in influence campaigns.⁸¹ In effect, AI could instantly create computational propaganda.

"Algorithmic Cognitive Warfare" was coined by the PRC in 2022 in response to witnessing the battle for narrative between Russia and Ukraine and the relevant need for exponential gains in the computing-CogWar relationship.⁸² In *Decoding China's AI Powered "Algorithmic Cognitive Warfare,"* Lindsey Lange offers a review of this concept by examining a theoretical model for algorithmic CogWar and positing a hypothetical data pipeline.⁸³

CHEMICAL/BIOLOGICAL/ NEUROSCIENCE

Modern neuroscience has illuminated many vulnerabilities in the human brain as presented previously in this article. Dr. James Giordano is a leading researcher and author of *Battlescape Brain: Engaging Neuroscience in Defense Operations*. In that book, Dr. Giordano explores a wide variety of current and future technologies that have neurological effects ranging from well-known drugs and organic toxins to advanced nano-particulate agents and neuromodulator technologies. Giordano provides four categories of weaponizable neuroscience technologies: pharmacological agents, microbial agents, organic toxins, and neurotechnology.⁸⁴

Giordano's exploration of neurotechnology presents startling possibilities for the coming decades. Cognitive warfare, which relies on perception and processing patterns in the human mind, may have new distinct characteristics resulting from direct interaction and interference with neural networks to disrupt the human brain by force, thus changing human perceptions through the direct use of neurotechnology.

WORKSHOP INSIGHTS

Winning and Losing in Cognitive War

Throughout the workshop conducted in May 2025, the discussion focused on the implications of CogWar as the presenters defined it in today's context and into the future. One participant posed a particular dilemma in which CogWar of the past relied on thinking errors and distortions of cognition . . . but CogWar in the future may rely more heavily on mechanical and chemical manipulation of the mind. He also spoke on the implications of big data and its use in creating tailored "targeting packages." Specifically, he was concerned with how medical and other confidential information could be used to

develop effective CogWar campaigns.

Another presenter made no concessions when illustrating the pacing threat that China poses in CogWar. He stated, "I think we lost." He seemed sincerely alarmed and troubled by the existing U.S. response to this issue. Others disagreed, pointing out that U.S. ongoing efforts to counter and engage in CogWar do not indicate that "we lost."

There were also advocates for a simple and clear response matrix for decision makers. They stressed the lack of concise and direct understanding of responses to CogWar operations, as well as the need for a common language to discuss the effects of CogWar campaigns.

Another participant brought to light what he saw as a shift in the conduct of war that was now impacting more and more non-military targets. He spoke about the four faces of war (societal, conventional, cognitive, and proxy). He stated that we are swimming in a soup of words and definitions regarding CogWar, while admitting that, after participating in the workshop discussions, he realized that his own existing definition of CogWar was obsolete.

Matters of Consensus

There was consensus that there is an urgent need for policymakers and senior officials to be made aware of CogWar. A sense of concern over the apparent pacing threat posed by near peers such as China and Russia in the cognitive space was also very evident. There was agreement that the unique origins and impacts of CogWar make it distinct from other forms of warfare and other domains of warfare. The participants believed that establishing the human cognitive processes as a domain was a necessary first step in developing a broader understanding of its power to influence the strategic outcomes of conflicts.

Gaps in Research

One participant stated that it was critical that we build an understanding of how to rehabilitate a group who had already been successfully targeted by a CogWar campaign. He asked if any victory is forever. Another stated that there is a lack of research in the development of “blue/friendly” applications with appropriate policy guidelines. All agreed that further research was needed to understand how Western democracies can deter, defend, and combat against authoritarian nations engaged in CogWar. A question to be answered, which grew out of the workshop as “What inherent characteristics make cognitive warfare more or less effective against or by different governing structures in individual nations?”

RECOMMENDATIONS FOR FUTURE RESEARCH

The current body of research offers differing perspectives on CogWar. However, they are predominantly focused on the tactics of CogWar and in the same way that the study of a rifle falls short of understanding battles or wars, they fall short of providing a complete explanation of CogWar. Ultimately, defending against and succeeding in CogWar begins with understanding the operating logic inherent in a CogWar campaign. This is done first generically, in the framework identified in this research and then specifically, in the context of operations against a particular adversary.

Recommendations for future research are as follows:

- Begin with an in-depth evaluation of CogWar through a Clausewitzian lens, since this is the lens through which most senior decisionmakers view war—whether they are conscious of it or not.
- Formulate a new definition of CogWar and one that holistically captures the campaign-like characteristics of CogWar.
- Conduct a wargame, with participants teamed with an AI would greatly benefit our collective understanding of the practical application of CogWar, as well as the practical application of AI.
- Identify organizational options for DOW to be better positioned to counter adversary CogWar initiatives and potentially to plan and execute a CogWar campaign.
- Examine current active CogWar campaigns against U.S. targets to appreciate the scale and scope of the challenge.
- Define existing U.S. CogWar capabilities—are they sufficient to counter the threats? Could those capabilities be structured in such a way within the civilian, military, and private sectors to achieve maximum effect? **PRISM**

Notes

¹ Cambone, Stephen and Robert Schmidle, “Organizing for 21st Century Warfare” (unpublished manuscript, 2023).

² Naganuma Kazumi, “Warfare in the Cognitive Domain: Narrative, Emotionality, and Temporality,” *The National Institute for Defense Studies Commentary No. 163*, March 30, 2021. <https://www.nids.mod.go.jp/english/publication/commentary/pdf/commentary163e.pdf>.

³ Fathali M. Moghaddam and Robert Schmidle, “A Narrative Societies-to-Cells Perspective on Cognitive Warfare” (unpublished manuscript, n.d.)

⁴ NATO Science & Technology Organization (STO), eds., *Proceedings of the First NATO Scientific Meeting on “Cognitive Warfare”* (Bordeaux, France, June 21, 2021), NATO STO, 2021.

⁵ Bernard Claverie and François du Cluzel, *The Cognitive Warfare Concept*, NATO Innovation Hub (Norfolk, VA, December 2023).

⁶ Dmitry Khodyakov, “Generating Evidence Using the Delphi Method,” *Integration and Implementation Insights*, October 16, 2023, <https://i2insights.org/2023/10/17/delphi-method/>.

⁷ Jim Giordano et al., “What is Cognitive Warfare?” (presentation, Barrett & O’Connor Center, Arizona State University, Washington, DC, May 20, 2025).

⁸Ludwig Wittgenstein, *Philosophical Investigations*, trans. G. E. M. Anscombe, P. M. S. Hacker, and Joachim Schulte, revised 4th ed. (Chichester, West Sussex: Wiley-Blackwell, 2009), §43.

⁹“APA Dictionary of Psychology,” n.d., <https://dictionary.apa.org/cognition>.

¹⁰Lera Boroditsky, “Does Language Shape Thought?: Mandarin and English Speakers’ Conceptions of Time,” Stanford University. 2001. http://www.cogsci.bme.hu/~ktkuser/KURZUSOK/BMETE47MC15/2018_2019_1/boroditsky2001.pdf.

¹¹Michael E. W. Varnum, Igor Grossmann, Shinobu Kitayama, Richard E Nisbett. “The Origin of Cultural Differences in Cognition,” *Current Directions in Psychological Science* 19, no. 1 (February 1, 2010): 9–13, <https://doi.org/10.1177/0963721409359301>.

¹²Genia Kostka, “China’s Social Credit Systems and Public Opinion: Explaining High Levels of Approval,” *New Media & Society* 21, no. 7 (February 13, 2019): 1565–93, <https://doi.org/10.1177/1461444819826402>.

¹³Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 75.

¹⁴Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), Book III, Chapter III, 178.

¹⁵Michael E. W. Varnum, Igor Grossmann, Shinobu Kitayama, and Richard E. Nisbett, “The Origin of Cultural Differences in Cognition: Evidence for the Social Orientation Hypothesis,” *Current Directions in Psychological Science* 19, no. 1 (2010): 9–13.

¹⁶Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 75.

¹⁷Amber BrittainHale, “Clausewitzian Theory of War in the Age of Cognitive Warfare” (December 14, 2023), in *Clausewitzian Theory Of War In The Age Of Cognitive Warfare*, Pepperdine University Digital Commons, accessed July 17, 2025.

¹⁸Amber BrittainHale, “Clausewitzian Theory of War in the Age of Cognitive Warfare” (December 14, 2023), in *Clausewitzian Theory Of War In The Age Of Cognitive Warfare*, Pepperdine University Digital Commons, accessed July 17, 2025.

¹⁹Amber BrittainHale, “Clausewitzian Theory of War in the Age of Cognitive Warfare” (December 14, 2023), in *Clausewitzian Theory Of War In The Age Of Cognitive Warfare*, Pepperdine University Digital Commons, accessed July 17, 2025.

²⁰David Pappalardo, “Win the War Before the War?: A French Perspective on Cognitive Warfare,” *War on the Rocks*, August 1, 2022, accessed July 17, 2025.

²¹David Pappalardo, “Win the War Before the War?: A French Perspective on Cognitive Warfare,” *War on the Rocks*, August 1, 2022, accessed July 17, 2025.

²²Peter B.M.J. Pijpers, “On Cognitive Warfare: The Anatomy of Disinformation,” TDHJ.org, April 3, 2024, <https://tdhj.org/blog/post/on-cognitive-warfare-the-anatomy-of-disinformation/>.

²³Woolley, Samuel C., and Philip N. Howard. *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*. Oxford: Oxford University Press, 2018.

²⁴Renée DiResta, “Computational Propaganda: If You Make It Trend, You Make It True,” *The Yale Review* 106, no. 4 (October 2018): 12–29, <https://doi.org/10.1111/yrev.13402>.

²⁵James Giordano, “Battlescape Brain: Military and Intelligence Use Of Neurocognitive Science,” n.d., https://www.usna.edu/NewsCenter/sites/Ethics/Dr._James_Giordano_Battlescape_Brain_Military_and_Intelligence_Use_of_Neurocognitive_Science.php.

²⁶James Giordano, “Battlescape Brain: Military and Intelligence Use Of Neurocognitive Science,” n.d., https://www.usna.edu/NewsCenter/sites/Ethics/Dr._James_Giordano_Battlescape_Brain_Military_and_Intelligence_Use_of_Neurocognitive_Science.php.

²⁷James Giordano, “Battlescape Brain: Engaging Neuroscience in Defense Operations–HDIAC,” Homeland Defense & Security Information Analysis Center, May 13, 2021, <https://hdiac.dtic.mil/articles/battlescape-brain-engaging-neuroscience-in-defense-operations/>.

²⁸Jonathan D. Moreno, Michael Tennison, and James Giordano, “Security Threats Versus Aggregated Truths: Ethical Issues in the Use of Neuroscience and Neurotechnology for National Security,” in *Neuroethics: Anticipating the Future*, ed. Judy Illes (New York: Oxford University Press, 2017).

²⁹DeFranco, Joseph, and Diane DiEuliis, L.R. Bremseth, James Giordano, MPhil. “WMD Threat Analysis: Emerging Technologies For Disruptive Effects in Non-Kinetic Engagements.” Homeland Defense & Security Information Analysis Center. August 29, 2019.

³⁰DeFranco, Joseph, and Diane DiEuliis, L.R. Bremseth, James Giordano, MPhil. “WMD Threat Analysis: Emerging Technologies For Disruptive Effects in Non-Kinetic Engagements.” Homeland Defense & Security Information Analysis Center. August 29, 2019.

³¹DeFranco, Joseph, and Diane DiEuliis, L.R. Bremseth, James Giordano, MPhil. “WMD Threat Analysis: Emerging Technologies For Disruptive Effects in Non-Kinetic Engagements.” Homeland Defense & Security Information Analysis Center. August 29, 2019.

- ³² DeFranco, Joseph, and Diane DiEuliis, L.R. Bremseth, James Giordano, MPhil. “WMD Threat Analysis: Emerging Technologies For Disruptive Effects in Non-Kinetic Engagements.” Homeland Defense & Security Information Analysis Center. August 29, 2019.
- ³³ DeFranco, Joseph, and Diane DiEuliis, L.R. Bremseth, James Giordano, MPhil. “WMD Threat Analysis: Emerging Technologies For Disruptive Effects in Non-Kinetic Engagements.” Homeland Defense & Security Information Analysis Center. August 29, 2019.
- ³⁴ Albert Einstein, *Relativity: The Special and the General Theory* (New York: Crown Publishers, 1961), 35–36.
- ³⁵ Werner Heisenberg, *Physics and Philosophy: The Revolution in Modern Science*, trans. Arnold J. Pomerans (New York: Harper & Row, 1958), 58.
- ³⁶ Werner Heisenberg, *Physics and Philosophy: The Revolution in Modern Science*, trans. Arnold J. Pomerans (New York: Harper & Row, 1958), 58.
- ³⁷ Ludwig Wittgenstein, *Tractatus Logico-Philosophicus*, trans. C.K. Ogden (London: Routledge & Kegan Paul, 1922), 89.
- ³⁸ Ludwig Wittgenstein, *Philosophical Investigations*, trans. G.E.M. Anscombe (Oxford: Blackwell, 1953), §§ 23–4
- ³⁹ Michel Foucault, *Discipline and Punish: The Birth of the Prison*, trans. Alan Sheridan (New York: Vintage Books, 1995), 27.
- ⁴⁰ Michel Foucault, in *Truth and Power*, in *Power/Knowledge: Selected Interviews and Other Writings, 1972–1977*, edited by Colin Gordon (Brighton: Harvester Press, 1980), p. 131.
- ⁴¹ Michel Foucault, “Truth and Power,” in *Power/Knowledge: Selected Interviews and Other Writings, 1972–1977*, ed. Colin Gordon, trans. Colin Gordon et al. (Brighton: Harvester Press, 1980), 131.
- ⁴² Leon Festinger, *A Theory of Cognitive Dissonance* (Stanford, CA: Stanford University Press, 1957), 3–5.
- ⁴³ Harré, Rom and Fathali M. Moghaddam, eds., *Psychology for the Third Millennium: Integrating Cultural and Neuroscience Perspectives* (Thousand Oaks, CA: SAGE Publications, 2012).
- ⁴⁴ Harré, Rom and Fathali M. Moghaddam, eds., *Psychology for the Third Millennium: Integrating Cultural and Neuroscience Perspectives* (Thousand Oaks, CA: SAGE Publications, 2012).
- ⁴⁵ Moghaddam, Fathali M. and Robert Schmidle, “A Narrative Societies-to-Cells Perspective on Cognitive Warfare” (unpublished manuscript, n.d.), 11.
- ⁴⁶ Ilya Yablokov and Precious N. Chatterje-Doody, *Russia Today and Conspiracy Theories: People, Power and Politics on RT* (Abingdon, Oxon: Routledge, 2021).
- ⁴⁷ Moghaddam, Fathali M. and Robert Schmidle, “A Narrative Societies-to-Cells Perspective on Cognitive Warfare” (unpublished manuscript, n.d.), 11.
- ⁴⁸ Ibrahim, Fabio, Steffen Rhode, and Monika Daseking, “A Systematic Review of Cognitive and Psychological Warfare,” *The Defence Horizon Journal*, April 9, 2024, <https://tdhj.org/blog/post/cognitive-psychological-warfare/>.
- ⁴⁹ Arden B. Dahl, *Command Dysfunction: Minding the Cognitive War* (Maxwell Air Force Base, AL: Air University Press, 1998), accessed July 17, 2025, https://archive.org/details/DTIC_ADA360756.
- ⁵⁰ NATO Strategic Communications Centre of Excellence, “What Is Cognitive Warfare?” *NATO StratCom COE*, May 2022, accessed July 17, 2025, <https://www.stratcomcoe.org/what-cognitive-warfare>.
- ⁵¹ Nikoula, Christos and David McMahon, “Cognitive Warfare: Securing Hearts and Minds,” (Center for Strategic and International Studies, February 2023), accessed July 17, 2025, <https://www.csis.org/analysis/cognitive-warfare-securing-hearts-and-minds>.
- ⁵² David Pappalardo, “Win the War Before the War?: A French Perspective on Cognitive Warfare,” *War on the Rocks*, August 1, 2022, accessed July 17, 2025, <https://warontherocks.com/2022/08/win-the-war-before-the-war-a-french-perspective-on-cognitive-warfare/>.
- ⁵³ Clavrie, Yves and Antoine du Cluzel, *The Cognitive Warfare Concept*, (Paris: Fondation pour la Recherche Stratégique, 2021), accessed July 17, 2025, <https://www.frstrategie.org/en/publications/cognitive-warfare-concept-2021>.
- ⁵⁴ Clavrie, Yves and Antoine du Cluzel, *The Cognitive Warfare Concept*, (Paris: Fondation pour la Recherche Stratégique, 2021), accessed July 17, 2025, <https://www.frstrategie.org/en/publications/cognitive-warfare-concept-2021>.
- ⁵⁵ Marjanović, Aleksandar and Dražen Smiljanić, “Cognitive Warfare – The Human Mind as the New Battlefield,” *Proceedings of the Defence and Security Conference 1*, no. 1 (2025): 84–114, accessed July 17, 2025, https://www.researchgate.net/profile/Drazen-Smiljanic/publication/391704397_Cognitive_warfare_-_the_human_mind_as_the_new_battlefield/links/6823c136d1054b0207eeb4c7/Cognitive-warfare-the-human-mind-as-the-new-battlefield.pdf?cf_chl_tk=.O01fqj0cQPRvjSDggncfIw77xZBbMocolyIxFNG1w-1764780488-1.0.1.1-gzdOPGK1UhW.ctgkGedIFZ8zBSUDfyrW3iQwL82McI4.

⁵⁶ Morelle, Marie, Cegarra Julien, Damien Marion, André Jean-Marc. Towards a Definition of Cognitive Warfare. Conference on Artificial Intelligence for Defense, DGA Maitrise de l'Information, Nov 2023, Rennes, France. 'hal-04328461'

⁵⁷ Frank Hoffman, "The Changing Character of Warfare: Cognitive Warfare or 21st Century Subversion," PowerPoint presentation, 2025. Personal Communication.

⁵⁸ Ibrahim, Fouad, Steffen Rhode, and Markus Daseking, "A Systematic Review of Cognitive and Psychological Warfare," *TDHJ.org*, April 9, 2024, accessed July 17, 2025, <https://tdhj.org/blog/post/cognitive-psychological-warfare/>.

⁵⁹ Ciprian PRIPOAE-ȘERBĂNESCU, "Cognitive Warfare: Beyond Dominance, Maneuvers, and Information," Romanian Military Thinking 2024, accessed July 17, 2025, <https://en-gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20reviste/RMT/2023/proceedings/PRIPOAE-SERBANESCU.pdf>.

⁶⁰ Ciprian PRIPOAE-ȘERBĂNESCU, "Cognitive Warfare: Beyond Dominance, Maneuvers, and Information," Romanian Military Thinking 2024, accessed July 17, 2025, <https://en-gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20reviste/RMT/2023/proceedings/PRIPOAE-SERBANESCU.pdf>.

⁶¹ Ciprian PRIPOAE-ȘERBĂNESCU, "Cognitive Warfare: Beyond Dominance, Maneuvers, and Information," Romanian Military Thinking 2024, accessed July 17, 2025, <https://en-gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20reviste/RMT/2023/proceedings/PRIPOAE-SERBANESCU.pdf>.

⁶² Kazuhiro Takagi, "New Tech, New Concepts: China's Plans for AI and Cognitive Warfare," War on the Rocks, April 15, 2022, accessed July 17, 2025, <https://warontherocks.com/2022/04/new-tech-new-concepts-chinas-plans-for-ai-and-cognitive-warfare/>.

⁶³ Clack, T. and R. Johnson, The World Information War: Western Resilience, Campaigning, 2021, accessed July 17, 2025, <https://www-taylorfrancis-com.ezproxy1.lib.asu.edu/reader/download/5e7e1450-27ab-4ed5-ad71-0353f16ea68e/book/pdf?context=ubx>.

⁶⁴ Clack, T. and R. Johnson, The World Information War: Western Resilience, Campaigning, 2021, accessed July 17, 2025, <https://www-taylorfrancis-com.ezproxy1.lib.asu.edu/reader/download/5e7e1450-27ab-4ed5-ad71-0353f16ea68e/book/pdf?context=ubx>.

⁶⁵ Clack, T. and R. Johnson, The World Information War: Western Resilience, Campaigning, 2021, accessed July 17, 2025, <https://www-taylorfrancis-com.ezproxy1.lib.asu.edu/reader/download/5e7e1450-27ab-4ed5-ad71-0353f16ea68e/book/pdf?context=ubx>.

⁶⁶ Ibrahim, Fouad, Steffen Rhode, and Markus Daseking, "A Systematic Review of Cognitive and Psychological Warfare," *TDHJ.org*, April 9, 2024, accessed July 17, 2025, <https://tdhj.org/blog/post/cognitive-psychological-warfare/>.

⁶⁷ Christopher Coker, Routledge Handbook of the Future of Warfare, Thinking About the Future of Warfare, PDF, 2024, accessed July 17, 2025.

⁶⁸ Peter B.M.J. Pijpers, "On Cognitive Warfare: The Anatomy of Disinformation," *TDHJ.org*, April 3, 2024, accessed

July 17, 2025, <https://tdhj.org/blog/post/on-cognitive-warfare-the-anatomy-of-disinformation/>.

⁶⁹ Peter B.M.J. Pijpers, "On Cognitive Warfare: The Anatomy of Disinformation," *TDHJ.org*, April 3, 2024, accessed July 17, 2025, <https://tdhj.org/blog/post/on-cognitive-warfare-the-anatomy-of-disinformation/>.

⁷⁰ Burke, Paul and Adam Henschke, "I Know My Truth... Now Tell Me Yours: From Active Measures to Cognitive Warfare in the Russian Invasion of Ukraine," NISS Panorama, 2022, accessed July 17, 2025, <https://niss-panorama.com/index.php/journal/article/view/141/141>.

⁷¹ Thomas Rid, Active Measures: The Secret History of Disinformation and Political Warfare (New York: Farrar, Straus and Giroux, 2020), 10–12.

⁷² Thomas Rid, Active Measures: The Secret History of Disinformation and Political Warfare (New York: Farrar, Straus and Giroux, 2020), 28.

⁷³ Ibrahim, Fouad, Steffen Rhode, and Markus Daseking, "A Systematic Review of Cognitive and Psychological Warfare," *TDHJ.org*, April 9, 2024, accessed July 17, 2025, <https://tdhj.org/blog/post/cognitive-psychological-warfare/>.

⁷⁴ Ibid.

⁷⁵ Koichiro Takagi, Cognitive Centric Warfare: Modelling Indirect Approach in Future Warfare, Hudson Institute, June 13, 2025, accessed July 17, 2025, <https://www.hudson.org/corruption/cognitive-centric-warfare-modelling-indirect-approach-future-warfare-koichiro-takagi>.

⁷⁶ Ibid.

⁷⁷ David Langbart, "Onoda of the Jungle," The Text Message (National Archives Blog), May 25, 2023, accessed July 17, 2025, <https://text-message.blogs.archives.gov/2023/05/25/onoda-of-the-jungle/>.

⁷⁸ Matthias Wasinger, Aspects of Cognitive Warfare: Then We Will Fight in the Shade, 2024, accessed July 17, 2025, <https://tdhj.org/blog/post/military-comprehensive-approach>.

⁷⁹ Alida Monica Doriana Barbu, China's Cognitive Warfare for the Peaceful Recovery of Taiwan, 2025, accessed July 17, 2025, <https://www.cceol.com/search/viewpdf?id=1391646>.

⁸⁰ Christopher Coker, Routledge Handbook of the Future of Warfare, Thinking About the Future of Warfare, PDF, 2024, accessed July 17, 2025.

⁸¹ Lindsey Lange, Decoding China's AI-Powered "Algorithmic Cognitive Warfare", 2024, accessed July 17, 2025, <https://www.scsp.ai/wp-content/uploads/2024/11/Decoding-Chinas-AI-Powered-%E2%80%98Algorithmic-Cognitive-Warfare-Final.pdf>.

⁸² Lindsey Lange, Decoding China's AI-Powered "Algorithmic Cognitive Warfare" (Special Competitive Studies Project, 2024), accessed July 17, 2025, <https://www.scsp.ai/wp-content/uploads/2024/11/Decoding-Chinas-AI-Powered-%E2%80%98Algorithmic-Cognitive-Warfare-Final.pdf>.

⁸³ Ibid.

⁸⁴ James Giordano, "Battlescape Brain: Engaging Neuroscience in Defense Operations," HDIAC, May 13, 2021, accessed July 17, 2025, <https://hdiac.dtic.mil/articles/battlescape-brain-engaging-neuroscience-in-defense-operations/>.

Medical Intelligence in Support of Irregular Warfare

By 2LT Ryan M. Leone, CAPT (Dr.) Mason H. Remondelli, 2LT Victoria M. Perez, 2LT Kirsten Lalli, Lt. Col (Dr.) Regan F. Lyon, Dr. Jay B. Baker, Dr. Dan Hanfling, Col (Dr.) Ronald D. Hardin, MAJ Robert G. Cockerham, Dr. Derek J. Licina (Col, retired)

Second Lieutenant Ryan M. Leone served as a Presidential Management Fellow at the Defense Health Agency and Department of State and is currently a fourth-year medical student at Columbia University while serving in the U.S. Army.

Captain (Dr.) Mason H. Remondelli graduated from the United States Military Academy and the Uniformed Services University and is currently a first-year U.S. Army general surgery resident at Walter Reed National Military Medical Center.

Second Lieutenant Victoria M. Perez served as an Air Force intelligence officer after graduating from the U.S. Air Force Academy and is currently a fourth-year medical student at the Uniformed Services University while serving in the U.S. Air Force.

Second Lieutenant Kirsten Lalli served as an intelligence officer and federal agent for the Department of Defense and is currently a fourth-year medical student at Yale School of Medicine while serving in the U.S. Army.

Lieutenant Colonel (Dr.) Regan F. Lyon is a U.S. Air Force emergency medicine physician who previously served on an Air Force Special Operations Surgical Team and within the office of the Assistant Secretary of Defense for Special Operations/Low Intensity Conflict and is now a squadron commander.

Dr. Jay B. Baker is an emergency medicine physician and retired U.S. Army Colonel who previously served in various global assignments, including time within the Special Operations community, and is currently an American Tech Fellow at Palantir.

Dr. Dan Hanfling is an emergency medicine physician who previously served at the White House Office of Pandemic Preparedness and Response Policy, in addition to time at In-Q-Tel and the Department of Health and Human Services, who is currently a Clinical Professor at George Washington University.

Colonel (Dr.) Ronald D. Hardin is a U.S. Army trauma surgeon with numerous deployments on a surgical team in support of Special Operations missions who currently serves as the Trauma Medical Director for the US Special Operations Command.

Major Robert G. Cockerham has served in conventional, interagency and Special Operations assignments, and is currently a U.S. Army operations officer in the Joint Medical Unit.

Dr. Derek J. Licina is a retired U.S. Army Colonel who served in various roles within the Department of Defense, consulting, and academia leading global health efforts, and is currently a senior advisor with the U.S. Department of Defense Joint Trauma System and Adjunct Professor of Global Health at The George Washington University.

In the rapidly shifting landscape of global conflict, irregular warfare (IW) is increasingly central to modern military operations, especially against near-peer and peer adversaries. As nations prepare for future wars that blend conventional and unconventional tactics, the ability to provide medical support in austere, denied, and high-risk environments becomes crucial for maintaining force effectiveness and survivability. A critical component of this medical support is timely and actionable medical intelligence (MEDINT). Medical intelligence includes information on local health threats, medical infrastructure, and both friendly and adversary medical capabilities. It is essential for both medical providers operating in these complex, hostile settings and commanders who may use this information to mitigate strategic, operational, or tactical risk. As defined in *Joint Publication 4-02, Joint Health Services*, MEDINT entails the “collection, evaluation, and analysis of information concerning the health threats and medical capabilities of foreign countries and non-state actors that have immediate or potential impact on policies, plans, or operations.”¹ It is also integral to the concept of Medical Intelligence Preparation of the Environment (MIPOE) — defined as “the systematic process used by a medical planner to analyze information on medical aspects of disease threats, enemy capabilities, terrain, weather, local medical infrastructure, potential humanitarian and refugee situations, transportation issues, and political, religious and social issues for all types of operations” — which further fits into *Joint Publication 2-01.3, Joint Intelligence Preparation of the Operational Environment*.²

As the U.S. and its partners prepare for IW, Medical Support to Irregular Warfare (MSIW) will be increasingly critical to force protection and sustainment. However, the nature of denied IW environments may limit the timely collection, analysis, and delivery of necessary MEDINT to keep

far-forward medical assets informed. MEDINT, which includes information on friendly and adversary medical assets and current health threats, is invaluable to medical providers who must rapidly adapt resuscitation, stabilization, and evacuation plans to the changing landscape. Barriers, including electronic warfare (EW) and drone targeting of incoming or outgoing signals, may preclude MEDINT from reaching end users.

Special Operations Forces (SOF), frequently tasked with missions deep inside enemy territory, face heightened risks of injury or death. Additionally, future wars may require that conventional units operate in environments traditionally only seen by SOF. As these units push the boundaries of operational reach, medical teams must not only be mobile, adaptable, and resilient but also well-informed by up-to-date MEDINT. The future battlefield will challenge traditional models of medical support, requiring new methods to ensure that frontline medical providers can rapidly adapt to evolving threats and health hazards. However, IW environments are characterized by disrupted communications, EW, and contested lines of movement, all of which can limit the timely delivery of critical MEDINT. This paper explores how the ability to provide MEDINT will shape the effectiveness of MSIW. As unconventional and guerilla medical teams work alongside SOF units, in addition to conventional units, their ability to deliver trauma care and damage control capabilities will depend not only on their medical expertise but also on having the most current MEDINT to anticipate and respond to local health threats and enemy tactics.

Even now, the National Center for Medical Intelligence (NCMI) faces obstacles in providing MEDINT to SOF medics and other healthcare providers on the frontlines, which will be further hampered by the degraded communications and ultra-low signature needs during IW operations. Consequently, by examining historical IW

operations, current conflicts like the Russia-Ukraine war, and advancements in medical technology and intelligence gathering, this paper underscores both the challenges and opportunities associated with integrating MEDINT into far-forward medical operations on future battlefields.

HISTORICAL PERSPECTIVE ON MEDICAL INTELLIGENCE IN IW

The evolution of MEDINT within IW reflects its increasing significance as a strategic tool, vital not only for force health protection but also for shaping operational and tactical decisions in complex combat environments. MEDINT's utility has spanned from disease prevention and force readiness to undermining adversary capabilities, making it an indispensable asset in historical and modern military contexts.

One of the earliest documented instances of MEDINT shaping military outcomes occurred during the Spanish-American War, particularly in the battle against yellow fever. Dr. Walter Reed's discovery that mosquitoes were the vectors for yellow fever dramatically transformed the military's public health approach, initially during the war and later during the construction of the Panama Canal.³ Despite widespread skepticism about Reed's mosquito-borne theory, the intelligence derived from disease vector identification enabled military engineers to protect workers and avoid significant disease-related casualties during construction, demonstrating how epidemiological intelligence could directly affect strategic military objectives.

During World War II (WWII), the role of MEDINT expanded significantly, showcasing the practical application of intelligence to disrupt enemy operations. A well-known case involved the identification of Japanese preference for hypodermic needles over oral preparations. Medical intelligence officers traced the origin of medical supplies, identifying a single factory responsible for producing

these items through labeling analysis. By locating the factory via phonebook records, U.S. forces were able to destroy the facility, effectively cutting off a crucial part of Japan's medical supply chain.⁴ This case illustrates the operational impact of MEDINT in degrading an adversary's medical infrastructure, a tactic that would evolve in subsequent conflicts.

The formal establishment of MEDINT as a distinct field can be traced to WWII when Dr. Edward T. Wolf was dispatched to gather epidemiological data in Northern New Guinea. His mission to understand the local disease landscape proved critical for safeguarding Allied forces operating in the region.⁵ This laid the foundation for developing more structured MEDINT capabilities, which would see rapid expansion in the post-war period. In the Vietnam War, MEDINT capabilities were enhanced with the creation of specialized units like the Walter Reed Army Institute of Research Field Epidemiology Survey Team (WRAIR-FEST), which integrated field-based epidemiological surveys to provide real-time intelligence on disease threats in austere environments. In parallel, physicians were used operationally by the intelligence community, particularly in the Office of Strategic Services (OSS), for clinical and intelligence purposes.⁶

The evolution of MEDINT continued post-WWII, particularly with the establishment of the U.S. Army Medical Intelligence and Information Agency (USAMIIA). However, where WWII saw the implementation of MEDINT as a matter of strategic importance and integrated within military intelligence, the National Security Act of 1947 ushered in the creation of the Central Intelligence Agency (CIA), and with it, uncertainty regarding ownership of MEDINT as an intelligence mechanism.⁷ Despite the Department of War (DOW) and Army Medical Department having the role previously, the Hawley Board, a congressional committee with representatives from both the Army Medical Department and CIA, was unable to reach a consensus. Indeed,

it wasn't until 1982 that the Armed Forces Medical Intelligence Center (AFMIC) was established, later becoming the National Center for Medical Intelligence (NCMI) under the Defense Intelligence Agency (DIA) in 2008. NCMI is currently the lead DOW activity for the production and coordination of medical intelligence, fulfilling the DOW policy mandate that there be a unified defense community for all MEDINT activities in support of national security objectives.⁸ This organizational evolution reflects the increasing recognition of MEDINT's importance in providing actionable intelligence for both military and humanitarian missions.

Post-9/11 operations demonstrated MEDINT's evolving role in counterterrorism efforts. A controversial instance was the use of a vaccination campaign in the hunt for Osama bin Laden.⁹ While the operation was successful in gathering intelligence on bin Laden's whereabouts, it had unintended consequences, including the increased targeting of public health workers and humanitarian organizations such as the Red Cross, as these groups were suspected of collaboration with intelligence agencies. As a result, the U.S. intelligence community implemented policies prohibiting the use of healthcare workers and Peace Corps volunteers in intelligence-gathering operations.¹⁰ This case highlights the delicate balance MEDINT must maintain between operational objectives and the broader implications for global health trust.¹¹

In more recent years, MEDINT has been leveraged to target terrorist organizations' medical capabilities. For instance, analysis of the ISIS medical system suggests that undermining a group's medical infrastructure with information operations can degrade its ability to sustain operations, reduce morale, and create vulnerabilities in enemy healthcare provisions.¹² This strategy exemplifies MEDINT's role in counterterrorism by safeguarding military personnel and countering structural targeting. Similarly, understanding medical capabilities

and locations has led to the direct destruction of healthcare assets by adversaries in Ukraine.¹³ This weaponization of health care assets has been seen in Syria.¹⁴ It has also taken place in the Democratic Republic of the Congo.¹⁵ Additionally, state actors have undermined medical care with information operations, likely informed by high-quality intelligence; for example, China capitalized on the chaos of the COVID-19 pandemic to spread misinformation and disinformation that diminished trust in the U.S. government's pandemic response, impacting healthcare at a systemic level.¹⁶

MEDINT's dual-use nature is further exemplified in NATO's MEDINT doctrine, which outlines its importance in both force health protection and broader strategic applications, such as assessing foreign leaders' health, monitoring risks of biomedical research, and assessing the adversary's development of chemical and biological weapons. This strategic approach integrates MEDINT into intelligence assessments beyond traditional health risks, highlighting its relevance in shaping geopolitical decisions and military planning.¹⁷

While much of MEDINT's work remains presumably classified, efforts by authors like Dr. Jonathan Clemente specifically tracked the history of such work by the intelligence community.¹⁸ One such piece covers the history of organizations like the CIA's Medical and Psychological Analysis Center.¹⁹ Another covered its efforts to evaluate the health of foreign leaders.²⁰ Additionally, Dr. Clemente wrote about parallels between medicine and intelligence.²¹ In fact, he argued that medicine can teach lessons to the intelligence community.²² Some of the CIA's work on foreign leaders' health has been published publicly as well, including an analysis of strokes among world leaders.²³ CIA authors have also written about the intelligence implications of disease.²⁴

Today, MEDINT remains a critical asset in IW operations, blending traditional medical practices

with covert intelligence gathering. The establishment of guerrilla trauma systems and covert medical intelligence networks can strengthen a protagonist's sphere of influence in IW, providing tactical support and ensuring medical resilience in hostile environments.²⁵ This approach is echoed by the French Special Operations Forces Medical Command, which emphasizes that success in IW requires integrating good medicine with sound tactics and strategic planning.²⁶ The utility of MEDINT and MIPOE for supporting counterterrorism (CT) and counterinsurgency (COIN) objectives is also extensively reviewed in the 2020 National Defense University publication "How Can USSOF Leverage Medical Intelligence for Unconventional Warfare?"²⁷ Indeed, O'Hara notes the potential intelligence windfall that judicious use of SOF medics in guerrilla hospitals could have in the context of COIN, wherein immersion with local culture is paramount to effective operations. Other current work suggests that MEDINT has useful implications in global health security, a field which overlaps in means with MSIW despite different objective ends.²⁸ This is particularly relevant in light of the COVID-19 pandemic.²⁹ Additionally, MEDINT is already being collected for many other purposes; resources like Shoreland Travax capture health system information for travelers, while the Centers for Disease Control and Prevention (CDC) and U.S. Department of State maintain internal repositories for global medical infrastructure assessment, and the CIA publishes public information like its World Factbook for public consumption. One important theme encompassing the work below is to ensure that MEDINT collected for independent reasons from various sources, whether it is even known as MEDINT by such organizations, can be integrated for MSIW purposes.

APPLICATION OF MEDINT IN KINETIC OPERATIONS: LESSONS FROM THE RUSSIA-UKRAINE CONFLICT

Before launching kinetic operations, MEDINT plays a critical role in determining injury patterns based on the adversary's order of battle and tactics, techniques, and procedures (TTPs) or based on situational factors that may complicate the treatment of disease non-battle injuries (DNBI). This intelligence is essential for enabling proactive measures such as prepositioning surgical assets, establishing evacuation hubs, and configuring medical logistic chains, including production and distribution. The ability to predict injury patterns allows for more effective placement of resources, resulting in better medical outcomes and improving the overall combat readiness of forces. Observations from the Russia-Ukraine war illustrate how emerging weapon systems and modern warfare tactics are creating new injury trends, emphasizing the importance of MEDINT in adapting medical support.³⁰ Both public and classified lessons from this conflict can be directly translated to American and allied military medical strategies.³¹

INJURY PATTERNS AND MEDICAL PLANNING

One of the notable differences between the Russia-Ukraine conflict and prior Global War on Terror (GWOT) operations is the prevalence of advanced weapon systems, such as anti-tank guided missiles (ATGMs), first-person view (FPV) drones, and incendiary munitions. These weapon systems have increased the incidence of blast injuries and thermal trauma, necessitating shifts in medical planning to address these specific injury types.³² By integrating MEDINT related to threat data, the types of weapons used, and associated injury patterns, military planners can ensure counter-threat

and risk mitigation structures are positioned to respond more effectively. For instance, the pre-positioning of trauma surgical teams in high-risk areas and aligning medical evacuation routes with anticipated blast zones ensures faster, more targeted care for combatants.

Furthermore, asymmetric and unconventional weapons such as Chemical, Biological, Radiological, and Nuclear (CBRN) agents have already played a role in the Russia-Ukraine war and highlight the necessity for MEDINT to inform preparation and responses against such threats. Indeed, the U.S. Department of State determined that Russia used the chemical weapon chloropicrin against Ukrainian forces, and assessed that Russia also used riot control agents as a method of warfare in Ukraine, both of which violate the Chemical Weapons Convention (CWC).³³ These instances came on the heels of Russian operations to poison Aleksey Navalny in 2020 and Sergei and Yulia Skripal in 2018, with Novichok nerve agents.³⁴ In these targeted cases, swift clinician recognition of toxidromes was essential to providing lifesaving treatment and ensuring the safety of all who came in contact with the victims. On a larger scale, current and future battlefields may be marked using CBRN agents. This necessitates that medical teams are armed with the knowledge of potential agents in use in a given battlefield scenario. It also demands that they recognize relevant toxidromes and have the space and logistical support to establish appropriate hot, warm, and cold zones for casualty decontamination and treatment.

Such precision in medical logistics and planning improves return to duty (RTD) and survivability rates while increasing the ability to operate with speed and agility in an IW environment, giving a strategic advantage in protracted conflicts. Advanced medical technologies, field-hardened medical facilities, and well-informed medical personnel are vital in reducing long-term casualty

impacts, ultimately contributing to mission success by enabling quicker recovery and redeployment of injured soldiers.

MEDICAL INFRASTRUCTURE AS A BATTLEFIELD TARGET

A disturbing trend in the recent wars, including the Russia-Ukraine conflict, has been the direct targeting of medical facilities.³⁵ These facilities are traditionally protected under international law through the Geneva Convention.³⁶ Despite this, attacks on healthcare may be becoming a new norm.³⁷ Russian forces' targeting of medical infrastructure in particular highlights the need for more resilient and hardened medical installations, among other interventions.³⁸ These attacks defy established norms and force medical personnel to provide care under direct threat, requiring military planners to rethink how they protect and deliver medical services in conflict zones. MEDINT enables planners to anticipate these risks, ensuring that medical facilities are appropriately fortified and positioned to continue providing care in hostile environments. By revealing the adversary's tactics, MEDINT can inform decisions about hardened medical shelters, advanced casualty evacuation routes, and the pre-positioning of mobile medical units.

Furthermore, the current conflict in the Gaza Strip has seen numerous incidents of medical facility targeting by the Israeli Defense Forces (IDF). This has been the subject of continued controversy, as accusations of war crimes have been met with IDF claims that medical facilities such as the al-Shifa Hospital in Gaza were being co-opted and utilized as a base of operations for Hamas forces.³⁹ In particular, tunnels beneath these hospitals have shown how medical infrastructure has been unfortunately entangled with combatant activities.⁴⁰ This highlights the importance of comprehensive, reliable MEDINT to clarify when medical infrastructure

and assets may or may not be manipulated by adversarial forces.

This reality underscores the importance of combat casualty care that integrates MEDINT to adjust for the unique medical challenges in each conflict. The intelligence gathered regarding enemy capabilities, weapon systems, and battlefield behaviors significantly influences how military forces prepare for the type of injuries they will likely face and the conditions under which care will be delivered. As a result, MEDINT becomes a force multiplier, enhancing survivability and combat effectiveness by improving casualty outcomes, while also mitigating risk through informed preventive efforts that address the more frequent DNBIs that affect personnel.

Pre-Invasion Indicators: Medical Supplies and Field Hospitals

Even before Russia invaded Ukraine on February 24, 2022, MEDINT provided critical indications and warnings about impending hostilities. In January 2022, reports surfaced of Russia stockpiling blood supplies along the Ukrainian border, a clear signal that large-scale military action was imminent. Stockpiling medical supplies such as blood products, which are essential for treating battlefield injuries, provided early insight into Russia's readiness for kinetic operations.⁴¹ These plans were further corroborated on February 10, 2022, when satellite images showed the deployment of a Russian field hospital near the Ukrainian border in Zyabrovka, Belarus, approximately 15 miles from Ukraine. Such a facility strongly indicated Russia's intent to engage in sustained military action, as it confirmed the preparation of medical support structures crucial for maintaining combat operations.

This use of MEDINT, particularly in monitoring the buildup of medical infrastructure, provided invaluable information not only about Russia's logistical readiness but also about the anticipated

scope and scale of the conflict. By identifying where and how medical assets were deployed, intelligence analysts could infer the likely direction and intensity of forthcoming operations.

Insights into Enemy Strategy from Medical Asset Placement

MEDINT can also reveal the strategic priorities of adversaries through the analysis of medical asset placement and casualty evacuation routes. The positioning of field hospitals behind the forward line of troops (FLOT) offers insight into what territory the enemy deems secure. As the FLOT moves, so too does the network of medical facilities. This forward movement can also help identify the operational reach of an adversary's integrated air defense systems, providing valuable intelligence on their defensive capabilities and geographical control. Additionally, the size, scope, and location of medical facilities can indicate the scale of conflict anticipated by the enemy and reveal their logistical preparedness.

An understanding of the medical capacity of the enemy can both inform commanders about enemy unit readiness as well as identify targets for operations. Indeed, noting the medical supplies' country of origin, supplies such as applied tourniquets, chest seals, medication vials or even IV tubing, could uncover logistics routes and sources of external support, which in turn could be exploited to further shape the battlefield.²⁷

MEDICAL INTELLIGENCE IN SUPPORT OF IRREGULAR WARFARE ON THE FUTURE BATTLEFIELD

The role of MEDINT in IW is rapidly expanding as future battlefields require decentralized, mobile, and adaptable medical support systems. MEDINT is ultimately oriented in two directions: to inform

adversary characteristics through contributions to intelligence, and to inform friendly medical support, resource allocation, and decision-making. MEDINT's integration with signals intelligence (SIGINT), geospatial intelligence (GEOINT), and human intelligence (HUMINT) ensures real-time situational awareness, improving casualty management and resource deployment in rapidly evolving operational environments. This section explores the growing significance of MEDINT in IW, particularly its contribution to enhancing medical infrastructure mobility, overcoming intelligence-sharing limitations, and preventing adversarial exploitation of medical data.

MEDICAL INTELLIGENCE IN FUTURE CONFLICTS

From the perspective of blue force advantage, or the recognition of friendly support forces or resources in a region, intelligence on local health infrastructure is required for casualty care in future conflicts. Evacuation times will be protracted in unconventional and guerrilla warfare conflicts.⁴² Providing medical care in such an environment is largely dependent on the capabilities of partner forces and the existence of safe zones.⁴³ Adequate MIPOE can identify indigenous medical personnel willing to aid, the level of training that personnel receive, and potential geographic safe zones.⁴³ Such data can be extracted from communications intelligence (COMINT), imagery intelligence (IMINT), HUMINT, and even open-source intelligence (OSINT), but it requires collection requests and analysis informed by medical requirements. The value of such analysis is that vetted local medical capabilities have the potential to decrease mortality when casualties are unable to be evacuated within the "golden hour," which refers to the mortality improvement seen in patients who are provided with appropriate medical and surgical care within 60 minutes of injury.

Irregular warfare places an increasing demand for placement and access to foreign countries, including heavy reliance on the healthcare infrastructure of host nations. The diversity and disparity of foreign medical care underscore the importance of MIPOE, which often centers on medical infrastructure assessments. However, MIPOE of the host nation's medical infrastructure requires practitioners to contend with several challenges to produce accurate and actionable information. For example, medical infrastructure information repositories are disparately stored across both U.S. government and nongovernmental siloes, with both structural and technical barriers to data sharing. Further, survey formats are generally inconsistent, with structure, content, and assessor differences impacting reliability. These issues often compound to result in duplicative efforts to collect foreign medical infrastructure information. Redundant or uncoordinated MEDINT collection impedes the accuracy and timeliness of available MEDINT. Uncoordinated efforts can also strain relations with host-nation facilities, undermining the effectiveness of IW. Therefore, IW medical practitioners should seek to coordinate collection efforts, share information, and streamline data sharing.

Future military conflicts are assessed to require more mobile command and control nodes and likely more mobile medical infrastructure, such as easily transportable operating tables with all associated supplies.⁴⁴ Conventional intel provides an enemy order of battle and probable locations of enemy defense systems, all represented on a common operating picture for utilization by command-and-control nodes at the operational level. With medical units required to be more mobile in future conflicts, intel capability must be available, especially in communication-denied environments, as anticipated with Russia and China. Threat maps from this information can be used to plan the mission for routes of infiltration and exfiltration mobile

surgical teams. Integration of regularly updated threat data with known requirements for medical operations enhances the U.S.' ability to operate low visibility, highly mobile medical infrastructure. Importantly, efforts must be made to translate intelligence products that are currently more strategic into ones that are operational and actionable by those in the field. Such efforts will require pulling insights from other fields of the intelligence community to determine how actionable intelligence can be transmitted to those in areas with limited connectivity and security to protect such material.

As the complexity of IW intensifies, so do the challenges in information-sharing among allied nations. Organizations like the North Atlantic Treaty Organization (NATO) often face doctrinal gaps, network limitations, and organizational shortcomings that prevent the rapid dissemination of critical MEDINT data.⁴⁵ These barriers hinder timely decision-making, particularly regarding medical logistics, evacuation hubs, and surgical team placement on the battlefield. Such barriers are worsened amongst partner nations, who lack official alliances that may help with overcoming these obstacles, but whose mutual support can be essential in IW environments.

To bridge these gaps, OSINT has emerged as a vital tool for collecting and distributing timely MEDINT updates. OSINT sources such as social media, satellite imagery, and native-language sites provide real-time insights into adversary movements and medical capabilities, which may be provided by organizations like the CDC, the World Health Organization (WHO), ReliefWeb, and other on-the-ground organizations. For example, the identification of a Russian field hospital in Zhabovka, Belarus, just before the 2022 Ukraine invasion was made possible through OSINT.⁴⁶ This allowed allied forces to assess Russia's medical support infrastructure and operational readiness.

This concept can be expanded to identify trafficking patterns and ratlines, as O'Hara discussed at length the correlation between the presence of trafficking and the rise of infectious disease in a particular region.²⁷ Furthermore, by utilizing real-time COVID-19 disease patterns derived from the CDC and WHO, along with their superimposed correlation to trafficking and poverty data derived from other open sources, O'Hara makes a case for MIPOE's potential contribution to counterterrorism mission planning, thereby strengthening the operational utility of MEDINT.

In addition to OSINT, initiatives like the Military Medical Almanac, an open-source database of country-specific health information collected from each nation using an annual questionnaire, can offer baseline data on country-specific health capabilities.⁴⁷ Studies have analyzed such data to evaluate the capabilities of various military medical services.⁴⁸ That work also led to the development of a more robust framework for future profiles.⁴⁹ However, the underlying data is self-reported, raising questions about accuracy, and limited in its ability to reflect military medical TTPs due to country-specific desires for security and ambiguity. Information in the Almanac can be potentially supplemented with other OSINT sources, such as native-language sites, social media, and articles about foreign medical capabilities.⁵⁰ Still, barriers to utilizing such OSINT include the language in which the data is published and the relevancy of publicly available data. However, linguists and OSINT analysts would be more readily able to exploit resources. Furthermore, it's important to note that the capabilities of the civilian sector rather than the military sector will be the most relied upon in IW settings.

Artificial intelligence (AI) and machine learning (ML) offer tremendous promise in making sense of mountains of OSINT data. NCMI or other MEDINT leaders should develop data structures that collect and store potentially relevant

information and enable algorithms to identify and report critical MEDINT far more quickly than humans can. AI-enabled translation and analytical capabilities will multiply the amount of available data and provide MEDINT with unprecedented transparency. For example, using AI tools like computer vision could quickly analyze satellite imagery from numerous sources to identify field hospital operations. Alternatively, AI/ML programs could analyze open-source information on wastewater epidemiology to identify covert lab operations. The utility of AI in military medicine is increasingly widespread and relevant.⁵¹ While clinical care and efficiency are areas that can already benefit, MEDINT is one of several areas in need of further development.⁵²

ADVERSARIAL USE OF MEDICAL INTELLIGENCE

While MEDINT enhances U.S. military capabilities, it also presents risks when exploited by adversaries. Cyber espionage and denied communications are critical threats to MEDINT, especially in IW environments where casualty evacuation and medical mission planning are crucial. For instance, gaining access to air refueling schedules for platforms like the C-130 or HH-60 could jeopardize evacuation missions, impacting force readiness and the survival of injured personnel.

Moreover, adversaries can exploit U.S. health records to target specific individuals within the military. In 2022, a U.S. Army major conspired to provide sensitive health information of U.S. personnel to Russia, highlighting the dangers of personal medical data being used for psychological operations.⁵³ Furthermore, recent cyber-attacks against different components of the U.S. healthcare system, from attacks on hospitals and blood suppliers to the Change Healthcare Ransomware Attack that compromised the protected health information of one in every three patients, illustrate the scale at which

such damage to care provision or information security can occur.⁵⁴ Case studies of such cyber-attacks can offer detail about the challenges at the hospital level for additional specificity.⁵⁵ Overall, such exploitation can degrade warfighter morale, eroding their confidence in receiving proper medical care and undermining combat effectiveness.

CONCLUSION

As future conflicts increasingly involve IW, decentralized operations, and communication-denied environments, MEDINT will be an essential enabler for force protection and operational success. The evolving nature of these conflicts necessitates the integration of OSINT, cybersecurity measures, and mobile medical infrastructures to maintain an advantage over adversaries. MEDINT's ability to predict injury patterns, assess local medical resources, and ensure the rapid deployment of mobile medical assets will be critical to improving casualty care and maintaining high return-to-duty rates. By leveraging novel intelligence methods and technology, including OSINT and traditional methods, MEDINT will continue to shape the future battlefield. This strategic capability ensures that U.S. forces can adapt to changing conditions and maintain operational dominance in complex IW environments, providing a critical edge in achieving operational overmatch and mission success. **PRISM**

Notes

¹ Joint Chiefs of Staff (JCS), *Joint Publication 4-02, Joint Health Services*. 2017.

² JCS, *Joint Publication 2-01.3, Joint Intelligence Preparation of the Operational Environment*. 2014.

³ Saul Jarcho. "Historical Perspectives of Medical Intelligence." *Bulletin of the New York Academy of Medicine* 67, no. 5 (September 1991): 501. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1807979/>.

⁴ Jarcho, "Historical Perspectives of Medical Intelligence," 501.

- ⁵ Sanders, Marble. “Medical Intelligence: Historical Background and Current Capabilities.” *Military Intelligence Professional Bulletin* 46, no. 1 (January 2020): 34–39.
- ⁶ Bush, Lester E., and Randy P. Burkett. “The Fighting Doctors of the Office of Strategic Services.” *Studies in Intelligence* 62, no. 3 (September 2018).
- ⁷ Jonathan D. Clemente. “The Fate of an Orphan: The Hawley Board and the Debates over the Postwar Organization of Medical Intelligence.” *Intelligence and National Security* 20, no. 2 (2005): 264–87.
- ⁸ U.S. Department of Defense (DOD). National Center for Medical Intelligence (NCMI) DOD Instruction 6420.01. March 20, 2009. Updated September 8, 2020. Accessed July 13, 2025. <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/642001p.pdf>.
- ⁹ Maryn McKenna. “Did the CIA Fake a Vaccination Campaign?” *The Best Science Writing Online* 2012, 194, 2012.
- ¹⁰ Legal Information Institute. 22 CFR §305.6—Eligibility. Cornell Law School. Updated January 1, 2024. Accessed July 11, 2025. <https://www.law.cornell.edu/cfr/text/22/305.6>.
- ¹¹ Lena H. Sun. “CIA: No more vaccination campaigns in spy operations.” *The Washington Post*, May 19, 2014. Accessed July 11, 2025. https://www.washingtonpost.com/world/national-security/cia-no-more-vaccination-campaigns-in-spy-operations/2014/05/19/406c4f3e-df88-11e3-8dcc-d6b7fed081a_story.html.
- ¹² Regan Lyon. “ISIS Medical System as a Target for Counterterrorism Efforts.” *Institutional Archive of the Naval Postgraduate School*. 2021. <https://calhoun.nps.edu/server/api/core/bitstreams/640454cd-b8c7-4f22-a29f-e6f861ec82dc/content>.
- ¹³ Heisler, Michele, Pavlo Kovtonyuk, and Christian De Vos. “Attacks on Health Care Used as a Weapon of War in Ukraine and Globally: The Demand for Accountability.” *JAMA* 329, no. 12 (2023): 973–74. <https://doi.org/10.1001/jama.2023.2787>.
- ¹⁴ Fouad, Fouad M., et al. “Health Workers and the Weaponisation of Health Care in Syria.” *The Lancet* 390, no. 10111 (December 2, 2017): 2516–26. [https://www.thelancet.com/article/S0140-6736\(17\)30741-9/fulltext](https://www.thelancet.com/article/S0140-6736(17)30741-9/fulltext)
- ¹⁵ Leonard Rubenstein. Violence Against or Obstruction of Health Care in the Democratic Republic of the Congo (DRC). *Safeguarding Health in Conflict Coalition*, 2021. <https://insecurityinsight.org/wp-content/uploads/2021/05/2021-SHCC-Democratic-Republic-of-the-Congo-DRC.pdf>.
- ¹⁶ Regan F. Lyon. “How China’s Cyber Operations During the COVID-19 Pandemic Worsened the United States Biodefense and National Security.” *Cyber Defense Review* (Fall 2022): 159–69. https://cyberdefensereview.army.mil/Portals/6/Documents/2022_fall/10_Lyon.pdf.
- ¹⁷ NATO. *NATO Guide to Medical Intelligence*. [https://www.coemed.org/files/stanags/02_AJMEDP/SRD-1_to_AJMedP-3_EDA_V1_E_\(4\)_2547.pdf](https://www.coemed.org/files/stanags/02_AJMEDP/SRD-1_to_AJMedP-3_EDA_V1_E_(4)_2547.pdf).
- ¹⁸ Jonathan D. Clemente. “Medical Intelligence.” *Intelligencer: Journal of U.S. Intelligence Studies* 20, no. 2 (2013). <https://www.securityscience.edu.rs/index.php/journal-security-science/article/view/151>.
- ¹⁹ Jonathan D. Clemente. “CIA’s Medical and Psychological Analysis Center (MPAC) and the Health of Foreign Leaders.” *International Journal of Intelligence and CounterIntelligence* 19, no. 3 (June 2006): 385–423.
- ²⁰ Clemente, Jonathan D. “In Sickness and in Health.” *Bulletin of the Atomic Scientists* 63, no. 2 (March 2007): 38–66. <https://journals.sagepub.com/doi/full/10.2968/063002010>.
- ²¹ Marrin, Stephen, and Jonathan D. Clemente. “Modeling an Intelligence Analysis Profession on Medicine.” *International Journal of Intelligence and CounterIntelligence* 19, no. 4 (December 2006): 642–65.
- ²² Marrin, Stephen, and Jonathan D. Clemente. “Improving Intelligence Analysis by Looking to the Medical Profession.” *International Journal of Intelligence and CounterIntelligence* 18, no. 4 (December 2005): 707–29.
- ²³ Brickfield, Francis X., and Leslie R. Pyenson. “The Impact of Stroke on World Leaders.” *Military Medicine* 166, no. 3 (March 2001): 231–232.
- ²⁴ Carey, Warren F., and Maxfield, Myles. “Intelligence Implications of Disease.” *Studies in Intelligence* 16, no. 2 (Spring 1972): 71–78.
- ²⁵ Mason H. Remondelli. “Strengthening the Medical Sphere of Influence Through Guerilla Trauma Systems and Covert Medical Intelligence Networks.” March 30, 2023.
- ²⁶ Pasquier, Pierre, et al. “Irregular Warfare Must Combine Good Medicine, with Both Good Tactics and Good Strategies: Position Paper by the French Special Operations Forces Medical Command.” *Journal of Trauma and Acute Care Surgery* (2023): 10-1097. <https://pubmed.ncbi.nlm.nih.gov/38569049/>.
- ²⁷ Logan O’Hara. “How Can USSOF Leverage Medical Intelligence for Unconventional Warfare?” Master’s thesis, National Defense University, College of International Security Affairs, 2020.

- ²⁸ Bowsher, Gemma, Milner, Charlotte, and Sullivan, Richard. "Medical Intelligence, Security and Global Health: The Foundations of a New Health Agenda." *Journal of the Royal Society of Medicine* 109, no. 7 (July 2016): 269–73. <https://pubmed.ncbi.nlm.nih.gov/27385714/>.
- ²⁹ Patrick F. Walsh. *Health Security Intelligence: Managing Emerging Threats and Risks in a Post-Covid World*. Taylor & Francis, 2025. <https://www.routledge.com/Health-Security-Intelligence-Managing-Emerging-Threats-and-Risks-in-a-Post-Covid-World/Walsh/p/book/9781032371443>.
- ³⁰ Remondelli, Mason H., et al. "Casualty Care Implications of Large-Scale Combat Operations." *Journal of Trauma and Acute Care Surgery* 95, no. 2S (2023): S180–S184. <https://pmc.ncbi.nlm.nih.gov/articles/PMC10389308/>.
- ³¹ Hodgetts, Timothy J., David N. Naumann and Douglas M. Bowley. "Transferable Military Medical Lessons from the Russo-Ukraine War." *BMJ Military Health* (2023).
- ³² Epstein, Aaron, et al. "Putting Medical Boots on the Ground: Lessons from the War in Ukraine and Applications for Future Conflict with Near-Peer Adversaries." *Journal of the American College of Surgeons* 237, no. 2 (2023): 364–73. <https://pubmed.ncbi.nlm.nih.gov/37459197/>.
- ³³ U.S. Department of State, Office of the Spokesperson. "Imposing New Measures on Russia for Its Full-Scale War and Use of Chemical Weapons Against Ukraine." *State.gov*, May 1, 2024. <https://www.state.gov/imposing-new-measures-on-russia-for-its-full-scale-war-and-use-of-chemical-weapons-against-ukraine-2/>.
- ³⁴ Morcos, Pierre, and Cyrus Newlin. "The Implications of the Poisoning of Alexey Navalny." CSIS, 2020. <https://www.csis.org/analysis/implications-poisoning-alexey-navalny>.
- ³⁵Haar, Rohini J., et al. "Violence Against Healthcare in Conflict." *Conflict and Health* 15, no. 1 (2021): 37. <https://link.springer.com/article/10.1186/s13031-021-00372-7>.
- ³⁶ International Committee of the Red Cross. *Geneva Convention Relative to the Protection of Civilian Persons in Time of War* (Fourth Geneva Convention), Article 19. 1949. <https://ihl-databases.icrc.org/en/ihl-treaties/gci-1949/article-19>.
- ³⁷ Blanchet, Karl, Leonard Rubenstein, Bertrand Taithe, and Larissa Fast. "Have Attacks on Healthcare Become the New Normal?" *Conflict and Health* 17, no. 1 (2023): 56.
- ³⁸ Druce, Philippa, Ekatarina Bogatyreva, Frederik Francois Siem, et al. "Approaches to Protect and Maintain Health Care Services in Armed Conflict." *Conflict and Health* 13 (2019): 2. <https://doi.org/10.1186/s13031-019-0186-0>.
- ³⁹ Julian Borger. "IDF Evidence so Far Falls Well Short of Al-Shifa Hospital Being Hamas HQ." *The Guardian*, November 17, 2023. <https://www.theguardian.com/world/2023/nov/17/idf-evidence-so-far-falls-well-short-of-al-shifa-hospital-being-hamas-hq>.
- ⁴⁰ Rosenberg, Matthew, Ronen Bergman, Aric Toler, and Helmuth Rosales. "A Tunnel Offers Clues to How Hamas Uses Gaza's Hospitals." *The New York Times*, February 13, 2024. <https://www.nytimes.com/interactive/2024/02/12/world/middleeast/gaza-tunnel-israel-hamas.html>.
- ⁴¹ Phil Stewart. "Russia Moves Blood Supplies Near Ukraine." *Reuters*, January 28, 2022. <https://www.reuters.com/world/europe/exclusive-russia-moves-blood-supplies-near-ukraine-adding-us-concern-officials-2022-01-28/>.
- ⁴² Regan F. Lyon. *When the Golden Hour is Dead: Preparing Indigenous Guerilla Medical Networks for Unconventional Conflicts*. Naval Postgraduate School, 2021. <https://calhoun.nps.edu/handle/10945/68685>.
- ⁴³ Jennifer B. Caci. "Application of Medical Intelligence Prep of the Environment." *Journal of Special Operations Medicine* 15, no. 4 (2015): 117–24. <https://pubmed.ncbi.nlm.nih.gov/26630107/>.
- ⁴⁴ Deb Henley. "DMOC Brings Next Generation C2 to Life." *Air Combat Command*, 2022. <https://www.acc.af.mil/News/Article/3063879/dmoc-brings-next-generation-c2-to-life/>.
- ⁴⁵ Bedubourg, Gabriel, et al. "Collection and Sharing of Medical Information in NATO." *BMJ Military Health* 164, no. 4 (2018): 271–76. <https://pubmed.ncbi.nlm.nih.gov/29626142/>.
- ⁴⁶ *Reuters*. "Satellite Images Show New Russian Military Deployments Near Ukraine." February 11, 2022. <https://www.reuters.com/world/europe/satellite-images-show-new-russian-military-deployments-near-ukraine-2022-02-11/>.
- ⁴⁷ *Military Medicine Worldwide*. <https://military-medicine.com>.
- ⁴⁸ Leone, Ryan M., et al. "Framework for the Evaluation of Military Health Systems." *BMJ Military Health* 169, no. 3 (2023): 280–84. <https://pubmed.ncbi.nlm.nih.gov/33619229/>.
- ⁴⁹ Leone, Ryan M., et al. "An Analysis of International Military Health Systems." *Military Medicine* 186, no. 9–10 (2021): e1017–23. <https://pubmed.ncbi.nlm.nih.gov/33241312/>.
- ⁵⁰ Homan, Zachary S., et al. "Analyzing International Military Medical Services." *International Journal of Intelligence and Counterintelligence* 34, no. 2 (2021): 235–58. <https://www.tandfonline.com/doi/full/10.1080/08850607.2020.1807781>.

⁵¹ Leone, Ryan M., et al. “Artificial Intelligence in Military Medicine.” *Military Medicine* 189, no. 9–10 (2024): 244–48. <https://pubmed.ncbi.nlm.nih.gov/39028176/>.

⁵² Adirim, Terry, and Cathaleen Madsen. “Artificial Intelligence in the US Military Health System.” *Military Medicine*, September 18, 2024. <https://academic.oup.com/milmed/article/190/7-8/199/7760198>.

⁵³ Lubin, Marcia. “Major in the United States Army and a Maryland Doctor Facing Federal Indictment for Allegedly Providing Confidential Health Information to a Purported Russian Representative to Assist Russia Related to the Conflict In Ukraine.” U.S. Attorney’s Office (Maryland), 2022. <https://www.justice.gov/usao-md/pr/major-united-states-army-and-maryland-doctor-facing-federal-indictment-allegedly>.

⁵⁴ Santos, Nicole, et al. “Navigating a Crisis: Level One Trauma Center Crisis Management Amid Blood Distribution Cyberattack.” *Military Medicine* (October 9, 2024). <https://doi.org/10.1093/milmed/usae461>.

⁵⁵ Kanter, Genevieve P., James R. Rekowski, and Joseph T. Kannarkat. “Lessons from the Change Healthcare Ransomware Attack.” *JAMA Health Forum* 5, no. 9 (September 2024): e242764. <https://jamanetwork.com/journals/jama-health-forum/fullarticle/2823757>.

Strategic Culture – A Complex Model for a Complex Concept

By Lawrence A. Kuznar, Nathan C. Heath, and George R. Popp

The 21st century began with the U.S. focused on asymmetric threats from non-state actors who held radically different views, values, and motivations from the Western world. Meanwhile, adversarial states motivated by their own interests, identities, and fears retooled their strategic approaches to compete with, and potentially undermine, Western power and its rules-based order. Adversaries embraced gray zone/hybrid warfare tactics and irregular warfare (IW) techniques that engage in activities under the threshold of major kinetic actions against the U.S. and allies to avoid defeat at the hands of militarily superior Western powers.¹ The need to understand the motives, interests, and potential actions of these culturally different state and non-state actors led to renewed interest in the role that an actor's culture plays in its strategic behavior, and sheds light on the adversarial embrace of irregular warfare techniques.

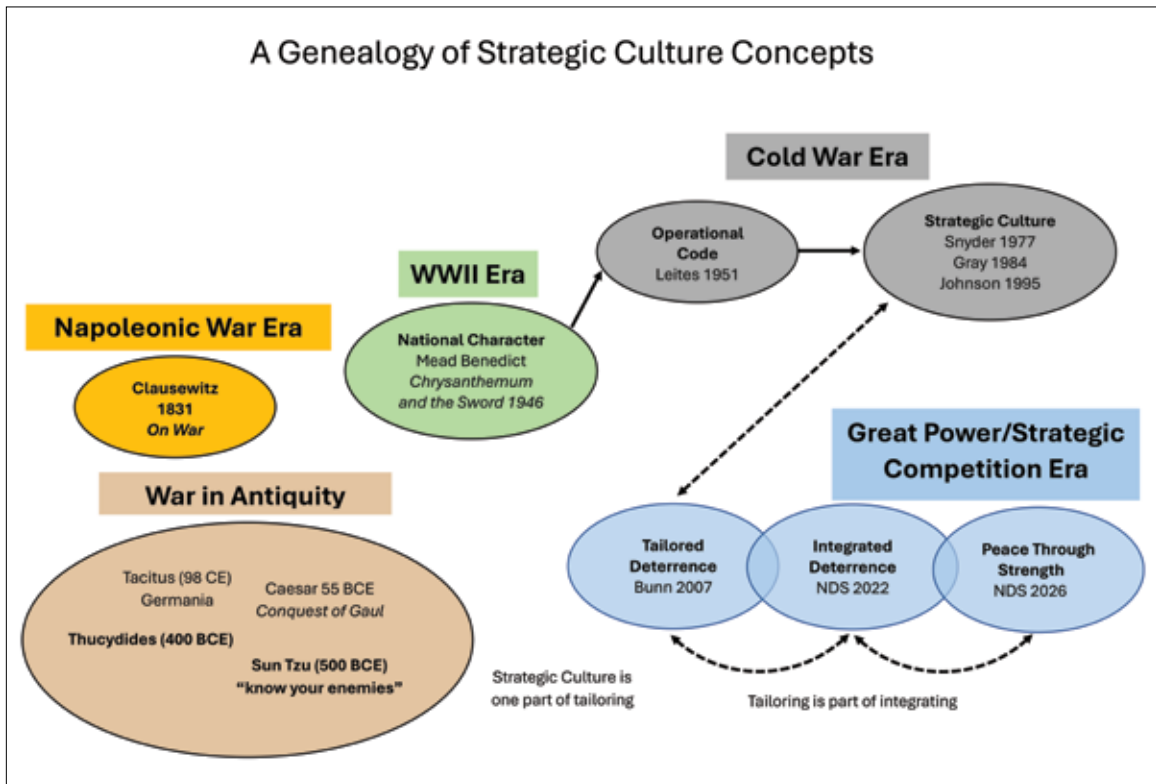
The strategic culture concept was born during the Cold War as Western powers struggled to understand Soviet worldviews in the service of deterring nuclear escalation. Subsequently, the strategic culture concept has since engendered theoretical challenges in definition, hypothesis generation, and scientific validation. Key issues include: what constitutes a strategic culture, how can it be measured, and what if any effect does it have on strategic behavior? In the context of these debates, scholars and practitioners have suggested that strategic culture itself is a complex system. We propose a complex systems model of strategic culture that we argue can resolve definitional and theoretical challenges, allowing for the generation of testable hypotheses regarding strategic culture's

Lawrence Kuznar is Emeritus Professor of Anthropology, Purdue University-Fort Wayne and Director of Cultural Sciences at NSI, Inc. His work includes application of anthropology, quantitative methods, and computational modeling to national security problems. His work has been published in *North Korean Review*, *NATO Open Publications*, *Dynamics of Asymmetric Conflict*, *Political Studies*, *American Anthropologist*, and *Current Anthropology*.

Nathan Heath is a Senior Research Scientist with National Security Innovations specializing in security cooperation, emerging technology risk, and AI integration. He previously worked in multiple public and private sector roles, and his work has also appeared in *War on the Rocks*, *Inkstick Media*, and *Global Security Review*. Nathan holds an M.A. in Law and Diplomacy from The Fletcher School.

George Popp is a Senior Research Scientist at NSI, Inc., specializing in national security and international affairs. His work centers on translating complexity into actionable insights that fuel effective decisions. A central focus of this is leading expert elicitation efforts to bridge the gap between communities of interest. George has an MA in public policy and international security from the University of California, San Diego.

Figure 1. A history of strategic culture-like concepts



Source: authors.

effects on strategic behavior, and anticipating likely red lines and adversarial responses useful for operational planning. We illustrate our approach with a Russian strategic culture example.

The idea that an actor’s strategic culture influences its strategic behavior is logical and ancient. It implies that different actors approach competition and conflict with different cultural lenses, assumptions, and perhaps behaviors. An early nod to strategic culture was proposed by the Chinese strategist Sun Tzu 2,500 years ago in his directive to, “know the enemy and know yourself; in a hundred battles you will never be in peril.”² At about the same time the ancient Greek historian Thucydides attributed Athenian power to their cultural attributes of innovation and restlessness. In *The Conquest of Gaul*, Julius Caesar provided descriptions of Germanic

culture and how he thought it inclined them for war. Centuries later, Prussian General Carl von Clausewitz stressed the moral qualities of combatants, an element of culture, as a key dimension of war.

An overview of strategic culture-like concepts in historical perspective is presented in Figure 1. The concept of strategic culture was fully developed in the 20th century. Prior to World War Two (WWII), anthropologists of the culture and personality school of thought proposed that the way people are socialized in a particular culture leads to the development of modal personality types that in turn give each culture a distinct character. The leaders of this school of thought, Margaret Mead and Ruth Benedict, used this approach during WWII in national character studies intended to provide insight into U.S., Japanese, and Soviet ways of war.³

During the Cold War, Nathan Leites credited Margaret Mead with influencing his notion of an *operational code* in his effort to understand the perspectives and behaviors of the Soviet Politburo.⁴ The next major work on culture and strategy was Jack Snyder's landmark 1977 RAND study of Soviet strategic decision making in which he coined the term "*strategic culture*."⁵

Snyder's work motivated academic scrutiny of the concept, resulting in several "generations" or schools of thought regarding what strategic culture is, whose strategic culture matters, and, most important, what if any effect strategic culture has on an actor's strategic behavior, which may include nuclear postures, military investments, deployments, military conduct in war, or operations under the level of armed conflict. This report will address these fundamental questions and propose a model of strategic culture along with a preliminary illustration of how the model can apply to Russian strategic culture.

STRATEGIC CULTURE – THE DEBATES

Important epistemological, theoretical, and empirical issues about the definition and usefulness of "strategic culture" remain unresolved. A key dispute, named after its protagonists as the Johnston-Gray Debate, concerns whether strategic behavior can be included as part of its definition. Ian Johnston argues that a definition that includes its dependent variable is tautological and therefore scientifically invalid, while Colin Gray maintains that the concept is primarily useful for providing a context for understanding behavior, stopping short of claiming that it necessarily has predictive value.⁶

In 2005, the then U.S. Department of Defense's Defense Threat Reduction Agency (DTRA) funded a workshop of scholars in an effort to resolve debates in the field of strategic culture, develop a methodology for systematic application of strategic culture to national security problems, apply that

methodology to specific case examples, and provide a curriculum for teaching comparative strategic culture.⁷ The scholars involved in that study continued their collective effort and published a major update in 2024 in which they refined their methodologies and incorporated insights from competing schools of thought.⁸

The DTRA workshop participants came to agreement on a number of crucial issues. The study produced a conceptual framework of strategic culture based on four key variables: identity, values, norms, and perceptive lens. Furthermore, the study authors proposed that these variables can be measured by dozens of inputs such as sacred texts, historical political systems, interactions with other nations, demographics, and global norms, and they applied their framework to analyze U.S., Russian, Chinese, Israeli, Indian, Pakistani, Iranian, Syrian, and al Qaeda strategic cultures.⁹ They agreed that strategic culture changes, although more slowly than other political influences, and therefore has the potential for long-term influences on strategic behaviors that typically occur on shorter timescales. Furthermore, all agreed that a state's strategic culture is only one among many factors that influence its strategic behavior. Pragmatic concerns such as military might and alliances also influence strategic behavior and may supersede the influence strategic culture may have on specific actions. The participants also agreed that in any nation, multiple sub-national groups and organizations are stakeholders who can have differing strategic cultures and that any complete analysis of a nation's strategic behavior must consider their interactions and their ultimate influences on an actor's strategic behavior. As to whether strategic culture causes behavior, contributors differed. Colin Gray reiterated his view that strategic culture is useful to provide context for behavior, while others such as Christopher Twomey, remained skeptical that strategic culture could usefully explain behavior.¹⁰

Interest in strategic culture continued.¹¹ Bloomfield attempted to unite competing views of strategic culture and concludes that, “From Gray we take the notion that culture provides context; that it guides and shapes interpretation: we just have to accept that culture is a disaggregated thing with contradictory elements rather than a monolithic whole.”¹² However, not all scholars find value in that concept; Echevarria concluded that strategic culture is a concept with “more problems than prospects” that should be abandoned because its key terms, such as culture, are poorly defined, change in strategic culture through time is not adequately addressed, and the fact that, despite historical differences, many of the world’s people still share many experiences, implying that cultures may not be as different as strategic culture researchers presume.¹³ Bloomfield and Echevarria’s comments highlight the fact that there remains room for improvement, despite the DTRA study’s accomplishments and the continued work of its scholars.

STRATEGIC CULTURE IN U.S. DETERRENCE CONCEPTS

The concept of strategic culture is implicitly and explicitly featured in important U.S. national security policy, particularly related to deterrence. The concept of tailored deterrence introduced in the 2006 U.S. Quadrennial Defense Review (QDR) directed that U.S. deterrence strategies and operations should be tailored to different types of adversaries, such as nuclear states, non-nuclear state adversaries, and non-state terrorist organizations, and stressed the need for understanding the cultures of adversaries and populations among whom warfighters operated. Elaine Bunn pointed out that by invoking the need to tailor deterrence to other types of actors, tailored deterrence implied a need for addressing questions such as, “What are the nation’s or group’s values and priorities?” and “How are these affected by its history and

strategic culture?” She also emphasized the need that communications to adversaries be tailored to adversaries’ perceptions, which are shaped by “an adversary’s national and cultural attributes as well as its unique history of dealing with and studying the United States.”¹⁴ Some researchers have argued that strategic culture makes some actors, such as Russia and China, more likely to engage in gray zone tactics such as subterfuge, deception, and undermining an adversary’s will through information operations.¹⁵ Later, the 2022 U.S. National Security Strategy (NSS) introduced the concept of integrated deterrence, and the 2022 U.S. National Defense Strategy (NDS) considered integrated deterrence its “centerpiece,” while noting that it should be “tailored to specific competitors and challenges.”¹⁶ Deterrence remains a cornerstone in the 2025 NSS and 2026 NDS, particularly in the objective of deterring China in the Indo-Pacific, which includes “working closely with our allies to incentivize and enable them to do more for our collective defense.”¹⁷ The focus on China and the need to coordinate with others in the region, all of whom have different strategic cultures,¹⁸ reinforces the need for tailored and integrated deterrence. The inclusion of tailored deterrence, and its implicit mandate to consider culture, logically connects strategic culture to the integrated deterrence concept and current deterrence priorities (Figure 1).

STRATEGIC CULTURE – WHAT IS IT?

We reviewed dozens of definitions of strategic culture, and while differing in detail, they generally conformed to the following definition, which we offer as a collation of their key elements. An actor’s strategic culture is composed of beliefs, experiences, assumptions, attitudes, and patterned behaviors that shape perceptions and preferences about its security-related interests, objectives, and activities. As to the central debate in strategic culture studies, we

have specified that the behaviors we include in our definition are *patterned*, by which we mean repeated traditional behaviors (i.e. *norms*) that reinforce ideological components of strategic culture; we do not mean all strategic behaviors, avoiding circular argumentation. For example, a tradition of using disinformation to undermine enemy's will or the use of mass formation and attritional warfare might be taught in military academies, reinforcing this type of warfare as part of a nation's strategic culture such that it habitually results in the use of propaganda and information operation or large military formations in times of war, respectively. Goldstein and Keohane's notion of principled beliefs about what is right or wrong versus causal beliefs about how the world works and things get done provides a framework for understanding the relationship between ideas and normative behaviors.¹⁹ Causal beliefs are the ideas that underly why normative behaviors are thought to be effective, strategic culture may influence how an actor understands the causal connection between actions and results, leading to the adoption of gray zone tactics such as information operations and disinformation or mass attacks.

Our definition of an actor is intentionally ambiguous. In part this is because 21st century adversaries can be state or non-state actors, all of whom potentially have different strategic cultures. Furthermore, an actor's strategic behavior is often the product of competing stakeholders within the actor's organization, such as competing political parties or branches of government, the topic explored in the next section.

AT WHAT LEVEL DOES STRATEGIC CULTURE OPERATE?

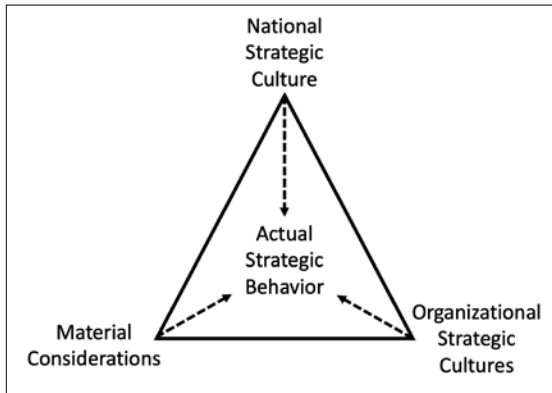
As we have seen, another question that strategic culture scholars debate concerns its appropriate unit of analysis. Whose strategic culture matters? Most scholars focus on the decision-making elite of a nation.²⁰ "Third generation scholars" emphasize

that the decision-making apparatus of a country involves different stakeholders and organizations, and that it is necessary to consider their different strategic cultures and how they interact to produce strategic behavior outcomes.²¹ As described above, the 2005 DTRA project and subsequent scholars appear to be largely in agreement that state actors consist of a variety of national security stakeholder organizations with different interests and strategic cultures, and that it is necessary to account for how their interactions lead to actual strategic behaviors.

The realization that policy is not the result of a sole decision-maker was advocated prior to Snyder's initial work on strategic culture and gave rise to the influential and debated bureaucratic politics school of thought, whose relevance was recognized by early proponents of strategic culture.²² Early bureaucratic politics scholars asserted the importance of internal competition among governmental stakeholders in formulating policy, leading to compromised positions that resulted in sub-optimal policy decisions. Critics pointed out that the bureaucratic politics model overly focused on American politics in a democratic system, ignored other key actors such as Congress, and lacked conceptual and scientific precision. Nonetheless, the bureaucratic politics model has seen a resurgence and has expanded to include the importance of individual personality and culture-influenced worldviews, and that competition and debate among intragovernmental factions may lead to more effective foreign policy. The relevance of recent bureaucratic politics research reinforces the importance of considering the strategic cultures of all actors within a state in a position to influence strategic behavior.²³

The operations of sub-national organizations can be influenced by their national strategic culture as well as the cultures of the sub-national organizations themselves. Along with practical, material concerns, either or both levels of strategic culture can influence strategic behavior.²⁴ Strategic

Figure 2. The competing influences of national strategic culture, organizational strategic culture, and material considerations on strategic behavior



Source: authors.

behavior is therefore potentially influenced by this triad of considerations, although not necessarily equally (Figure 2). Scholars debate which of these three potential influences has the most influence on a nation’s strategic behavior. We propose that the relative influence of each element of the triad is an empirical question that is sensitive to a particular national or geopolitical context. Knowing what strategic culture is and whose culture matters are necessary prerequisites to analyzing strategic behavior, which is the key theoretical question explored in the next section.

STRATEGIC CULTURE – WHAT DOES IT DO?

The fundamental debate concerning strategic culture is whether it matters at all. What, if anything, does strategic culture do? And does it impact strategic behavior in any meaningful way? According to Johnston’s analysis of ancient Chinese Confucian strategic culture, such culture is symbolic and does not do much at all in terms of influencing the state’s strategic behavior.²⁵ By contrast, analysts of Russian strategic culture repeatedly highlight its impor-

tance, drawing extensive connections between critical components such as history, geography, Russian Orthodoxy, and centralized decision-making to Moscow’s strategic policy from Imperial Russia to the present.²⁶

A review of the strategic culture literature indicates that strategic culture can:

- *Influence thinking and decision-making.* In fact, this is the most common function attributed to strategic culture.²⁷ For instance, Snyder proposed that it “guides and circumscribes thought on strategic questions.”²⁸ Legro says that it “shapes organizational cognition.”²⁹
- *Frame issues.* Strategic culture scholars also posit how strategic culture influences the framing of issues and events; how they are perceived and how actions are justified.³⁰
- *Justify elite power and actions taken.* According to “Second Generation” scholars, strategic culture is a narrative construct used to convince publics and allies to agree with the machinations of a dominant political elite, and similar arguments have been made by Johnston and Tannenwald.³¹
- *Provide meaning and context.* The final function attributed to strategic culture is that it provides contextual understanding for why things happen. This approach is explicitly interpretive; strategic culture is a device through which actors interpret the events of history and the implications of geography and the meanings they assign to strategic issues.³²

In summary, most scholars argue that strategic culture has some influence on thinking and decision-making, perception, and a role in justifying actions taken. It also provides actors with meaningful interpretations and analysts with a means of gaining a deeper understanding of another actor’s strategic behavior.

STRATEGIC CULTURE AS A COMPLEX SYSTEM

Snyder, after reviewing anthropological theories of war, first suggested that strategic culture was best framed as an open complex system in which behavior, symbols, and ideas are connected through feedback loops, although he did not develop an explicit model to test his theory.³³ We propose that modeling strategic culture as a complex system can incorporate the current consensus and at least partially resolve the debate over strategic behavior.

COMPLEX SYSTEMS

A complex system has elements that interact through direct and indirect feedback.³⁴ The interactions between elements of the system form a web of causal links, which may have non-linear influences on one another. Complex systems can exhibit unpredictable, emergent behaviors that involve the evolution of new structures and relationships, especially when non-linear connections exist, and have been useful in modeling phenomena in the physical, biological, and social worlds, and have also been applied to national security problems.³⁵

Culture concepts lend themselves to complex analysis. An often cited anthropological definition of culture from the 19th century is “that *complex whole* which includes knowledge, belief, art, law, morals, custom, and any other capabilities acquired by man as a member of society [emphasis added].”³⁶ Another foundational definition of culture, and one cited by many strategic culture theorists, is “a *system* of inherited conceptions expressed in symbolic forms by means of which men communicate, perpetuate, and develop their knowledge about, and attitudes toward life [emphasis added].”³⁷ For anthropologists, whether culture includes behavior or is a system of symbolic meanings, it has always been seen as a complex system. By extension, since the strategic culture concept was derived from

anthropological concepts, it should also be conceived as a complex system.

STRATEGIC CULTURE AS A COMPLEX SYSTEM: A MODEL

We take the DTRA strategic culture model as our starting point for developing a model of strategic culture as a complex system—what we will abbreviate as the Strategic Culture System Model (SCSM). The DTRA model’s four basic variables — identity, values, norms, and perceptive lens — function as nodes in a complex system. These four variables have been extensively applied in strategic culture research as part of the Cultural Topography methodology developed by Jeannie Johnson.³⁸ However, the DTRA model did not specify how these elements related to one another or their relative influences on strategic behavior. In this section, we present a model that specifies how their four variables may integrate into a cohesive model of strategic culture.

Viewed as a system of influences, normative strategic behavior is an important aspect of a strategic culture system. This is because some behaviors, especially if they are repeated in a routine, patterned way, can reinforce the ideational and emotional aspects of strategic culture. For example, standing at attention and listening to a national anthem when a flag is raised or lowered is a behavior that reinforces a patriot’s national identity and the symbolic meanings attached to the flag. There is feedback from the repeated routine and the system of symbolic meanings. Sociologist Pierre Bourdieu incorporated some but not all behavior in his definition of *habitus* as “a subjective but not individual system of internalized structures, schemes of perception, conception, and action common to all members of the same group or class [emphasis added].”³⁹ Snyder’s original definition of strategic culture specifically singled out “patterns of habitual behavior,” not necessarily all behaviors. In complex system terminology, Snyder’s and Bourdieu’s definitions propose a feedback loop between habitual

behaviors and meaning. Furthermore, recall that the DTRA model defined norms as “accepted and expected modes of behavior.” As the flag example illustrates, norms reinforce identity and values. In addition, norms influence perceptions. Positive feedback in this system represents circular influences that reinforce identities, values, perceptions, and normative behaviors. Examples of normative strategic behavior proposed by strategic culture scholars include U.S. reliance on technology in warfare, Russian use of mass wave formations, and Chinese use of active defense.⁴⁰

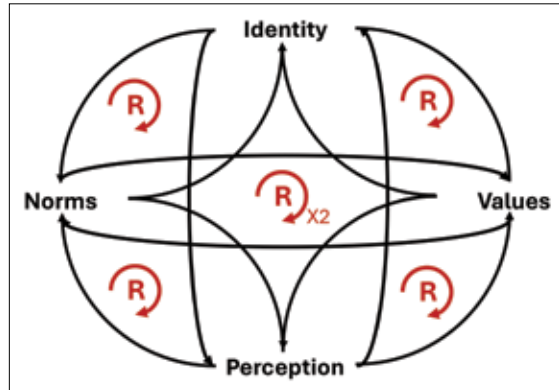
The core of our SCSM is comprised of the four DTRA strategic culture variables.⁴¹ We nominally amended them as follows:

- **Identity:** “A nation-state’s view of itself, comprising the traits of its national character, its intended regional and global roles, and its perceptions of its eventual destiny;”
- **Values:** “the material and/or ideational factors which are given priority, and selected over others;”
- **Norms:** “Accepted and expected modes of behavior;” and
- **Perceptive lens:** “Beliefs (true or misinformed) and experiences or the lack of experience, which color the way the world is viewed.”

THE STRATEGIC CULTURE SYSTEM MODEL (SCSM)

The DTRA research as well as much of the academic literature reviewed above implies that each of the four strategic culture variables can influence the others, creating a complex system of six mutually and positively reinforcing relationships (Figure 3). Reinforcing relationships are especially significant in complex systems because they can entrench one another, forming a configuration that is resistant to change. Conversely, if reinforcing relationships break, time-honored configurations of strategic

Figure 3. SCSM: A complex system model of strategic culture. Rs indicate reinforcing relationships.

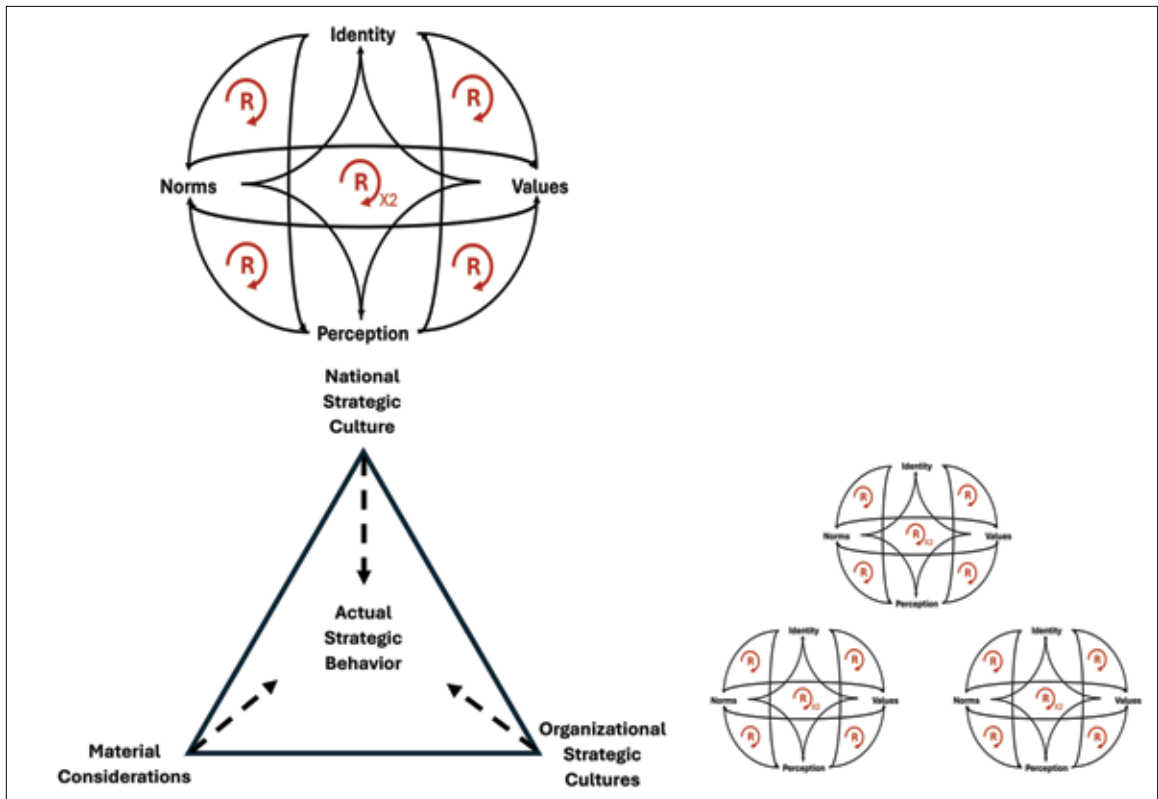


Source: authors.

culture can unravel. This model does not preclude the influence of exogenous factors such as geopolitical power differentials and differences in military might on manifest strategic behavior. The purpose of the model is to provide a means of assessing how the elements of strategic culture create a “complex whole” through their mutual influence.

We propose that in a particular case, not all these connections will be equally influential. A connection’s relevance will depend on a particular organization’s broader sociopolitical, cultural, geographic, historical, and geopolitical context. This is important because when certain connections are weak or non-existent, it is a relatively easier task to trace the causal effect of the remaining variables and identify the nodes that have the most influence in a particular strategic culture in that context. For instance, if, in a given context, there is a strong link between values and perception but comparatively weak links between these variables and norms, then normative behavior is less central to that strategic culture, and analysis of the potential impact of strategic culture should focus on the reinforcing relationship between values and perceptions. As an example, placing a positive value on democracy directly leads Western liberal democracies to perceive

Figure 4. The interaction of systems of national strategic culture, organizational cultures, and material considerations in the generation of strategic behavior.



Source: authors.

authoritarianism as a threat, without necessarily affecting how they go to war.⁴²

In other cases, strategic norms may skew perceptions, which in turn reinforce norms. Norms and values may reinforce one another. For example, strategic culture analysts have noted that historically the U.S. has placed a high value on preserving the lives of its troops. This has led to a norm of emphasizing force protection in its military behavior.⁴³ Norms may also influence identity and values. Some scholars have argued that reliance on industrial, high-tech warfare is a U.S. strategic culture norm.⁴⁴ Indeed, U.S. history includes examples of the military-industrial complex searching for technological solutions to U.S. threats and celebrating the workers who do so from Rosie the

Riveter to J. Robert Oppenheimer. Likewise, norms can directly reinforce values. Scholars have argued that building walls reinforced ancient Chinese defensive values drawn from Confucian ethics, or that Sun Tzu's emphasis on stratagem created a Chinese preference for irregular warfare tactics like disinformation and deception.⁴⁵

We propose this dynamic system of feedback and indirect influence as a model for operationalizing many of the concepts discussed in the strategic culture literature. In the end, the actual strategic behavior a nation manifests will be the result of the interactions of national strategic culture, sub-national organizational cultures and bureaucratic culture, and pragmatic material considerations (Figure 4).

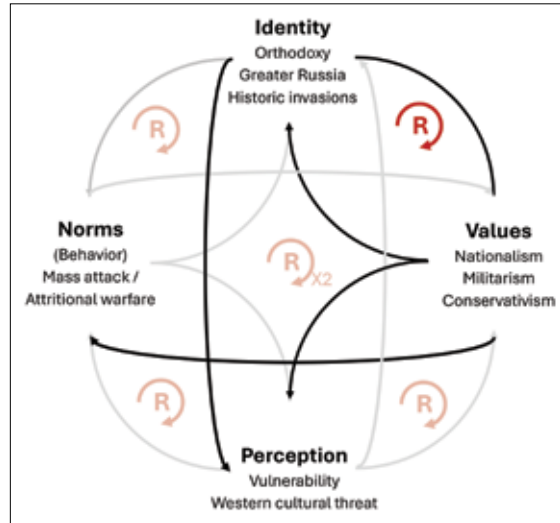
We argue that this model is sufficiently flexible to be adapted to varied strategic cultures yet structured enough to guide empirical data collection and the testing of propositions about a particular actor's strategic culture. Admittedly, complex systems models are difficult to test, and one reviewer recommended limited qualitative testing of key edges in the model as a means of rendering it scientifically testable. Such validation would be useful for both scholarly research and application by practitioners. Additionally, in our experience of applying complex models with practitioners, we have found that the conceptual clarity and immersion in the dynamics of the system provides users with deeper insights and conceptual clarity about the system. A brief example of how this model could be applied to Russian culture will hopefully make the point.

RUSSIAN STRATEGIC CULTURE

Applying the SCSM to the 2022 Ukrainian war illustrates how Russian strategic culture may manifest in relationships between identity, values, and perception. We have focused our analysis on what appears to be the prevailing views of Russia's prime decision-maker, Vladimir Putin. A complete analysis would consider other decision influencing units such as the Russian Orthodox Church (ROC), Russian intelligence apparatus, and the Russian military. Our illustration is meant to be suggestive and not necessarily comprehensive, but we hope it illustrates how some relationships may be more prominent than others and how the system and its strengths and weaknesses may be better understood. This understanding can then be used to anticipate strategic behavior and expose ways that the system of strategic culture may be weakened or even unraveled.

Core aspects of Russian national identity appear to drive the values Putin expresses in his political discourse. The centrality of Russian Orthodox identity reinforces Russian nationalism (i.e., its sense

Figure 5. Russian strategic culture as a complex system. Bold lines illustrate relationships described in vignette and does not imply that other connections are not also relevant. Rs indicate reinforcing relationships.



Source: authors.

of itself), as well as a highly militaristic culture, which is supported by the ROC.⁴⁶ The relationship between identity and religious values can be seen when prominent Russian Orthodox voices, including Patriarch Kirill, bless Russian military action driving the war in Ukraine and Russian nuclear silos and submarines incorporate Russian Orthodox priests and chapels.⁴⁷

Values reciprocally drive core aspects of Russian identity, forming a reinforcing loop. Putin emphasizes nationalism and militarism as important to the defense of the historical concept of a greater Russia.⁴⁸ In the wake of Russia's invasion of Ukraine, conservative values also reinforce Russian Orthodox identity on a global scale, as an increasing number of thinkers espousing traditional, nativist values have joined the ROC.⁴⁹

Russian identity can also impact how Russian decision-makers or populations perceive their

environment. The country's vulnerable geography and history of repeated invasions—from the Mongols to Napoleon to Hitler—have deepened its threat perception towards Ukraine, NATO, and Western countries and institutions.⁵⁰ Russia's heavily Orthodox identity has also been used to influence popular perception of its war in Ukraine as key ROC leaders cast Russia's invasion as a battle against perceived Western immorality.⁵¹

Likewise, Russian values may influence the country's perceptions. Putin emphasizes the importance of conservative Russian values, notably in areas such as gender and sexuality, and casts Ukraine's push for closer ties with the liberal West as a moral and existential threat to Russia.⁵² Values can also influence norms. The Russian military has historically favored the use of massed formations and exhibited an indifference to casualties, whether of their own troops or civilians, as was exhibited in the indiscriminate bombing of Syrian cities, and most recently in the Ukraine war which has been replete with indiscriminate bombing and the use of mass wave attacks in places like Bakhmut.⁵³ Considering IW tactics, Russian norms of using disinformation going back to Imperial Russia and through the Soviet era, reinforce its use of media to influence news cycles in its favor as well as targeted messaging to Ukrainian families before the 2022 invasion to undermine their will to fight.⁵⁴

We do not mean to imply that linkages do not exist elsewhere in this model of Russian strategic culture, but based on the literature, the links we have emphasized seem to be the strongest. A key reinforcing loop appears to exist between identity and values, which if weakened would cause this manifestation of Russian strategic culture to weaken and presumably lessen its influence on strategic behavior. Norms and perceptions are primarily influenced by identity and values without correspondingly strong reciprocal effects. Therefore, a weakening of the reinforcing loop between identity

and values could in turn weaken perceptions and norms, decreasing Russian threat perception and perhaps even weakening their use of brutal normative tactics. Conversely, changing threat perception with actions external to this system, for instance by voluntarily reducing NATO posturing, is unlikely to influence the system as a whole since we assessed the links from perception to other variables as weak.

CONCLUSION

This review of strategic culture aimed to provide an overview of the concept, its significance to deterrence, and provide a model that could be operationalized to inform questions of strategic culture. Each of these objectives is summarized below.

Strategic culture is an ancient concept, but its modern form developed in the 20th century context of WWII and the Cold War. A key unresolved issue is the relationship between strategic behavior and strategic culture. If the aim of using the strategic culture concept is to predict the totality of strategic behavior, then including those same behaviors in its definition is a tautology that undermines causal inference or prediction. However, we argue that inclusion of normative forms of national-security behavior in the definition, provided they are repeated, traditional, patterned behaviors does not undermine a causal understanding of all strategic behavior; traditions can reinforce perceptions and ideational aspects of strategic culture.

Furthermore, the evidence that a state's strategic culture has a causal impact on its strategic behavior is not conclusive. Resolving the causal effect of complex social phenomena is tremendously difficult and is exacerbated by competing social theories and the multitude of factors that can impact a state's security behavior. Therefore, we take the issue of the causal effect of strategic culture to be an empirical question that must be carefully tested in the particular context in which it is applied.

The areas in which there is consensus on strategic culture may aid application of strategic culture in context. The DTRA study and subsequent scholarship has identified four variables — *identity, values, norms, and perceptive lens* — that comprise strategic culture and social science methods that can be used to operationalize these and measure their effects. Identity, values, and perceptions can be accessed through systematic analysis of documents, discourse, and symbolism. Behavioral norms can be identified through historical analyses of actions. Each of these will be specific to a particular country's cultural, historic, and geographic context.

Another area of consensus is that the strategic cultures of all stakeholders that can influence strategic behavior must be accounted. Accounting for the interaction between these competing strategic cultures further adapts strategic culture to a specific context.

We have proposed a complex system model of strategic culture as a guide for adapting strategic culture to a particular context. Not every possible linkage in the model will be relevant in every context, allowing the model to be adapted to different contexts based on the strengths of the relationships between its variables and consideration of factors outside of strategic culture. In this way, we hope to provide a viable model of strategic culture that can explain and anticipate strategic behavior when appropriate, but that allows other factors to be accounted as well. We think the model can serve further scholarly work on strategic culture and be useful to practitioners by providing insight and clarity to the complexity of strategic culture. **PRISM**

Notes

¹ M. Elaine Bunn, "Can Deterrence Be Tailored?" *Strategic Forum* 255 (2007): 1–8, <https://digitalcommons.ndu.edu/strategic-forums/25/> and Ariel Cohen, "The 'Primakov Doctrine': Russia's Zero-Sum Game with the United States," *F.Y.I.*, no. 167 (1997): 1–6, <https://www.heritage.org/report/the-primakov-doctrine-russias-zero-sum-game-the-united-states>. Office of Net Assessment, China: Three Warfares (Washington, DC: Office of Net Assessment, Office of the Secretary of Defense, 2013), <https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Litigation\%20Release/Litigation%20Release%20-%20China-%20The%20Three%20Warfares%20%20201305.pdf>.

² Sun Tzu, *The Art of War* (London: Oxford University Press, 1963), 84.

³ Margaret Mead, *And Keep Your Powder Dry: An Anthropologist Looks at America* (New York: William Morrow Company, 1942); Ruth Benedict, *The Chrysanthemum and the Sword: Patterns of Japanese Culture* (New York: Houghton Mifflin, 1946).

⁴ Nathan C. Leites, *The Operational Code of the Politburo* (Santa Monica, CA: RAND Corporation, 1951), https://www.rand.org/pubs/commercial_books/CB104-1.html.

⁵ Jack L. Snyder, *The Soviet Strategic Culture: Implications for Limited Nuclear Operations* (RAND Corporation, Santa Monica, California, 1977). <https://www.rand.org/content/dam/rand/pubs/reports/2005/R2154.pdf>.

⁶ Alastair Ian Johnston, *Cultural Realism: Strategic Culture and Grand Strategy in Chinese History* (Princeton: Princeton University Press, 1995). Colin S. Gray, "Strategic Culture as Context: The First Generation of Theory Strikes Back," *Review of International Studies* 25 (1999): 49–69. Colin S. Gray, "Out of the Wilderness: Prime Time for Strategic Culture," in *Comparative Strategic Cultures Curriculum Project*, ed. J. A. Larsen (Washington, DC: Defense Threat Reduction Agency Advanced Systems and Concepts Office, 2006), 1–30, <https://apps.dtic.mil/sti/pdfs/ADA521640.pdf>.

⁷ Jeffrey A. Larsen, ed., *Comparative Strategic Cultures Project: Assessing Strategic Culture as a Methodological Approach to Understanding WMD Decision-Making by States and Non-State Actors* (Washington, DC: Defense Threat Reduction Agency Advanced Systems and Concepts Office, 2006), <https://apps.dtic.mil/sti/pdfs/ADA521640.pdf>.

⁸ Kerry M. Kartchner, Briana D. Bowen, and Jeannie L. Johnson, eds., *Routledge Handbook of Strategic Culture* (New York: Routledge, 2024).

⁹Jeannie L. Johnson, “Strategic Culture: Methodologies for a Research Program,” in *Comparative Strategic Cultures Curriculum Project*, ed. J. A. Larsen (Washington, DC: Defense Threat Reduction Agency Advanced Systems and Concepts Office, 2006), 1–25, <https://apps.dtic.mil/sti/pdfs/ADA521640.pdf>.

¹⁰Christopher P. Twomey, “Chinese Strategic Culture: Survey and Critique,” in *Comparative Strategic Cultures Curriculum Project*, ed. J. A. Larsen (Washington, DC: Defense Threat Reduction Agency Advanced Systems and Concepts Office, 2006), 1–21, <https://apps.dtic.mil/sti/pdfs/ADA521640.pdf>.

¹¹Kartchner, Kerry M., Briana D. Bowen, and Jeannie L. Johnson, eds., *Routledge Handbook of Strategic Culture* (New York: Routledge, 2024). Dmitry Adamsky, *The Russian Way of Deterrence: Strategic Culture, Coercion, and War* (Stanford: Stanford University Press, 2023). Graeme P. Herd, *Understanding Russian Strategic Behavior: Imperial Strategic Culture and Putin’s Operational Code* (New York: Routledge, 2022). Michael Pillsbury, *The Hundred-Year Marathon: China’s Secret Strategy to Replace America as the Global Superpower* (New York: Griffin, 2015). Ashley J. Tellis, “Overview: Understanding Strategic Cultures in the Asia-Pacific,” in *Understanding Strategic Cultures in the Asia-Pacific*, ed. A. J. Tellis, A. Szalwinski, and M. Wills (Seattle, WA: National Bureau of Asian Research, 2016), <https://www.nbr.org/publication/strategic-asia-2016-17-understanding-strategic-cultures-in-the-asia-pacific/>.

¹²Alan Bloomfield, “Time to Move On: Reconceptualizing the Strategic Culture Debate,” *Contemporary Security Policy* 33, no. 3 (2012): 465, <https://doi.org/10.1080/13523260.2012.727679>

¹³Antulio J. I. Echevarria, “*Strategic Culture: More Problems than Prospects*,” *Military Strategy Magazine* 3, no. 2 (2013): 4–7, <https://www.militarystrategymagazine.com/article/strategic-culture-more-problems-than-prospects/>

¹⁴Bunn, “Can Deterrence Be Tailored,” 2007, 2.

¹⁵Timothy L. Thomas, *China’s Military Strategy: Basic Concepts and Examples of its Use* (Fort Leavenworth, KS: Foreign Military Studies Office, 2014), XX, <https://fmso.tradoc.army.mil/2014/chinas-military-strategy-basic-concepts-and-examples-of-its-use-timothy-l-thomas/>.

¹⁶White House, *National Security Strategy* (Washington, D.C., 2022), <https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf>. Department of Defense, *National Defense Strategy of the United States of America* (Washington, D.C., 2022), <https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF>.

¹⁷White House, *National Security Strategy of the United States of America* (Washington, D.C., 2025), <https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf>. Department of War, *National Defense Strategy: Restoring Peace Through Strength for a New Golden Age of America* (Washington, D.C., 2026), <https://media.defense.gov/2026/Jan/23/2003864773/-1/-1/0/2026-NATIONAL-DEFENSE-STRATEGY.PDF>.

¹⁸See special edition, “Strategic Cultures and Security Policies of the Asia-Pacific,” *Contemporary Security Policy* 35, no. 2 (2014).

¹⁹Judith Goldstein and Robert O. Keohane, “Ideas and Foreign Policy: An Analytical Framework,” in *Ideas and Foreign Policy: Beliefs, Institutions, and Political Change*, ed. J. Goldstein and R. O. Keohane (Ithaca: Cornell University Press, 1993). Leo Blanken and Justin Overbaugh, “Distinguishing Principled Beliefs from Causal Beliefs in American Foreign Policy,” *Journal of Strategic Security* 16, no. 4 (2023): 90–104, <https://doi.org/10.5038/1944-0472.16.4.2158>.

²⁰Colin S. Gray, “National Style in Strategy: The American Example,” *International Security* 6, no. 2 (1981): 21–47. Johnston, *Cultural Realism*. Bradley S. Klein, “Hegemony and Strategic Culture: American Power Projection and Alliance Defence Politics,” *Review of International Studies* 14, no. 2 (1988): 133–48. Eugene B. Rumer and Richard Sokolsky, *Etched in Stone: Russian Strategic Culture and the Future of Transatlantic Security* (Washington, DC: Carnegie Endowment for International Peace, 2020), <https://carnegieendowment.org/research/2020/09/etched-in-stone-russian-strategic-culture-and-the-future-of-transatlantic-security?lang=en>.

Andrew Scobell, “China’s Real Strategic Culture: A Great Wall of the Imagination,” *Contemporary Security Policy* 35, no. 2 (2014): 211–26, <https://doi.org/10.1080/13523260.2014.927677>. Snyder, *The Soviet Strategic Culture*. Nina Tannenwald, “The Nuclear Taboo: The United States and the Normative Basis of Nuclear Non-Use,” *International Organization* 53, no. 3 (1999): 433–68.

²¹Thomas U. Berger, *Cultures of Antimilitarism: National Security in Germany and Japan* (Baltimore: Johns Hopkins University Press, 1998). Elizabeth Kier, “Culture and Military Doctrine: France between the Wars,” *International Security* 19, no. 4 (1995): 65–93. Edward Lock, “Refining Strategic Culture: Return of the Second Generation,” *Review of International Studies* 36, no. 3 (2010): 685–708.

²²Allison, Graham T. and Morton H. Halperin, “Bureaucratic Politics: A Paradigm and Some Policy Implications,” *World Politics* 24 (1972): 40–79.

- ²³ Christopher M. Jones, “Bureaucratic Politics and Organizational Process Models,” *Oxford Research Encyclopedia of International Studies*, (2017), <https://oxfordre.com/internationalstudies/view/10.1093/acrefore/9780190846626.001.0001/acrefore-9780190846626-e-2>.
- ²⁴ Jeannie L. Johnson, “Strategic Culture in the Service of Strategy: The Founding Paradigm of Colin S. Gray,” *Comparative Strategy* 40, no. 2 (2021): 179–84, <https://doi.org/10.1080/01495933.2021.1880833>
- ²⁵ Johnston, Cultural Realism . Since Johnston, research and debate about Chinese and in particular PRC strategic culture has continued. See Twomey, “Chinese Strategic Culture,” and Scobell, “China’s Real Strategic Culture.”
- ²⁶ Adamsky, Dimitry, *The Russian Way of Deterrence*. N. Eitelhuber, “The Russian Bear: Russian Strategic Culture and What it Implies for the West,” *Connections* 9, no. 1 (2009): 1–28, <https://connections-qj.org/article/russian-bear-russian-strategic-culture-and-what-it-implies-west>.
- ^{Fritz} W. Ermarth, “Russia’s Strategic Culture: Past, Present, and... in Transition?,” in *Comparative Strategic Cultures Curriculum Project*, ed. J. A. Larsen (Washington, DC: Defense Threat Reduction Agency Advanced Systems and Concepts Office, 2006), 1–21, <https://apps.dtic.mil/sti/pdfs/ADA521640.pdf>.
- Herd, *Understanding Russian Strategic Behavior*. Rumer and Sokolsky, Etched in Stone. Snyder, *The Soviet Strategic Culture*.
- ²⁷ Gray, “National Style in Strategy,” “Strategic Culture as Context,” “Out of the Wilderness.” Johnson, “Strategic Culture.” Jeffrey W. Legro, “Culture and Preferences in the International Cooperation Two-Step,” *The American Political Science Review* 90, no. 1 (1996): 118–37. Snyder, *The Soviet Strategic Culture*.
- ²⁸ Snyder, *The Soviet Strategic Culture*, 9.
- ²⁹ Legro, “Culture and Preferences in the International Cooperation Two-Step,” 121.
- ³⁰ Bloomfield, “Time to Move On.” Gray, “Out of the Wilderness.” Kier, “Culture and Military Doctrine.” Legro, “Culture and Preferences in the International Cooperation Two-Step.” Snyder, *The Soviet Strategic Culture*.
- ³¹ Johnston, Cultural Realism . Nina Tannenwald, “The Nuclear Taboo: The United States and the Normative Basis of Nuclear Non-Use,” *International Organization* 53, no. 3 (1999): 433–68.
- ³² Gray, “Out of the Wilderness.”
- ³³ Jack L. Snyder, “Anarchy and Culture: Insights from the Anthropology of War,” *International Organization*, 56, no. 1 (2002): 7–45.
- ³⁴ Donella H. Meadows, *Thinking in Systems* (White River Junction, Vermont: Chelsea Green Publishing, 2008).
- ³⁵ Claudio Cioffi-Revilla, *Introduction to Computational Social Science* (London: Springer, 2014). Claudio Cioffi-Revilla and Pedro P. Romero, “Modeling Uncertainty in Adversary Behavior: Attacks in Diyala Province, Iraq, 2002–2006,” *Studies in Conflict & Terrorism* 32, no. 3 (2009): 253–76. Josh Kerbel, “Our Cold War Frame Distorts More than Just Our View of China,” *The Hill* (2021), <https://thehill.com/opinion/national-security/586921-our-cold-war-frame-distorts-more-than-just-our-view-of-china?r=1>. Lawrence A. Kuznar, “The COVID-19 Pandemic: Gray Rhinos, Complexity, Prediction, and National Security,” in *Contagion Effect: Radicalization, Unrest, and Competition in the COVID-19 Era*, ed. A. Farhadi and A. Masys (New York: Springer-Verlag, 2022), 167–84. Lawrence A. Kuznar and Stacey Pollard, “Conclusion: The Pandemic System,” in *A World Emerging from Pandemic: Implications for Intelligence and National Security*, ed. S. Pollard and L. A. Kuznar (Bethesda, Maryland: National Intelligence University Press, 2022). Ian S. Lustick and Philip Tetlock, “The Simulation Manifesto: The Limits of Brute-Force Empiricism in Geopolitical Forecasting,” *Futures & Foresight Science* (2021): e64, <https://doi.org/10.1002/ffo2.64>.
- ³⁶ Edward Burnett Tylor, *Origins of Culture [Primitive Culture]* (London: John Murray, 1958).
- ³⁷ Clifford Geertz, *Interpretation of Cultures* (New York: Basic Books, 1973).
- ³⁸ Jeannie L. Johnson, “Strategic Culture Scholarship: A User’s Guide to the Cultural Topography Methodology,” in *Routledge Handbook of Strategic Culture*, ed. Kerry M. Kartchner, Briana D. Bowen, and Jeannie L. Johnson (New York: Routledge, 2024).
- ³⁹ Pierre Bourdieu, *Outline of a Theory of Practice* (Cambridge: Cambridge University Press, 1977).
- ⁴⁰ Gray, “National Style in Strategy.” Robin Luckham, “Of Arms and Culture,” *Current Research on Peace and Violence* 7, no. 1 (1984): 1–64. Thomas G. Mahnken, “United States Strategic Culture,” in *Comparative Strategic Cultures Curriculum Project*, ed. J. A. Larsen, 1–25 (Washington, DC: Defense Threat Reduction Agency Advanced Systems and Concepts Office, 2006), <https://apps.dtic.mil/sti/pdfs/ADA521640.pdf>. Anna Antczak, “Russia’s Strategic Culture: Prisoner of Imperial History?” *Athenaeum* 60 (2018): 223–42, <https://doi.org/10.15804/athena.2018.60.13>. Scobell, “China’s Real Strategic Culture,” <https://doi.org/10.1080/13523260.2014.927677>; Thomas, *China’s Military Strategy*. Tiejun Zhang, “Chinese Strategic Culture: Traditional and Present Features,” *Comparative Strategy* 21, no. 2 (2002): 73–90, <https://doi.org/10.1080/01495930290043056>.
- ⁴¹ Johnson, “Strategic Culture.”

⁴² White House, *National Security Strategy*. (Washington, DC, 2022) <https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf>.

⁴³ Gray, “National Style in Strategy.” Mahnken “United States Strategic Culture.”

⁴⁴ Gray, “National Style in Strategy.” Luckham “Of Arms and Culture.”

⁴⁵ Johnston Cultural Realism . Scobell “China’s Real Strategic Culture.” Twomey “Chinese Strategic Culture.” Mahnken Secrecy & Strategem.

⁴⁶ Dmitry Adamsky, *Russian Nuclear Orthodoxy: Religion, Politics, and Strategy* (Stanford, California: Stanford University Press, 2019). Eitelhuber, “The Russian Bear.” Herd, *Understanding Russian Strategic Behavior* . Polina Sinovets, “From Stalin to Putin: Russian Strategic Culture in the XXI Century, Its Continuity, and Change,” *Philosophy Study* 6, no. 7 (2016), <https://doi.org/10.17265/2159-5313/2016.07.002>. Stanislaw Zarobny and Agnieszka Salek-Iminska, A. “Conditions of the Russian Federation’s Strategic Culture and Its Impact on Russia’s Foreign Policy,” *Security Dimensions* 35 (2021): 65–80, <https://doi.org/10.5604/01.3001.0014.8240>.

⁴⁷ Adamsky, *Russian Nuclear Orthodoxy*, 2019. G. Fagan, “How the Russian Orthodox Church is Helping Putin’s War,” *Time* (2022), <https://time.com/6167332/putin-russian-orthodox-church-war-ukraine/>

⁴⁸ Vladimir Putin, *Address by the President of the Russian Federation* (2022) <http://en.kremlin.ru/events/president/news/67843>.

⁴⁹ O. Yousef, “Orthodox Christian Churches Are Drawing in Far-Right American Converts,” NPR (2022), <https://www.npr.org/2022/05/10/1096741988/orthodox-christian-churches-are-drawing-in-far-right-american-converts>.

⁵⁰ Dutt, D. (2023). *Russian Strategic Culture and Its Implications on the Russia-Ukraine War*. The United Service Institution of India . <https://usiofindia.org/publication/cs3-strategic-perspectives/russian-strategic-culture-and-its-implications-in-the-russia-ukraine-war/>. Eitelhuber, “The Russian Bear.” E. Gotz and J. Staun, “Why Russia attacked Ukraine: Strategic culture and radicalized narratives. *Contemporary Security Policy* 43(3), 482-497, <https://doi.org/10.1080/13523260.2022.2082633>. Herd, *Understanding Russian Strategic Behavior*. Sinovets, “From Stalin to Putin.”

⁵¹ Fagan, “How the Russian Orthodox Church is Helping Putin’s War,” 2022; Herd, *Understanding Russian Strategic Behavior*, 2022.

⁵² A. Faiola, “Analysis: How Putin is Weaponizing ‘Traditional Values’ to Defend Russian Aggression in Ukraine,” *Washington Post* (2022) Retrieved from <https://www.washingtonpost.com/world/2022/03/23/putin-russia-ukraine-orthodox/>. Herd *Understanding Russian Strategic Behavior* 2022; Putin 2022.

⁵³ Antczak, 2018; Eitelhuber, “The Russian Bear” 2009; Ermarth, “Russia’s Strategic Culture” 2006; German, “Harnessing Protest Potential” 2020. Dmitry Adamsky, “Continuity in Russian Strategic Culture” 2020. “In the ‘Bakhmut meat grinder’, deadlocked enemy forces slog it out” *The Guardian*, December 10, 2022, <https://www.theguardian.com/world/2022/dec/10/russia-ukraine-war-bakhmut-meat-grinder-deadlock>.

⁵⁴ Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Strauss, and Giroux 2020). Todd C. Helmus & Khrystyna Holynska, *Ukrainian Resistance to Russian Disinformation: Lessons for Future Conflict* (Santa Monica, California: RAND Corporation 2024).

Maskirovka and the Olympics

The Russian Choice to Initiate Conflict During the Olympic Games

By G. Doug Davis, Michael Slobodchikoff, and Elizabeth Holley Dubose

The Olympic Games have been celebrated as a platform for peace and unity but recently have been exploited as a geopolitical tool to provide cover for aggressive military campaigns. Russia has initiated multiple invasions that coincided with the Olympics and was able to strategically use the games as a distraction to weaken international opposition. This paper examines three instances where Russia used the Olympic games as a tool to advance its goals: Georgia in 2008, Crimea in 2014, and Ukraine in 2022. Russia uses the Games as a cover for aggression as part of its broader strategy rooted in *maskirovka*—the Russian military concept of deception and misdirection. Moscow can use Olympic diplomacy as a shield and stage to advance its geopolitical interests, and this undermines the goal of maintaining the Olympics as a politically neutral and unifying event.¹

The *maskirovka* tactic has its roots in Soviet military doctrine and draws on several strategies that include disinformation, misdirection, and reflexive control that are designed to confuse and mislead opponents by targeting their perceptions. Russia exploits global media events, such as the Olympic Games, to manipulate the international media and weaken and delay global responses to its aggressive action. *Maskirovka* uses existing media events in the West as a strategic fog to prevent the international community from focusing on Moscow's operations and this allows Russia to undertake offensive operations without facing immediate retaliation. This approach took place in the 2014 Sochi Olympics where unmarked military forces, reported as

Dr. G. Doug Davis, Ph.D. is a professor of Political Science at Troy University where he focuses on irregular warfare, NATO, international security, diplomacy, and Eastern and Central Europe. He has published four books including *The Challenge to NATO: Global Security and the Atlantic Alliance* and *American Global Leadership: Ailing U.S. Diplomacy and Solutions for the Twenty-First Century*.

Michael Slobodchikoff is Professor of Political Science and the Founding Director of the Center for Eastern and Central European, Russian, and Eurasian Studies at Troy University. His research focuses on the dynamics of international alliances, treaty networks, and the geopolitical tensions surrounding NATO expansion. He has published on conflict resolution, great power politics, and Russian foreign policy, with notable works including *Strategic Cooperation: Overcoming the Barriers of Global Anarchy* and *Building Hegemonic Order Russia's Way*.

Elizabeth Holley Dubose is a Troy University graduate and political science research scholar. She is currently pursuing legal studies at Drake Law School.

'little green men, entered and emerged in Crimea to 'protect' ethnic Russians.² The Olympics provided Russia with an opportunity to take the Crimea without interference from Western powers.³

Russia uses international events to serve its military objectives, and this is not merely a practical approach but is an example of its reflexive control doctrine where Moscow gets its adversaries to make decisions that inadvertently advance Russian objectives. *Maskirova* does not only confuse or distract its opponents but accurately understands and predicts the adversary's response which allows Moscow to exploit this for its interests. When the 2022 Ukrainian invasion began, Putin waited until the Olympics ended to undertake his military operation. According to Wong and Barnes, China asked Russia to delay its invasion until the Olympic Games finished so that the war would not diminish Beijing's time in the global spotlight.⁴ This also served Moscow's interests and showed that *maskirovka* is adaptable so that its military activity can be adjusted to serve broader strategic needs.

While deception is integral to *maskirovka*, this extends further to incorporate political, military, and information operations to broadly coordinate activities that obscure the military operations.⁵ Pynnöniemi and Rácz show how this creates a 'fog of falsehood' that allows Russia to consolidate its offensive ground gains before its adversaries can coordinate their response.⁶ For example, the global media was focused on the 2008 Beijing Olympics when Russia invaded Georgia. The Russian media campaign marketed its operation as a defensive maneuver to protect South Ossetians. This shows how Moscow employs *maskirovka* not only to achieve military goals but simultaneously to shape the international narrative.⁷ To make this more effective, Russia times its military operations to coincide with the global media events, such as the Olympics, which allows it to move its armed forces

into neighboring states without risking immediate, coordinated retaliation from the West.

One advantage to initiating its military interventions during the Olympics is that the initial diplomatic response and media scrutiny is defused. The Games attract a global audience and, since the games are every four years, it becomes more costly for viewers to divert their attention to international conflicts that do not directly involve them. The Russian *maskirovka* strategic approach provides cover to protect its interests while engaging in hybrid warfare. Modern conflicts have a strategic ambiguity where global audiences are unable to distinguish between conflict and peace—military engagement is increasingly 'gray' and more difficult to perceive.⁸ This tactic allows Moscow to behave aggressively and conduct offensive operations while denying any responsibility for the attacks. Plausible deniability allows Russia to market itself as a stabilizing international force even while violating the sovereignty of neighboring states. Ironically, while the Olympics work to bring humanity together to admire outstanding athletic performances, it also is a time where the international system is vulnerable. The very same forces that bring people together give revisionist states, like Russia, cover to engage in military operations and face less media scrutiny.

The Russians employed *Maskirovka* during the Olympics and used a clever plan to use international media events as a diversionary maneuver. In every instance when Moscow initiated conflict during the Olympics, from Georgia to Ukraine, there was a calculated, strategic approach that effectively combined military force, diplomatic diversion, and global media. Russia was able to exploit the Olympic Games and use its global media presence to lessen the scrutiny it would otherwise face when it conducted aggressive military operations. The international community needs to assess the strategic vulnerability it faces when there is a global media event. This paper examines how Putin

employs *maskirovka* to minimize the opposition and retaliation caused by aggressive military moves. He effectively exploits the Games and uses the media attention to undertake risky operations at a time when it is most advantageous. The West needs to develop a response that will preserve the Olympic symbolism and provide a way to effectively respond to global crises that emerge during the games.

The Olympic Games have historically provided a means to bring together people throughout the world where the world's greatest athletes compete peacefully. One long-held tradition is the Olympic Truce, which attempts to get states that are at war to lay down their arms for the competition. When successful, the Games provide hope to the world and work to increase internal goodwill and friendship. These goals have been threatened and come under attack as pariah states, such as Russia, seek to use the Olympics as a diversion to shield them from negative consequences when they initiate offensive military operations. Ironically, Russia tried to gain prestige by hosting the 2014 Winter Games and sought to use the Olympics as a soft power instrument to advance its image as a state promoting international camaraderie and stability. Putin followed a Machiavellian strategy by initiating undertaking the Crimean hybrid operation during the games he hosted.⁹ Russia was able to gain prestige by hosting the Olympics but used this to simultaneously bring about the Crimean annexation.

Russia has used the Olympics as a diversion for its military aggression for the past twenty years as it launched invasions during the 2008, 2014, and 2022 Games. The 2008 Beijing Olympics provided cover for Moscow's Georgia invasion. This was repeated six years later when Russia hosted the 2014 Winter Games in Sochi. Putin received positive international media coverage by hosting the games and used this to distract the world as irregular forces moved into Crimea; 'Little Green Men' came to the peninsula without any insignia indicating that they

were Russian forces and took over the area militarily and provided the pretext for Moscow to annex Crimea. The 2022 Beijing Winter Olympics provided the background for Russia to place troops on the Ukrainian border. Putin and Chinese leader Xi Jinping met prior to the Games and Russia agreed to not initiate its invasion during the games.¹⁰ The Olympics finished on February 20th and Russia invaded four days later. It is not a coincidence that Putin has used the Olympic games multiple times to provide cover for his foreign military campaigns and this shows that global media events, such as the Olympics, are an important strategic factor for determining the timing of its military engagements.¹¹

Putin focuses on using his strategic arsenal to prioritize his influence in the former Soviet states.¹² He has used the Olympics as a distraction that allowed him to successfully make territorial gains in Georgia and Ukraine. In the West this strategic approach is termed hybrid warfare and military operations are combined with diplomatic, economic, and media events to allow Russia to reach its objectives and leaving its adversaries confused and unable to formulate a quick response.¹³ Each time Russia timed its military aggression to coincide with the Olympics it was able to gain time and delay the West's response. It stopped its adversaries from agreeing to a quick, clear, and cohesive response. The distraction was a convenient excuse for some Western leaders to ignore the aggression and to not respond meaningfully. Russia was also successful in generating a narrative that its intervention coincided with the Olympic truce by defending its action as a protective measure to protect vulnerable Russian populations. The Olympics monopolized media attention and worked to weaken or prevent any quick Western response to its aggression. Putin was strategically successful in his choice to initiate attacks during the Olympics.

Putin's success in using the Olympic Games to prevent the West from responding to military aggression provides some insights into Russia's geopolitical ambitions and shows us strategic vulnerabilities in the Western alliance.¹⁴ While Moscow has repeatedly invaded neighboring states during the Olympics, the Western response has been erratic and the diplomatic effort to come together and formulate a response was prevented and delayed due to the consular events related to the games. While the IOC strives to be neutral and to keep the sporting events free from politics, this has not stopped states, like Russia, from exploiting the event to advance its geopolitical interests. The intense international focus on the games prevented media resources and time from focusing on the geopolitical crisis.¹⁵ The IOC's goals cannot prevent states from using the games as a diversion to advance their national interests. The international community has not been able to provide a method to overcome this vulnerability and, until there is an adequate response, the Games are likely to be used by revisionist states.

RESEARCH DESIGN

This research uses the case study method to examine Russian aggression during the Olympic Games and examines the 2008 Georgia invasion, the 2014 Crimean annexation, and the 2022 Ukraine War. Our research examines media coverage, official statements, and historical and scholarly works to examine Russia's motivations and goals, the international community response, and the media's role in building discourse which is critical for public perception. These cases show how Russia gained a strategic advantage that undermined its adversaries by initiating conflict during the Olympic games. Our analysis has three goals: (i) to show how Russia used the Olympic media coverage to serve its geopolitical goals; (ii) to assess the strategic effectiveness by examining international community's response; (iii) and to identify the consequences for

international diplomacy and global security.

This case study seeks to broadly assess how Russia uses the media as a diversionary tool to advance its strategic interests. We hope to provide some insights into sports diplomacy, and the role international institutions play in preventing great powers from the strategic use of global media events. While the Olympics have traditionally served as a unifying event to build bridges and promote international peace, these global events are likely to be exploited by revisionist states wishing to engage in military conquests while the world is focused on the Games. International institutions and Western states need to reassess how they manage global media events and take preventative measures to mitigate the vulnerabilities that aggressive states exploit. This action would work to preserve the Games' mission to be a unifying force and to advance the global cause of peace.¹⁶

THE 2008 BEIJING OLYMPICS AND THE RUSSIAN INVASION OF GEORGIA

2008 Beijing Summer Olympics provided China with a platform to highlight its development, economic prowess, and new global influence. While the world was focusing on the athleticism and pageantry present in the competition, geopolitical tension was increasing in the Caucasus. August 8, 2008 was the opening day for the Olympics and was the date Russia chose to initiate its military conquest where it would take two Georgian provinces: Abkhazia and South Ossetia. There was a small independence movement within South Ossetia which was supported by Russia. Moscow aggravated situation by the granting Russian citizenship to many people in South Ossetia. Georgia, led by President Mikheil Saakashvili, wanted to assert sovereignty over the region and consolidate his political control.¹⁷ He was motivated by the desire to gain membership in NATO and the EU and es-

establish internal support for membership in European institutions.¹⁸ Russia was deeply concerned with NATO expansion and saw Saakashvili's initiatives as a direct threat to its security.

Tensions grew four months prior to the Olympics when Jaap de Hoop Scheffer, NATO's Secretary General, announced at the 2008 Bucharest Summit that Ukraine and Georgia would eventually become members in the Atlantic Alliance. France and Germany would not agree to the NATO Membership Action Plan (MAP), which would create a fast-track for joining the Atlantic Alliance. The announcement was troubling to Moscow which perceived this as a serious security threat. Upon hearing the news, Russia reacted and sent a thousand additional troops to Abkhazia to prevent any resolution between Tbilisi and Abkhazia. A border dispute would make it impossible for Georgia to be admitted to the alliance. Moscow initiated a diplomatic campaign in European capitals to prevent Georgia from being granted a MAP for NATO membership when the Atlantic Alliance Foreign Ministers would gather in December.¹⁹ Russia believed that NATO expansion into former Soviet states would constitute a direct threat to its domestic security and it worked aggressively to maintain its geopolitical dominance within this region.²⁰ Georgia countered with its own diplomatic effort actively waging a campaign to secure support before the December foreign minister meeting. The tension grew and turned violent when Saakashvili sent troops into South Ossetia, which was a region of Georgia, and this provided a pretext for Russia to justify its military invasion, which it stated was to protect Russian citizens and made an absurd claim that it was to prevent a genocide. Dmitry Medvedev was President of Russia during the invasion, and he argued that the invasion was morally legitimate because it was a temporary defensive maneuver to protect civilians.²¹ Moscow marketed the moral rightfulness of its invasion

which gave it additional time to maneuver without facing an international response.²²

Russia was able to provoke Saakashvili to send forces into South Ossetia during a time when it was most advantageous for Moscow. The military operations were precisely timed and illustrates the *maskirovka* doctrine in action—the Olympics provided a distraction that kept the Western world from formulating an immediate response to the Georgian crisis.²³ The United States and most Western states continued to focus the majority of their media coverage on the Games. The Olympics produced a global media event that worked to pull viewers away from the day-to-day news and worked to lessen the pressure to create an immediate response.²⁴ The Olympics functioned as a 'media shield' that worked to minimize coverage. NBC covered the Games for the United States, and it invested heavily in the event. It paid \$2.3 billion to win the contract to cover the Olympics from 2004 to 2008 and then needed to attract a large audience to cover the expenses.²⁵ It was successful as an average 27 million viewers tuned in to watch the Olympics daily.²⁶ To devote more coverage to the Georgian War, NBC would have risked a financial loss on the games—the 2008 U.S. Presidential election was also receiving significant air time and this further reduced the available airtime. The American media coverage focused on how the two presidential candidates would respond to the crisis, so it became a domestic issue rather than an international emergency that needed a quick response.²⁷

The Russian, state-controlled media created a different narrative and defended the conflict as a defensive intervention to protect vulnerable Russian-speaking population in South Ossetia. Moscow was able to build domestic support for this fight by arguing that it was necessary to protect Russia's interests and prevent NATO expansion. The national media was able to bring the Russian people to endorse their interpretation and use it to foster national pride

and unity.²⁸ The Russian domestic marketing tied the operation to the broader Olympic theme which focused on peace and unity. The Orwellian argument worked domestically while the Western media focused on covering the Olympic games.

The international reaction to Russia's invasion was slow and cautious. France held the EU presidency and President Nicolas Sarkozy was able to push through a ceasefire agreement on August 12th, four days into the conflict. The agreement required both Georgia and Russia to end combat and to withdraw from the battlefield. However, the agreement has been criticized because it accepted Russia's territorial gains and allowed Moscow to maintain soldiers in South Ossetia and Abkhazia, which gave Russia de-facto control over these regions. Sarkozy was eager for the conflict to end and was less concerned with the precedent this set—Russia was able to change international borders through offensive military action. It increased the likelihood that this strategy, which was successful, would be used again.²⁹ The weak international response provides insights into the geopolitical complexities at that time. The Bush administration sought to end the conflict but had no interest in escalating it. The U.S. was working to manage its relations with Moscow and was also focused on the Olympics. Analysts suggest that the weak response worked to encourage Russia to conduct new offensive operations in the future as one lesson was that regional aggressiveness would not provoke serious Western responses.³⁰

The 2008 Beijing Olympics generated extensive media coverage that was exploited by Russia to deflect criticism when it invaded Georgia. Moscow successfully used the Olympics as a distraction to weaken the international response. The short duration allowed Russia to complete the war during the Olympics and the ceasefire agreement was reached before serious discussion could take place in the Western media. Putin and Medvedev were able to initiate a war that changed international

borders during a time when the West was otherwise distracted by the Olympic Games, which provided Russia with the ability to make geo-political gains without incurring a serious Western response.³¹ The strategy worked and made it more likely that this would be repeated.

2014 SOCHI WINTER OLYMPICS AND THE RUSSIAN ANNEXATION OF CRIMEA

Russia hosted the 2014 Winter Olympics and used the Games to showcase its national culture and to market its international economic and political image. The government spent over \$55 billion to build the infrastructure to host the events, spectators, and media centers and it was the most expensive Winter Games in history. Putin sought to host the Games to advance Russia's geopolitical image and to make a statement showing that Russia was a serious international player.³² The Olympics provided an opportunity to show Russian resurgence after the difficult post-Soviet period. Sochi is a resort city on the Black Sea that also showed the geographic beauty and cultural heritage to change Russia's international image. While Russia was projecting itself internationally, its relations with Ukraine were growing more tense and a serious confrontation was percolating.

Tensions grew in November 2013 when Viktor Yanukovich decided not to sign the European Union association agreement and instead chose to strengthen its ties to Russia. The Euromaidan protest movement started on November 21st and gained strength, forcing Yanukovich to flee the country in February 2014. After Yanukovich fled, pro-Russian protests emerged in Crimea, located in the Black Sea and internationally recognized as part of Ukraine, and created the justification Putin needed to launch an irregular campaign where special forces the peninsula claiming to defend ethnic Russians. Crimea is home to Sevastopol Naval Base which houses the

Russian Black Sea Fleet and provides Russia with a warm-water port and allows the Kremlin to project power into the Mediterranean.

The Sochi Olympics provided Russia with the strategic cover to be able to initiate its plans to annex the Crimea.³³ The Games took place on February 7 to February 23 and Yanukovych fled Ukraine on February 22. Russia began executing its plan to take the Crimea by sending unmarked troops who would manifest themselves in the peninsula by February 27th. Since the soldiers has no insignia or other visible ties connecting them to Russia, they were known as “little green men.” These irregular forces occupied and controlled key Crimean areas. This caused confusion in the West which made it difficult to clearly blame Russia in the popular media as Moscow denied any knowledge or responsibility.³⁴ When the international community understood what happened, the Russian forces controlled all the key infrastructure points on the peninsula.³⁵ A quick referendum was held and the residents voted to join the Russian Federation.

Russia employed *maskirovka* during the Sochi Olympics by creating a broad effort that combined military, political, and informational tactics which allowed it to make territorial gains that minimized international opposition.³⁶ The operation coincided with the Olympic closing and made international coordination to gain consensus for a response difficult.³⁷ The host nation gains economic and reputational benefits and the additional standing may allow the goodwill that comes from hosting the games work to protect the host country from criticism.³⁸ In this case, Russia gained reputational prowess that it was able to use to deflect the international censure it would otherwise receive for initiating military conflict. The Sochi Olympics media coverage worked to impact how the international public perceived the Crimean annexation. The Western media covered multiple Russian domestic laws that were opposed to Western norms, such as the anti-LGBTQ promotion

to adolescents’ laws and the limitations on press freedom.³⁹ This focus inadvertently worked to lessen decrease coverage for the tension in Ukraine—including its change in leadership.⁴⁰ Several global leaders, including President Barack Obama, chose to boycott the games to protest against human rights violations, these gestures were irrelevant to the public who were captivated by the Games drama.

When the ‘little green men’ began taking over the Crimea, there was confusion over the anonymous soldiers who did not have anything to identify their nationality. The Crimean vote to approve its annexation into Russia was condemned in the West and seen as an attack on the principles that guided the post-World War II international order. It was a threat to the principles that led to European unity. The Russian media, in contrast, created a narrative stating that the annexation was necessary to protect Russian-speaking populations from Ukrainian nationalists, which its media called ‘fascists.’ This argument resonated with the Russian people who saw it as a legitimate defensive maneuver rather than an aggressive take-over.⁴¹ The Kremlin was successful in framing the annexation in a way that increased the Russian people’s support and domestically countered the international condemnation.

The Russian approach to annexing Crimea was timed to weaken and minimize Western retaliation.⁴² When irregular forces took control and secured the peninsula, there was no support for a military response.⁴³ Western states, led by the United States and European countries, targeted Russian institutions by initiating sanctions on financial enterprises, the energy sector, and high-ranking officials. The response was symbolic as it was inadequate to reverse the annexation, but it sent a message that the West would punish Moscow financially. The Russian economy was largely unaffected and responded by deepening its trade relationships with non-Western countries, particularly China, which allowed it to avoid the negative costs imposed by sanctions.

The Sochi Olympics and the Crimean annexation show how Putin was able to leverage the Games as an instrument to advance his geopolitical goals.⁴⁴ The Olympics helped Russia to showcase its culture and build a positive international image while simultaneously shielding Russia while it deployed its military to expand its borders.⁴⁵ This was the second time in six years that Putin was able to use the Olympics as a diversion to take territory from a neighboring state and it shows that the IOC is unable to preserve the neutrality and unity promised by the Games. Observers can no longer assume that the Olympic truce will not be used by revisionist countries to cover expansionist objectives. If international institutions do not focus on this problem and devise a plan to prevent this exploitation in the future, the Olympics will continue to be used by strong states that time their military conquests to coincide with the Games.

2022 BEIJING WINTER OLYMPICS AND THE RUSSIAN INVASION OF UKRAINE

Russia launched a full-scale invasion into Ukraine in February 2022, but it had been fighting in the Donbas region for the previous eight years. Russian-backed militias took over towns in the Donetsk and Luhansk in 2014 and declared themselves independent and this action started the Donbas war. Russian armed forces have been active in Ukraine since 2014 and had to use increasingly advanced equipment to maintain its positions.⁴⁶ When 2022 began, Russian soldiers, in the hundreds of thousands, were prepositioned on Ukraine's border preparing for war. Russia's military forces were ready to invade in February 2022, but before the invasion Russian President Vladimir Putin met with Chinese President Xi Jinping in Beijing before the Winter Olympics opening ceremony. The meeting displayed the deepening strategic cooperation between Russian and China as both

states had tense relations with the West. The two leaders issued a joint statement opposing NATO expansion and stating that they “intend to counter interference by outside forces in the internal affairs of sovereign countries under any pretext, oppose color revolutions and will increase cooperation in the aforementioned areas.”⁴⁷ This meeting showed Russian and Chinese strategic collaboration to oppose the U.S. and NATO and to weaken American influence in Europe and Asia. China avoided criticizing Russia's military buildup on Ukraine's border. It was clear to Xi that Putin was planning on initiating his invasion during the Olympics and the Chinese leader asked Russia to avoid conflict until the Games finished.⁴⁸ It was important to China that the war not intervene with Beijing's time in the spotlight and Putin complied with this request.

Putin appears to have altered his military plans to satisfy Xi's wishes and this shows how Russia is able to strategically adapt the *maskirovka* approach. Russia consented to China's diplomatic request and was still able to benefit from the Olympic coverage by timing the invasion to coincide with the Games conclusion. This allowed Moscow to move forward and attack Ukraine and simultaneously deepened its relationship with Beijing. This strengthened the Sino-Chinese partnership in opposing the West and, gained support from China who does not want to see Russia lose to Ukraine. Xi worked to help Russia indirectly and, at the same time, appeared to outsiders as neutral and objective.⁴⁹ Beijing was successful in getting Russia to delay its military invasion so that it could gain as many benefits as possible by hosting the Olympics. Both Russia and China were successful diplomatically and gained from this arrangement.

The 2008 and 2014 Russian invasions caught the world by surprise, but the 2022 invasion was anticipated due to the public military build-up on Ukraine's borders. In March and April 2021, the Russian military placed military equipment and

thousands of soldiers on the Ukrainian border. The soldiers were withdrawn in June but left their equipment in place. Putin commenced a second military buildup in October and by December over a hundred thousand troops were present on three sides, but Putin denied that he had any intention of invading. The massive military presence left no doubt as to the Kremlin's intention regarding Ukraine, but Putin would choose to commence his war when it was most advantageous.⁵⁰ This constitutes a major difference from the other cases because it continued to be a media story even during the Olympic games, even if the overall attention it received decreased.

The Western world was closely following Russia's military build heading into the Olympics and there was widespread awareness that a military invasion was in the works. The Games did not provide the same coverage to Moscow, although the Olympics diverted some media attention, but the anticipation and invasion was so large that it received intense coverage.⁵¹ While the invasion took place four days after the Olympics ended, the scale was so large, the invasion involved most of Russia's military, that it became the leading news story for weeks. The Western media highlighted that the invasion broke international law and constituted a major threat to European stability and NATO; it featured reports showing the human impact and the impact the war had on global security.⁵² The Western response did not provide Russia with the same strategic advantage it had gained in Georgia and Crimea.

The international response was rapid and showed diplomatic and strategic coordination to overcome the vulnerability caused by the intense media focus on the Olympics that Russia had exploited in the past. The response was strengthened by the public military buildup that preceded the conflict; the international community was able to respond quickly because the war was expected. The two previous military campaigns that took

place during or proximate to the Olympics caught the world by surprise, this was not the case in 2022. Western governments moved quickly to impose sanctions on Russia's financial institutions, energy exports, and on high-ranking government officials. This response sought to isolate Moscow diplomatically and to generate world-wide retaliatory measures, stronger than the responses in 2008 and 2014. The world moved to condemn Russia, but few states outside Europe joined in the sanctions.⁵³ The condemning words were strong but in Latin America, Africa, and for most of Asia, this was the extent of their opposition.⁵⁴

The state-controlled Russian media projected a different narrative by stating that the invasion was a defensive maneuver to protect Russian-speaking populations in eastern Ukraine from persecution by the Ukrainian military.⁵⁵ This narrative was presented as one element in Russia's broader national defense strategy which sought to protect Moscow from NATO and the West.⁵⁶ Putin sees Ukraine as vital to Russian national culture and identity and he argued that national security required that Moscow prevent Kiev from joining NATO. The Russian media sought to rally the masses to support the Kremlin by using images to support national unity and pride so it could stand against international sanctions.⁵⁷ The media was an important tool for Russia as it sought to create a national consensus for the war and argue that the conflict was necessary for national defense. It also justified crackdown on dissent and minimized sanctions negative effect on the wider population.

Even before the Beijing Games, Moscow and Minsk were under sanction by the IOC for doping in the 2014 Sochi Olympics, but there was no official punishment for initiating war during the competition. Russian and Belarusian athletes were able to compete but not under their national flag—they had to compete as independent contestants with no national symbols, anthems, or colors allowed at

the Olympics. FIFA took a more active approach and bared Russia from the 2022 World Cup and moved the 2022 Champions League Final from St. Petersburg in response to the war. The IOC followed and banned Russian athletes from competing under their national flag in the 2024 Paris Olympics. The IOC altered its political neutrality and punished Moscow for its invasion and worked with other international institutions to create a broad diplomatic consensus to isolate and punish Russia. Putin called the move a form of national discrimination and sought to overcome the challenge it posed to its soft power strategy and national identity.

China tried to appear neutral and use the conflict to advance its global standing as an outside great power with the detachment and impartiality to manage the diplomatic negotiations that could end the war. Beijing was careful to avoid providing public support for Putin, but it provided economic assistance by increasing its consumption of energy exports that allowed Russia to mitigate Western sanctions.⁵⁸ China approached the war to increase its global prowess and maintained its diplomatic flexibility while maintaining its support for Russia's anti-Western policy. Beijing provided diplomatic cover to the small states in Latin America, Africa, and Asia who wished to maintain their trade with Russia—particularly for agricultural products—and it was successful in limiting the sanctions to Western states and their strongest allies.⁵⁹ China's diplomatic maneuver built strategic arrangements with small states which constitute a threat to Western global leadership.

The 2022 Ukraine War was different from the previous engagements we have considered because Putin telegraphed his intentions before the war and blatantly violated the Olympic truce. While the West was able to impose some sanctions, it was not enough to prevent the war. The conflict shows how global media events are contextually important to the timing of geopolitical wars. Russia has

repeatedly and blatantly violated the Olympic truce to provide cover for its aggressive wars that gave Moscow additional territory. The international response was greater, but not sufficient to prevent the conflict, and if Xi had not asked Russia to delay its military engagement, the war would have started during the Games. The West was able to get the world to condemn Moscow for the war but was not able to get most states to join the sanctions regime. The international response was more rapid because the aggression was more visible and easier to condemn. The IOC (and FIFA) banned Russian athletes and there was widespread diplomatic censure—while it generated a response it was not enough to impose costs sufficient to prevent Russia from doing this again.

STRATEGIC CONSEQUENCES

Russia has repeatedly used the Olympic Games as a cover to prevent the international community from effectively responding to Moscow's aggressiveness, which shows strategic employment of *maskirovka*. All three military engagements saw Russia engage in offensive operations to take territory during or immediately after the Olympics. Putin times his invasions to coincide with media events that shield Russia from immediate diplomatic reprisals—Moscow gains time and faces less severe consequences. The Kremlin was also successful in creating a domestic narrative that defended these operations as defensive maneuvers designed to protect at-risk Russian-speaking populations.⁶⁰ Each case—Georgia in 2008, Crimea in 2014, and Ukraine in 2022—shows that Moscow was able to use the international media focus on the Games to weaken global opposition to its conquests. Every instance violates a norm that has guided international relations since WWII: it is not legitimate to change state borders by force. Putin has violated this norm three times and has suffered some economic and reputational costs, but the international community

was not able to stop him from making territorial gains. The Olympics provided a ‘media shield’ that allowed Russia to undertake rapid military operations that expanded Moscow’s geopolitical control and lessened the international reaction.

This is an example of hybrid warfare, which combines regular and irregular tactics that put together diplomatic, economic, psychological, media, and military operations to accomplish a strategic objective.⁶¹ The Olympic truce benefited Russia and allowed it to mask its intentions—using ambiguous, tactics that make it more difficult for its adversaries to form a clear, coordinated response. The 2008 and 2014 operations were successful as Putin was able to make the territorial gains quickly which did not give the international community time to offer an effective response. Since the objectives were accomplished, the West was only able to offer symbolic punishment.⁶² The 2022 Ukraine War was different because the Russian troop movements were apparent, and the invasion’s massive scale placed the war in the global media spotlight. In the other cases, Russia was able to confuse the West through plausible deniability and by initiating the conflict to coincide with the Olympic Games which distracted international community and allowed Moscow to generate its own narrative.

Russia has repeatedly timed its military campaigns to coincide with the Olympics and this has important implications for Games symbolic significance and global security. Putin has challenged and weakened the Olympics foundational principles as a non-political, unifying event. The International Olympic Committee has recognized this vulnerability and has struggled to come up with a preventive plan that could alter the cost-benefit outcome enough to prevent these wars. While the IOC seeks to maintain neutrality, this does not prevent great powers from taking advantage of the Games for its geopolitical ambitions. The three Russian invasions that have taken place in conjunction with the

Olympics ultimately weaken the IOC’s credibility and the Games now bring with them the risk that a state will use the media event as a shield that allows it to conduct military conquests.

The IOC response to the 2022 Ukraine war was significantly different from its response to Russia’s 2008 Georgia invasion or the 2014 Crimean annexation. The IOC punished Russian and Belarusian athletes by not allowing them to compete under their country’s flag. This is a change from the IOC’s previous neutrality and shows the IOC is working to preserve the Game’s role in promoting unity and peace. When a state repeatedly violates the Olympic truce and uses the Games to provide cover for military invasions, the IOC is no longer passively watching. There is a recognition that the IOC needs to actively work to promote the Game’s integrity. The IOC sanction against Russia’s athletes displaying any national symbols, anthems, or flags provides some consequences for countries that repeatedly use the Olympics as a tool to advance national interests.

The global Olympic media promotion created a vulnerability that Moscow was quick to recognize and exploit as the intense focus on the Games automatically lowered the space available for other news stories. The networks covering the events paid vast sums to secure the right to cover the games and would have needed to take an economic loss if attention were diverted elsewhere.⁶³ In 2008 and 2014, the Western media focused on the Olympics and were not able to provide in-depth coverage of Russia’s invasion of Georgia or Ukraine. The networks inadvertently supported Russia’s strategy by lessening the public’s awareness of the war.⁶⁴ As a result, public pressure to respond was less than normal and the pressure to create diplomatic consensus to punish Moscow declined and allowed Russia to consolidate its gains before the West could act. The 2022 Ukraine War was fundamentally different as Moscow engaged in a massive troop buildup prior to the invasion and, unlike the situation in 2008

or 2014, this war was not a surprise. It is revealing that even when Putin was going to invade Ukraine, he initially chose to have the war coincide with the Olympic games. The global media was focused on Russia's military presence, and, after the earlier wars, it was prepared to respond decisively to cover the war. The punishment was not sufficient to prevent Russia from invading, but the international response showed increased media prowess in responding to geopolitical crisis during global media events.

The three case studies reveal Putin's strategic focus to prioritize the former Soviet territories while working to stop Western expansion into Eastern and Central Europe. Each invasion sought to prevent NATO's eastward expansion and suggests that Russia will not be a passive spectator as the Atlantic Alliance gains new members—the Georgian and Ukrainian invasions were Moscow's response to the 2008 Bucharest declaration where NATO stated that both states would eventually become members of the alliance.⁶⁵ Putin created the domestic support to actively subvert NATO's expansion into former-Soviet states and convinced the public that it was in Russia's security interests to act.⁶⁶ The three cases used the Olympics as a shield to delay an international response and showed how global media events can weaken diplomatic coordination to respond to global events. Putin sees the Olympics as a tool he can use to allow Russia to provide cover for aggressive military interventions and prevent an immediate response. The Games were exploited to provide Russia with additional control over its near-abroad.⁶⁷ Putin successfully employed *maskirovka* to achieve a strategic advantage in multiple instances that the West was powerless to stop.

The international community has not developed an effective response to this threat. The cases suggest that the Olympic games are likely to be used to provide cover for international aggression and this will weaken their ability to foster unity

and peace. This undermines the IOC's mission and raises questions about global sporting bodies responsibilities. Managing boards need to more broadly consider how their events may be used by countries who can engage in a quick war. As the IOC is forced to intervene against states who abuse the Games it will be forced to take sides and will no longer appear objective and neutral. One additional approach is for the IOC to consider new rules to uphold the Game's integrity and implement stricter criteria for the host state to be based on political stability and human rights.⁶⁸ The difficult reality is that no matter what policies or rules the IOC chooses to impose, the changes are not likely to be punitive enough to stop states intent on using the Games to provide some strategic cover for aggressive behavior.

CONCLUSION

Russia has three times engaged in aggressive military behavior coinciding with the Olympics that resulted in territorial changes, and this illustrates the vulnerabilities present within international media events. Revisionist states can use global media events, such as the Olympics, to deflect attention and consolidate their gains prior to incurring an international response, which is likely to be sanctions. The international community was more effective in organizing a response in 2022, but this invasion was different and easy to anticipate. Serious questions remain about the international community's ability to respond to a surprise attack that occurs during the Olympics. The IOC is working to develop punitive sanctions as a means to preserve the Games neutrality.

Moscow strategically employed *maskirovka*—the multilayered approach that combines deception, misinformation, and misdirection—and this was an effective doctrine in 2008 and 2014. It is a fundamental element in Russia's hybrid warfare strategy.⁶⁹ In initiating conflict during the Olympics when the media is saturated with Game coverage,

Russia has successfully undermined global media's watchdog function. It attacks when the world's focus is directed elsewhere. This is hybrid warfare where military actions are nested within a broader economic, social, media, and diplomatic tactics to achieve objectives while minimizing opposition.⁷⁰

Staging aggression during the Olympic games allows Russia to use *maskirovka* to create a 'gray zone' where the traditional understanding of warfare is deliberately blurred. The international community needs a widely accepted, cohesive understanding of the conflict before diplomats can come to an agreement and punish the aggressor. Putin's approach deliberately creates confusion and the first problem the global community has is to properly understand the aggression. This delays the international community's response and prevents the world from reacting with a unified, immediate response.⁷¹ Moscow times its wars to minimize the costs its aggression will generate, and the Olympics provide a temporal opportunity for *maskirovka* and hybrid warfare. This allows Putin to project an image of strength while pursuing territorial change in its near-abroad.

The Russian *maskirovka* approach where Moscow initiates its most important conflicts during the Olympics shows how effective hybrid warfare is in the contemporary international climate.⁷² Putin was able to repeatedly exploit a vulnerability before the West was able to formulate a response. This approach allows Putin to exploit the Olympics—long considered a symbol for international peace and cooperation—as a tool to help it make territorial gains. The intentional uniting the Olympics with military conquest undermines a global norm and prevents the international community from responding decisively and quickly. Russia gains time to consolidate its military gains. The Western response has been inadequate to change the cost-benefit analysis that allows Moscow to continue to misuse the Olympics as a geopolitical tool.

The global community is vulnerable to similar attacks in the future.⁷³ Other revisionist states are likely to follow Russia's example and use global media events to cover their aggressive actions. The global security implications are serious and significant.⁷⁴ States following this example can use similar events as cover that allows them to violate their neighbor's sovereignty without crossing the conventional understanding of warfare. This creates pressure on the West to come up find a way to clearly understand hybrid tactics and come up with a response. The traditional diplomatic and military responses are not adequate to deter states wishing to use hybrid tactics in the future).⁷⁵ The global community does not have the means to prevent these attacks.

The international community needs to have a stronger response to hybrid tactics, like *maskirovka*, to counter this danger. Coordinated intelligence-sharing, real time media reporting, and proactive diplomatic engagement can mitigate this vulnerability, which will allow state-led misinformation and deception operations to be countered quickly and accurately.⁷⁶ It is also important to educate the public on the danger hybrid warfare brings so that people can recognize when they are being manipulated. This will not take away the vulnerability, but it can increase the costs to states that wish to violate global events, like the Olympics, and preserve their integrity and purpose.

Russia strategically times its offensive military operations using *maskirovka* to delay and weaken the international community's response to its war. The Olympic Games provide cover, and this is an effective adaptation of hybrid tactics. International conflict has evolved in the 21st century and revisionist powers can exploit international norms and symbols to prevent the international community from a rapid response. States wishing to preserve the Olympics as a unifying, politically-neutral event need to proactively anticipate the threat and develop

a coordinated international response. It will be difficult to overcome and neutralize the vulnerability targeted in *maskirovka* and hybrid warfare, but it is essential to preserve global security. **PRISM**

Notes

- ¹ Burleson, Cindy and Ramón Spaaij. *The Olympic Movement and the Sport of Peacemaking*. Routledge, 2013.
- ² Furgacz, Przemyslaw. "Russian Information War in Ukrainian Conflict." In *Countering Hybrid Threats: Lessons Learned from Ukraine*. Edited by N. Ian; A. Fortuna, C. Barna, M. Teodar. STM Publishing House: Amsterdam, Berlin, Washington, 2016.
- ³ Jonsson, O., & Seely, R. (2015). Russian full-spectrum conflict: An appraisal after Ukraine. *Journal of Slavic Military Studies*, 28, no. 1 (2015): 1-22.
- ⁴ Wong, Edward and Julian E. Barnes. "China Asked Russia to Delay Ukraine War Until After Olympics, U.S. Officials Say." *New York Times*. March 3, 2022, Section A, Page 9. Also available: <https://www.nytimes.com/2022/03/02/us/politics/russia-ukraine-china.html>.
- ⁵ Roberts, James Q. *Maskirovka 2.0: Hybrid threat, hybrid response*. Occasional Paper. December 2015. JSOU Press.
- ⁶ Pynnöniemi, Katri Pauliina, and András Rác. *Fog of Falsehood: Russian Strategy of Deception and the Conflict in Ukraine*. 320 pages. Helsinki: FIIA Report from The Finish Institute of International Affairs, 2016.
- ⁷ Holloway, Michael. How Russia weaponized social media in Crimea. *The Strategy Bridge*. May 10, 2017. <https://thestrategybridge.org/the-bridge/2017/5/10/how-russia-weaponized-social-media-in-crimea>.
- ⁸ Mumford, Andrew and Pascal Carrucci "Hybrid Warfare: The Continuation of Ambiguity by Other Means." *European Journal of International Security*. 8 (2023): 192-206.
- ⁹ Rațiu, Aurelian, and Alexandra Munteanu. "Hybrid Warfare and the Russian Federation Informational Strategy to Influence Civilian Population in Ukraine." *Revista Academiei Forțelor Terestre*, 3, no. 91 (2018):192-200.
- ¹⁰ Wong, Edward and Julian E. Barnes. "China Asked Russia to Delay Ukraine War Until After Olympics, U.S. Officials Say." *New York Times*. March 3, 2022, Section A, Page 9. Also available: <https://www.nytimes.com/2022/03/02/us/politics/russia-ukraine-china.html>.
- ¹¹ Jonsson, O., & Seely, R. Russian full-spectrum conflict: An appraisal after Ukraine. *Journal of Slavic Military Studies*, 28, no. 1 (2015): 1-22.
- ¹² Muradov, I. The Russian hybrid warfare: the cases of Ukraine and Georgia. *Defence Studies*, 22, No. 2 (2022), 168–191.
- ¹³ Tsygankov, A. P. *The dark double: US media, Russia, and the politics of values*. Oxford University Press, 2019.
- ¹⁴ Lexmann, Miriam. "The European Union and Russia: Mirror Like Asymmetry in Hybrid Conflict." *International Issues & Slovak Foreign Policy Analysis*. XXVI, no. 3-4 (2017): 35-55.
- ¹⁵ Holloway, Michael. How Russia weaponized social media in Crimea. *The Strategy Bridge*. May 10, 2017. <https://thestrategybridge.org/the-bridge/2017/5/10/how-russia-weaponized-social-media-in-crimea>.
- ¹⁶ Burleson, Cindy and Ramón Spaaij. *The Olympic Movement and the Sport of Peacemaking*. Routledge, 2013.
- ¹⁷ Jones, Stephen. *Georgia: A Political History Since Independence*. I.B. Tauris, 2013.
- ¹⁸ Galeotti, M. *Russia's Five-Day War: The Invasion of Georgia*, August 2008. Osprey Publishing, 2023.
- ¹⁹ Dempsey, Judy. "Russia steps up effort to keep Georgia out of NATO." *New York Times*. May 1, 2008 <https://www.nytimes.com/2008/05/01/world/europe/01iht-georgia.4.12494457.html>.
- ²⁰ Rotaru, Vasile. "When Words Are Sharper than Swords: Russia's Post-2014 Narrative on NATO." In *Russia's Emerging Global Ambitions*. eds. Marcin Kaczmarek, Wojciech Michnik, Andrew Monaghan, and Vasile Rotaru; NDC Research Paper No. 11—July 2020. Rome, Italy: NATO Defense College: 29-41.
- ²¹ Sakwa, Richard. 2015. "The Death of Europe? Continental Fates after Ukraine." *International Affairs* 91, no. 3 (2015): 553-579.
- ²² Dickinson, Peter. "The 2008 Russo-Georgian War: Putin's green light." *Atlantic Council*. March 15, 2023, <https://www.atlanticcouncil.org/blogs/ukrainealert/the-2008-russo-georgian-war-putins-green-light>.
- ²³ Sutil Toledano, J. *The Use of Hybrid Warfare to Achieve Strategic Objectives: Comparing Russian and Chinese Approaches*. 2023 Master's Thesis. University of Glasgow.
- ²⁴ Akhvediani, Margarita "The fatal flaw: the Media and the Russian invasion of Georgia." Chapter 6; Pg 114-140 in *Crisis in the Caucasus: Russia, Georgia and the West* edited by Paul Rich. Routledge, 2013.
- ²⁵ Hersh, Philip. "NBC Makes \$2.3 Billion Bet on Olympic TV Rights." *Chicago Tribune*. Published December 13, 1996, Accessed December 5, 2024. <https://www.chicagotribune.com/1995/12/13/nbc-makes-23-billion-bet-on-olympic-tv-rights/>.

²⁶ International Olympic Committee (IOC). Official Report of the XXIX Olympiad, Volume III: The Games of the XXIX Olympiad, Beijing 2008. Accessed December 5, 2024. <https://stillmed.olympic.org/Documents/Reports/Official%20Past%20Games%20Reports/Summer/ENG/2008-RO-S-Beijing-vol3.pdf>; Nielsen. "Beijing Olympics Draw Largest-Ever Global TV Audience." 2008. Accessed December 5, 2024. <https://www.nielsen.com/insights/2008/beijing-olympics-draw-largest-ever-global-tv-audience/>.

²⁷ Dickinson, Peter. "The 2008 Russo-Georgian War: Putin's green light" *Atlantic Council*. March 15, 2023. <https://www.atlanticcouncil.org/blogs/ukrainealert/the-2008-russo-georgian-war-putins-green-light>.

²⁸ Holloway, Michael. How Russia weaponized social media in Crimea. *The Strategy Bridge*. May 10, 2017. <https://thestrategybridge.org/the-bridge/2017/5/10/how-russia-weaponized-social-media-in-crimea>.

²⁹ Oğuz, Şafak. "The New NATO: Prepared for Russian Hybrid Warfare?" *Insight Turkey*. 18, no. 4 (2016): 165-180.

³⁰ Cornell, S. E., Starr, S. F. *The Guns of August 2008: Russia's War in Georgia*. London: Routledge, 2015.

³¹ Śliwa, Zdzisław, Viljar Veebel, Maxime Lebrun. "Russian Ambitions and Hybrid Modes of Warfare." *Sõjateadlane (Estonian Journal of Military Studies)* 7 (2018): 86-108.

³² Davis, G. D., & Slobodchikoff, M. O. *Cultural imperialism and the decline of the liberal order: Russian and Western soft power in Eastern Europe*. Rowman & Littlefield, 2018.; Davis, G. D., & Slobodchikoff, M. O. Great-Power Competition and the Russian Invasion of Ukraine. *Journal of Indo-Pacific Affairs*, 5, no 4 (2022): 215-226.; Davis, G. D., & Slobodchikoff, M. O. "Great Power Competition Following the Ukraine War," In *The Great Power Competition Volume 5: The Russian Invasion of Ukraine and Implications for the Central Region* (pp. 35-45). Cham: Springer Nature Switzerland, 2023.

³³ Wallace, R. "On Maskirovka: the dynamics of delay in threat recognition." *The Journal of Defense Modeling and Simulation*, 20, no. 2 (2023): 171-180.

³⁴ Renz, Bettina. "Russia and 'Hybrid Warfare'" *Contemporary Politics*. 22, no. 3 (2016): 283-300.

³⁵ Erol, Mehmet Seyfettin and Şafak Oğuz "Hybrid Warfare Studies and Russia's Example in Crimea." *Akademik Bakis* 9, no. 17 (2015): 261-277.

³⁶ Osflaten, A. "Russian strategic culture after the Cold War: The primacy of conventional force." *Journal of Military and Strategic Studies*, 20, no. 2 (2021): 110-132.

³⁷ Alexandru, R., & Totir, V. C. "Russian military diversion—maskirovka, used in the Black Sea area." *Strategies XXI-Command and Staff College*, 17, no. 1 (2021): 147-152.

³⁸ Rose, A. K., & Spiegel, M. M. "The Olympic effect." *The Economic Journal*, 121, no. 553 (2011): 652-677; Randeree, K. (2013). "Reputation and mega-project management: Lessons from host cities of the Olympic Games." *Change Management*, 13, no. 2 (2013): 1-7.

³⁹ Bernstein, Jacob. "Anti-Gay Policies Chill Viewers' Interest." *New York Times*. February 2, 2014. Section ST, Page 9.

⁴⁰ Olympics.com. "Success of Sochi 2014 Lives On." Published February 6, 2015. Accessed December 5, 2024. <https://olympics.com/en/news/success-of-sochi-2014-lives-on>; IOC Global Broadcast and Audience Report Sochi 2014. Accessed December 5, 2024. <https://stillmed.olympics.com/media/Document%20Library/OlympicOrg/Games/Winter-Games/Games-Sochi-2014-Winter-Olympic-Games/IOC-Marketing-and-Broadcasting-Various-files/Global-Broadcast-and-Audience-Report-Sochi-2014.pdf>.

⁴¹ Holloway, Michael. "How Russia weaponized social media in Crimea." *The Strategy Bridge*. May 10, 2017. <https://thestrategybridge.org/the-bridge/2017/5/10/how-russia-weaponized-social-media-in-crimea>; Takacs, David. "Ukraine's Deterrence Failure: Lessons for the Baltic States." *Journal on Baltic Security*. 3, no. 1 (2017): 1-1.

⁴² Asmus, R. D. *A Little War That Shook the World: Georgia, Russia, and the Future of the West*. Palgrave Macmillan, 2010.; Monaghan, Andrew. "The War in Russia's 'Hybrid Warfare'" *Parameters* 45, no. 4 (2015-2016):65-74.

⁴³ Slobodchikoff, M. O. 2014. *Building hegemonic order Russia's way: order, stability, and predictability in the post-Soviet space*. Lexington Books, 2014.; Slobodchikoff, M. O. Challenging US hegemony: The Ukrainian crisis and Russian regional order. *The Soviet and Post-Soviet Review*, 44, no. 1 (2017), 76-95.; Slobodchikoff, M. O. (Ed.), *Breaking Point: Russia, Ukraine, and the Future of International Relations*. Rowman & Littlefield, 2025.; Slobodchikoff, Michael O. *Building Hegemonic Order Russia's Way: Chasing International but Not Regional Multiplicity*. Bloomsbury Publishing USA, 2025.

⁴⁴ Bercean, Ioana-Nelia. "Ukraine: Russia's New Art of War." *The Online Journal Modeling the New Europe* 21/2016: 155-174.; Davis, G. D., & Slobodchikoff, M. O. *Cultural imperialism and the decline of the liberal order: Russian and Western Soft Power in Eastern Europe*. 2018. Rowman & Littlefield.; Davis, G. D., & Slobodchikoff, M. O. Great-Power Competition and the Russian Invasion of Ukraine. *Journal of Indo-Pacific Affairs*, 5, no. 4, (2022): 215-226.

⁴⁵ Bachmann, Sascha Dov and Håkan Gunneriusson. "Russia's Hybrid Warfare in the east; The Integral Nature of the Information Sphere." *Georgetown Journal of International Affairs* 16 (2015): 198-211.

⁴⁶ Kimmage, Michael and Michael Kofman. "Russia Won't Let Ukraine Go without a Fight." *Foreign Affairs*. November 22, 2021, Online.; Savage, Patrick J. "Traditional War; The Conventionality of Russia' Unconventional Warfare." *Parameters* 48, no. 2 (2018): 77-85

⁴⁷ Myers, Steven Lee and Anton Troianovski. "Russia and China join in opposing any expansion of NATO." *New York Times*. Feb. 3, 2022. <https://www.nytimes.com/live/2022/02/03/world/russia-ukraine-xi-putin/ukraine-briefing-xi-putin>.

⁴⁸ Wong, Edward and Julian E. Barnes. "China Asked Russia to Delay Ukraine War Until After Olympics, U.S. Officials Say." *New York Times*. March 3, 2022, Section A, Page 9. Also available: <https://www.nytimes.com/2022/03/02/us/politics/russia-ukraine-china.html>.

⁴⁹ Boot, M. China's diplomatic balancing act over Russia's invasion of Ukraine. *Council on Foreign Relations*. May 17, 2023. <https://www.cfr.org>.

⁵⁰ Cheskin, Ammon. "Russian soft power in Ukraine: A structural perspective." *Communist and Post-Communist Studies*. 50 (2017): 277-287.; Bachmann, Sascha-Dominik Dov, Dries Putter, and Guy Duczynski. "Hybrid warfare and disinformation: A Ukraine war perspective." *Global Polic* 14, no. 5 (2023): 858-869.

⁵¹ IOC Marketing Report Beijing 2022. Accessed December 5, 2024. <https://stillmed.olympics.com/media/Documents/Olympic-Movement/Partners/IOC-Marketing-Report-Beijing-2022.pdf>; NBC Sports. "NBC Universal's 2022 Beijing Olympics: The Most Extensive Winter Games Presentation Ever Dominates Media Landscape." (2022) Accessed December 5, 2024. <https://www.nbcsports.com/pressbox/olympics/press-releases/nbcuniversals-2022-beijing-olympics-the-most-extensive-winter-games-presentation-ever-dominates-media-landscape>.

⁵² Adgate, B. TV ratings for Beijing Winter Olympics were an all-time low, for streaming it was an all-time high. *Forbes*. February 23, 2022. <https://www.forbes.com/sites/bradadgate/2022/02/23/tv-ratings-for-beijing-winter-olympics-was-an-all-time-low-for-streaming-it-was-an-all-time-high/>;

Pavlik, J. V. "The Russian war in Ukraine and the implications for the news media." *Athens Journal of Mass Media and Communications*, 8 (2022): 1-17.

⁵³ Slobodchikoff, M. O. *Building hegemonic order Russia's way: order, stability, and predictability in the post-Soviet space*. Lexington Books, 2014.; Slobodchikoff, Michael, and Aakriti A. Tandon. *India as kingmaker: status quo or revisionist power*. University of Michigan Press, 2022.

⁵⁴ Davis, G. D. and Khemaies Jhinaoui. "Africa and Russia after the Ukraine War." In Michael O. Slobodchikoff (editor), *Breaking Point: Russia, Ukraine, and the Future of International Relations*, page 167-186. Rowman & Littlefield, 2025.

⁵⁵ Jakubczak, R. Use of genocide by the Russian Federation in the conduct of hybrid activities and warfare in Ukraine. *Studia Prawnicze KUL*, 4 (2023), 81-99.

⁵⁶ Mehdiyeva, Nazrin. *The Problems of the Applied Theory of War: A Review of A. A. Kokoshin's the Problems of the Applied Theory of War*. NATO Defense College (Rome: NATO Defense College, 2022). <https://www.ndc.nato.int/research/research.php>.

⁵⁷ Holloway, Michael. "How Russia weaponized social media in Crimea." *The Strategy Bridge*. May 10, 2017. <https://thestategybridge.org/the-bridge/2017/5/10/how-russia-weaponized-social-media-in-crimea>.

⁵⁸ Krauss, Clifford; Alexandra Stevenson and Emily Schmall. "In Russia's War, China and India Emerge as Financiers." *New York Times*. Published June 25, 2022, Section B, Page 1. <https://www.nytimes.com/2022/06/24/business/russia-oil-china-india-ukraine-war.html>.

⁵⁹ Davis, G. D. and Khemaies Jhinaoui. "Africa and Russia after the Ukraine War." In Michael O. Slobodchikoff (editor), *Breaking Point: Russia, Ukraine, and the Future of International Relations*, page 167-186. Rowman & Littlefield, 2025.

⁶⁰ Kimmage, Michael and Michael Kofman. "Russia Won't Let Ukraine Go without a Fight." *Foreign Affairs*. November 22, 2021, Online.

- ⁶¹ Bērziņš, Jānis. “Russian New Generation Warfare Is Not Hybrid Warfare.” In *War in Ukraine: Lessons for Europe*, edited by Artis Pabriks and Andis Kudors, 40-51. Riga: The Centre for East European Policy Studies & University of Latvia Press, (2015).; Pocheptsov, G., “Cognitive attacks in Russian hybrid warfare.” *Information & Security*, 41 (2018), pp.37-43.; Singer, P. W., and Emerson T. Brooking. “What Clausewitz Can Teach Us About War on Social Media.” *Foreign Affairs*. October 19, 2018. Accessed October 19, 2018. <https://www.foreignaffairs.com/articles/2018-10-04/what-clausewitz-can-teach-us-about-war-social-media>; Slobodchikoff, Michael O. *Building Hegemonic Order Russia's Way: Chasing International but Not Regional Multipolarity*. Bloomsbury Publishing USA, 2025.
- ⁶² Thornton, R. “The changing nature of modern warfare: Responding to Russian information warfare.” *RUSI Journal*, 160, no. 4 (2015), 40-48.
- ⁶³ Hersh, Philip. “NBC Makes \$2.3 Billion Bet on Olympic TV Rights.” *Chicago Tribune*. Published December 13, 1996, Accessed December 5, 2024. <https://www.chicagotribune.com/1995/12/13/nbc-makes-23-billion-bet-on-olympic-tv-rights/>.
- ⁶⁴ Ajir, Media and Bethany Vaillant. “Russian Information Warfare: Implication for Deterrence Theory.” *Strategic Studies Quarterly*. Fall 2018: 70-89.
- ⁶⁵ Baev, Pavel K. “The Military Dimension of Russia’s Connection with Europe.” *European Security*. 27, no. 1 (2018): 82-97.
- ⁶⁶ Cohen, A., Hamilton, R. E. *The Russian Military and the Georgia War: Lessons and Implications*. (Strategic Studies Institute, U.S. Army War College, 2011).
- ⁶⁷ Toal, Gerard. *Near Abroad: Putin, the West and the Contest Over Ukraine and the Caucasus*. London, United Kingdom: Oxford University Press, 2016.
- ⁶⁸ Boykoff, Jules. *Power Games: A Political History of the Olympics*. London, United Kingdom: Verso Books, 2016.
- ⁶⁹ Darczewska, Jolanta and Piotr Zöchowski. 2017 “Russia’s ‘Activity’ toward the West—Confrontation by Choice.” *Russian Analytical Digest*. No 212 (2017): 2-6.
- ⁷⁰ Bartles, Charles K. “Getting Gerasimov Right.” *Military Review*. Jan. Feb 2016 Issue (2016): 30-38; Ermus, Aarne, and Karl Salum. “The Changing Concepts of War: Russia’s New Military Doctrine and the Concept of Hybrid Warfare.” In *Russian Information Campaign against the Ukrainian State and Defence Forces*, ed. V. Sazanov, K. Müür and H. Mölder. Tartu (Estonia) NATO Strategic Communications Center of Excellence, 2016; and Gerasimov, Valery. “The value of science is in the foresight: New challenges demand rethinking the forms and methods of carrying out combat operations.” *Military Review* 96, no. 1 (2016): 23.
- ⁷¹ Lunak, Petr. “Security for Eastern Europe: The European Option.” *World Policy Journal*, 11, no. 3 (1994): 128-131.
- ⁷² McDermott, Roger N. “Does Russia Have a Gerasimov Doctrine?” *Parameters*. 46, no. 1 (2016): 97-105.
- ⁷³ Colby, Elbridge. “Step Up to Stand Down.” *Foreign Affairs*, 13 August 2015, <https://www.foreignaffairs.com/articles/poland/2015-08-13/step-stand-down>. Accessed 21 November 2024.
- ⁷⁴ Gardner, Hal. “The Russian Annexation of Crimea: Regional and Global Implications.” *European Politics and Society*. 17, no. 40 (2016): 490-505.
- ⁷⁵ Lanoszka, Alexander. “Russian hybrid warfare and extended deterrence in eastern Europe.” *International affairs* 92, no.1 (2016): 175-195.
- ⁷⁶ Sokolosky, Capt. Johnny (US Army). “The Future of War: How Globalization Is Changing the Security Paradigm.” *Military Review*. 96, no. 1(2016): 8-16.

Soft Power by Design

China's United Front Strategy for Taiwan's Civil Society in the Age of Irregular Warfare

By Yenting Lin

A NEW FORM OF CONFLICT: HOW CHINA IS RESHAPING ITS STRATEGY ON TAIWAN

China's campaign against Taiwan may already be underway, but not in the form most observers expect. Rather than relying primarily on military force, the Chinese Communist Party (CCP) is conducting a long-term effort to shape how Taiwanese society understands China, Taiwan, and reunification.¹ This strategy works through media, education, social networks, and routine social interaction, targeting political identity at the societal level rather than through direct coercion. Civil society has become a central arena for this effort, even though much of the activity remains quiet and outside sustained public scrutiny.

This strategy has been stated clearly in official policy. In January 2019, the Taiwan Work Office of the CCP Central Committee outlined Beijing's Taiwan policy during the fortieth anniversary of the Message to Compatriots in Taiwan. The statement promoted "peaceful reunification" while explicitly refusing to renounce the use of force and reserving "all necessary measures."² It defined the 1992 Consensus as acceptance of the One China principle and tied it directly to the One Country, Two Systems framework. Beijing's position made clear that its concept of peace requires Taiwan to accept China's political terms rather than negotiate them.

To carry out this policy, the CCP relies heavily on the United Front Work system.³ The United Front Work Department reports directly to the CPC Central Committee and operates across education, business, media, religion, youth organizations, and online platforms. Its purpose is to influence and divide target societies by working through non-government actors rather than overt state channels.⁴ Taiwan-related influence

Yenting Lin is a Master's student in Public Policy at George Mason University and a research associate affiliate at the PiVoT Peace Lab (Polarization and Violence Transformed) at the Carter School for Peace and Conflict Resolution. He also serves in the Taiwan Army Reserve. His research focuses on Taiwan China relations, East Asia security, hybrid and gray zone tactics, digital repression, and disinformation, examining how authoritarian states leverage emerging technologies and information operations to influence public opinion and national security.

work is treated as a priority task and is coordinated with the Taiwan Affairs Office and other Party and state institutions.

Since 2022, this influence apparatus has been placed under tighter central control. Oversight of United Front operations has been consolidated under Wang Huning, a member of the Politburo Standing Committee and a senior ideological adviser to the CCP leadership.⁵ This arrangement indicates that societal and cognitive influence toward Taiwan is regarded as a core national mission rather than a supporting activity.

Taiwan therefore faces a coordinated state campaign operating simultaneously across political, social, legal, and information domains. These efforts are designed to weaken resistance, normalize Beijing's narratives, and lower the costs of future coercion. Any assessment of Taiwan's security environment must account for this system-wide approach, not only military balance or crisis scenarios.⁶

INFLUENCER DIPLOMACY: HOW CHINA USES SOCIAL MEDIA TO TARGET TAIWAN'S YOUTH

China treats Taiwanese social media influencers as political assets rather than entertainers. Under the CCP's United Front system, online platforms are used to shape attitudes and normalize Beijing's narratives, consistent with the People's Liberation Army's (PLA) "Three Warfares" framework, which treats public opinion and cognition as strategic domains rather than military targets.⁷

This activity is organized, not informal. United Front Work Department and Taiwan Affairs Office networks are directed by Party regulations to expand political work into online spaces and youth culture. Programs such as the Training Thousands of Taiwan Youth Anchors initiative operationalize this guidance by identifying Taiwanese creators, bringing them into controlled settings in China, and

supporting content that presents China positively without overt political messaging.⁸ Influence is achieved through familiarity and repetition rather than direct persuasion, reducing the likelihood of resistance.

On the operational level, participation is enabled through hosting and access rather than formal agreements. Taiwan government investigations have documented cases in which Taiwanese influencers were invited to China, provided travel accommodation, and production assistance, and encouraged to promote themes of cross-Strait closeness or criticize Taiwan's government without disclosing sponsorship. In several cases, creators altered or deleted earlier content after participating. Public praise from the PRC Taiwan Affairs Office further elevates selected influencers as approved voices while remaining below clear legal thresholds for enforcement.⁹

For younger audiences, short-form video platforms have become primary sources of social interaction and political awareness, while media literacy training remains uneven and limited outside formal education. This creates high exposure to narrative influence with relatively low resistance, especially when messages are delivered by familiar local figures rather than official PRC outlets.

The effects of this strategy were visible during the 2024 presidential election period.¹⁰ Coordinated short-form content questioning electoral integrity and promoting pro-Beijing narratives circulated widely in the final weeks of the campaign. Individual videos were not decisive on their own, but their cumulative presence shaped attention, trust, and perceived legitimacy in ways consistent with influence operations rather than normal political debate.

For Beijing, influencer engagement offers a practical advantage. It allows political influence to be exercised at low cost, with low visibility, and without military escalation by operating inside civilian information spaces and outside conventional

national security frameworks. This logic explains why influencer diplomacy has become a persistent feature of China's Taiwan strategy rather than a temporary tactic.¹¹

EDUCATIONAL EXCHANGE: HOW CHINA TARGETS YOUNG TAIWANESE BY SOCIALIZATION INFRASTRUCTURE

Even student exchange programs have become tools of CCP political influence. Rather than debating politics directly, these programs shape how young Taiwanese experience China, authority, and social order through daily life, social relationships, and managed environments during early adulthood, when political identity is still forming. This method focuses on shaping interpretation and habit rather than persuading through argument, consistent with the PLA's emphasis on influence in the cognitive domain.¹²

The scale of this exposure is large enough to have strategic effects. Over the past decade, more than 60,000 Taiwanese have participated in short-term or degree-based programs in China, with thousands enrolled in institutions later identified by Taipei as politically affiliated.¹³ This is not symbolic engagement or cultural outreach. It is sustained, population-level contact targeting future voters, professionals, and social intermediaries at formative stages of life.

Taiwan's Ministry of Education has formally identified several mainland universities, including Jinan University, Huaqiao University, and Beijing Chinese Language and Culture College, as operating under political control rather than normal academic governance.¹⁴ Enrollment at these schools places Taiwanese students inside managed campus environments where political messaging is embedded into coursework, student activities, and daily social life rather than presented as explicit propaganda.

During these exchanges, political influence is delivered through routine rather than instruction. Content is normalized through guided visits, structured social activities, and peer interaction under institutional rules that explicitly direct United Front organs to expand political work into education and youth exchange. Students encounter consistent cues about cross-Strait relations through what is praised, restricted, or framed as normal, rather than through overt political teaching.

The influence does not stop when participants return to Taiwan. Authorities have documented that former exchange students often become informal transmitters inside their peer networks, sharing favorable narratives about China through trusted personal relationships.¹⁵ This turns lived experience into an influence channel, allowing political messaging to circulate without appearing coordinated or state driven.

Taiwan's response shows that these exchanges are now understood as a security issue rather than a cultural one. In 2025, Taipei revoked recognition of degrees from United Front-affiliated universities, explicitly concluding that these institutions serve political objectives rather than educational ones.¹⁶ This policy shift reflects a broader reassessment: educational exchange is no longer treated as neutral contact, but as part of competition in the cognitive domain that requires active countermeasures.¹⁷

GRASSROOTS DELEGATIONS: HOW FREE TRIPS AND GIFTS BECOME A TOOL CHINA USES FOR RECRUITING LOCAL LEADERS IN TAIWAN

China works through Taiwan's most trusted local figures to influence older communities. Village and neighborhood representatives and temple leaders are targeted because they control access to seniors' daily social life and command high levels of social authority.¹⁸ These actors organize events, resolve

disputes, and mobilize turnout, making them effective intermediaries for political messaging in local communities.

The main tool is organized delegation travel to mainland China. Local leaders are invited on free or heavily subsidized trips framed as cultural exchange, tourism, or local governance visits, with itineraries carefully managed by Taiwan Affairs Office officials. Delegates are taken to Fujian-based cultural sites and exposed to narratives emphasizing shared ancestry, economic opportunity, and political stability under Beijing's system. Political messaging is delivered indirectly through hospitality, ceremonies, and emotional framing rather than explicit advocacy.

These trips have had tangible political consequences. In 2023, prosecutors in New Taipei City charged multiple village representatives under Taiwan's Anti-Infiltration Act after their mainland-sponsored exchange trips included coordinated messaging on unification and cross-Strait cooperation.¹⁹ Investigators found that after returning, participants often repeated these narratives in community meetings and local events, presenting them as personal observations rather than political claims.

Religious networks are also mobilized through similar exchanges. Mazu temples, which attract older worshippers, provide effective platforms for influence activity. Temple leaders are invited to pilgrimage events in mainland China that blend religious ceremony with political symbolism and messages about cross-Strait spiritual unity.²⁰ After returning, temple representatives often host local events that reinforce these themes without using overt political language.

Taiwan's security agencies have warned that these trips and exchanges are sometimes used to influence elections and collect local political information. Local leaders often return from these delegations with guidance and insights that allow political narratives to circulate quietly in communities, leveraging trust and routine social interaction.

LONG-TERM DOMESTICIZED INFLUENCE: CHINESE IMMIGRANT WIVES

Chinese immigrant wives represent one of Beijing's most durable influence channels because they enter Taiwan through family law rather than media or political institutions. By 2024, Taiwan had approximately 366,000 mainland spouses, more than 90 percent of whom were women.²¹ Cross-Strait marriages increased by 185 percent between 2023 and 2024, making this a large and growing population embedded in Taiwanese society.²² Unlike short-term visitors or online influencers, these individuals are permanent residents integrated into households, neighborhoods, and local communities.

Long-term residence and legal integration are the core mechanisms that make this channel politically relevant. After several years of residency, mainland spouses can obtain full household registration and voting rights under Taiwan's naturalization rules.²³ By the late 2010s, more than 200,000 mainland spouses had already become Taiwanese citizens.²⁴ This gives them direct participation in elections and creates an electorally meaningful group in local districts where margins are often small.²⁵

Political influence in this context does not operate through public campaigning. It occurs inside families. Many mainland spouses live with elderly parents or extended relatives, where information flows through daily conversation, caregiving, and private messaging groups. These family spaces are the most trusted sources of information for older Taiwanese and are largely outside the reach of media regulation or fact-checking systems.²⁶

Narratives introduced in these settings are usually subtle rather than ideological. Taiwan may be described as unstable, its government as unfriendly to cross-Strait families, and China as orderly or economically inevitable. Because these views are shared

through family experience rather than political argument, they are difficult to challenge without creating personal or social conflict.

Legal status also creates long-term economic ties. Naturalized spouses can inherit property, participate in household asset decisions, and pass wealth to children who are Taiwanese citizens under existing family and inheritance law. These arrangements link family stability and material security to cross-Strait continuity, reinforcing preferences that favor predictability over confrontation.

Recent enforcement cases highlight why this channel has drawn official attention. In 2025, Taiwanese authorities deported several mainland spouses after investigations found public promotion PLA messaging and unification narratives.²⁷ These cases were notable not because of their scale, but because they confirmed that marriage-based integration can provide a protected space for political messaging inside private family life.

RECOMMENDATION: TAIWAN MUST STRENGTHEN WHOLE-OF-SOCIETY DEFENSE AGAINST NEW FORMS OF IRREGULAR WARFARE

China's influence operations in Taiwan rely more on everyday social connections than on overt propaganda. Effective defense therefore requires coordinated action across government agencies, civil society, local institutions, and international partners. To respond, Taiwan needs a strategy built around five key pillars.

First, Taiwan's media literacy efforts must go beyond schools to reach older adults and those embedded in informal information networks. While the Ministry of Education has incorporated digital and media literacy into K-12 curricula, research shows that older users remain disproportionately exposed to disinformation.^{28,29} Community centers, temples, libraries, and local media outlets can deliver practical training aligned with real-world

information habits, and institutionalized funding would ensure continuity and scale.

Second, Taiwan should support civic technology and fact-checking organizations through stable, multi-year funding. Platforms such as Cofacts and the Taiwan FactCheck Center play a critical role in identifying false narratives and issuing corrections during election periods.³⁰ Sustained support allows these organizations to operate at national scale while maintaining independence.

Third, Taiwan's legal framework must keep pace with influence tactics that fall outside traditional definitions of infiltration.³¹ Current law does not fully address algorithmic amplification or political messaging embedded in entertainment and lifestyle media. Updating regulations and improving coordination among judicial and digital governance institutions would allow faster responses as tactics evolve.³²

Fourth, local governments need better tools to detect and respond to influence activities. Village representatives, religious networks, and micro-influencers are frequently targeted through low-cost, low-visibility operations. Standardized risk indicators and training modules would enable earlier identification and intervention before narratives spread widely.³³ These efforts can complement media literacy and fact-checking programs without overlapping.

Fifth, international engagement is a key part of building resilience. Programs such as the Global Cooperation and Training Framework help Taiwan share lessons, coordinate responses, and experiment with platform governance and election integrity in collaboration with other democracies.³⁴

Together, these five measures form a whole-of-society approach that integrates government, civil society, local institutions, and international partnerships. The goal is to protect trust, identity, and political judgment through coordinated preventive measures, rather than reacting only to individual false messages.³⁵

CONCLUSION: TAIWAN STANDS AT THE FRONT LINE OF DEFENDING DEMOCRACY

A new war and a new world are emerging. This conflict is not centered on military force, but on influence, information, and control over society. China's actions toward Taiwan should be understood as hybrid warfare. Beijing is not trying to win a single argument or election; it seeks to wear down trust, divide society, and weaken democratic confidence over time by operating below the level of armed conflict.

Taiwan stands at the front of this struggle as a beacon of democracy facing sustained authoritarian pressure. What happens in Taiwan will shape how other democratic societies confront similar threats. Taiwan's decision to ban the Chinese social media app RedNote shows that the threat is no longer theoretical. Taipei is beginning to treat digital platforms as part of the national security environment, not just a business or speech issue, reflecting growing recognition that everyday online activity can be exploited for political influence and fraud by authoritarian states.³⁶

The future of Taiwan's democracy will be shaped not only by how it resists external pressure, but by how it strengthens internal cohesion. Stronger legal protections, smarter digital infrastructure, civic education, and trusted local networks are all essential, but they must work together. Taiwan cannot rely on any single tool or actor. Defense must be multi-layered, proactive, and embedded in daily life. China's strategy is clear and so must be Taiwan's response.

Defending Taiwan is therefore not only about one country. It is about whether democratic systems can withstand this new form of authoritarian challenge. Democracies must recognize this shift and prepare to confront it together. **PRISM**

Notes

¹ Rawnsley, Gary D. "Taiwan's Soft Power and Public Diplomacy." *Journal of Current Chinese Affairs* 43, no. 3 (September 2014): 161–74. <https://doi.org/10.1177/186810261404300307>.

² Taiwan Affairs Office of the State Council. "Working Together to Realize Rejuvenation of the Chinese Nation and Advance China's Peaceful Reunification." January 2, 2019. https://www.gwytb.gov.cn/wyly/201904/t20190412_12155687.htm.

³ China Law Translate (CLT), "CCP Regulations on United Front Work," *China Law Translate*, April 17, 2025, <https://www.chinalawtranslate.com/en/CCP-Regulations-on-United-Front-Work/>.

⁴ Brady, Anne-Marie. "Magic Weapons: China's Political Influence Activities under Xi Jinping | Wilson Center." *Wilson Center*, September 18, 2017. <https://www.wilsoncenter.org/article/magic-weapons-chinas-political-influence-activities-under-xi-jinping>.

⁵ John Dotson, "Wang Huning's First Year Supervising the United Front System: Taiwan Policy and Discourse," *Global Taiwan Institute*, January 10, 2024, <https://globaltaiwan.org/2024/01/wang-hunings-first-year-supervising-the-united-front-system-taiwan-policy-and-discourse/>.

⁶ Chien-Yuan Sher et al., "In the Name of Mazu: The Use of Religion by China to Intervene in Taiwanese Elections," *Foreign Policy Analysis* 20, no. 3 (April 27, 2024), <https://doi.org/10.1093/fpa/orae009>.

⁷ Aukia, Jukka. "China's Hybrid Influence in Taiwan: Non-State Actors and Policy Responses," 2023. <https://www.hybridcoe.fi/wp-content/uploads/2023/04/20230406-Hybrid-CoE-Research-Report-9-Chinas-hybrid-influence-in-Taiwan-WEB.pdf>.

⁸ Aukia, Jukka. "China's Hybrid Influence in Taiwan: Non-State Actors and Policy Responses," 2023. <https://www.hybridcoe.fi/wp-content/uploads/2023/04/20230406-Hybrid-CoE-Research-Report-9-Chinas-hybrid-influence-in-Taiwan-WEB.pdf>.

⁹ Nathan Beauchamp-Mustafaga, "Exploring Chinese Military Thinking on Social Media Manipulation against Taiwan–Jamestown," *Jamestown Foundation*, 2021, <https://jamestown.org/exploring-chinese-military-thinking-on-social-media-manipulation-against-taiwan/>.

¹⁰ Ho-Chun Herbert Chang, Austin Horng-En Wang, and Yu Sunny Fang. "US-Skepticism and Transnational Conspiracy in the 2024 Taiwanese Presidential Election," May 20, 2024. <https://doi.org/10.37016/mr-2020-144>.

¹¹ Brian Hioe, “Chinese Influencer Ordered to Leave Taiwan over Pro-Unification Content,” *The Diplomat*, April 2025, <https://thediplomat.com/2025/04/chinese-influencer-ordered-to-leave-taiwan-over-pro-unification-content/>.

¹² Kerry Gershaneck, “Political Warfare against Intervention Forces,” Air University (AU), April 21, 2025, <https://www.airuniversity.af.edu/JIPA/Display/Article/4167178/political-warfare-against-intervention-forces/>.

¹³ Yu, Cheryl. “Viral Documentary Exposes CCP’s United Front Operations in Taiwan–Jamestown.” *Jamestown Foundation*, 2025. <https://jamestown.org/viral-documentary-exposes-ccps-united-front-operations-in-taiwan/>.

¹⁴ The Overseas Community Affairs Council–Taiwan, “Taiwan to No Longer Recognize Qualifications from United Front Schools,” 2026, <https://www.ocac.gov.tw/OCAC/Eng/Pages/Detail.aspx?nodeid=329&pid=72907824>.

¹⁵ Bowe, Alexander . “China’s Overseas United Front Work Background and Implications for the United States,” 2018. https://www.uscc.gov/sites/default/files/Research/China%27s%20Overseas%20United%20Front%20Work%20-%20Background%20and%20Implications%20for%20US_final_0.pdf.

¹⁶ Davidson, Helen, and Chi Hui Lin. “A Race against Time’: Taiwan Strives to Root out China’s Spies.” *The Guardian*, February 2, 2024, <https://www.theguardian.com/world/2024/feb/02/taiwan-china-spies-beijing-espionage>.

¹⁷ United States House Select Committee on Strategic Competition between the United States and the Chinese Communist Party. “MEMORANDUM: UNITED FRONT 101,” <https://chinaselectcommittee.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/uf-101-memo-final-pdf-version.pdf>.

¹⁸ Suzuki, Takashi. “China’s United Front Work in the Xi Jinping Era – Institutional Developments and Activities.” *Journal of Contemporary East Asia Studies* 8, no. 1 (January 2, 2019): 83–98. <https://doi.org/10.1080/24761028.2019.1627714>.

¹⁹ Lee, Yimou. “China Courts Taiwanese Worshippers in Religious Charm Offensive, Study Shows.” *Reuters*, October 23, 2025. <https://www.reuters.com/world/china/china-courts-taiwanese-worshippers-religious-charm-offensive-study-shows-2025-10-23/>.

²⁰ Wu, Guoguang . “The United Front, Comprehensive Integration, and China’s Nonmilitary Strategy toward Taiwan.” *Asia Society*, 2024. <https://asiasociety.org/policy-institute/united-front-comprehensive-integration-and-chinas-nonmilitary-strategy-toward-taiwan>.

²¹ Zhang, Yi in. “Mainland Sees Sharp Rise in Cross-Strait Marriages.” *China Daily HK*, 2023. <https://www.chinadailyhk.com/hk/article/352090>.

²² Mainland Affairs Council, Republic of China (Taiwan). “MAC Issues Stern Clarification: Only 278 Mainland Chinese Spouses Have Not Complete Supplementary Submission of Proof of Cancellation of Household Registration in Mainland China due to Loss of Contact; Taiwan Status Will Not Be Revoked without Prior Contact.” *Mainland Affairs Council*, Republic of China (Taiwan), March 29, 2017. https://www.mac.gov.tw/en/News_Content.aspx?n=A921DFB2651FF92F&sms=37838322A6DA5E79&s=489AF4839CCD58B3.

²³ Lara Momesso, “‘I Vote so I Am’: Marriage Migrants’ Political Participation in Taiwan,” *Journal of Current Chinese Affairs*, May 3, 2022, 186810262210798, <https://doi.org/10.1177/18681026221079834>.

²⁴ Ministry of the Interior National Immigration Agency Republic of China (Taiwan). “2025.12Foreign Residents by Nationality.” *Immigration.gov.tw*. 內政部移民署 A01050000A, 2025. https://www.immigration.gov.tw/5475/5478/141478/141380/405675/cp_news.

²⁵ Ministry of the Interior National Immigration Agency Republic of China (Taiwan). “0303 Notices for the Application of National Living Abroad without Registered Household in Taiwan Area for Residence in Taiwan Area.” *Immigration.gov.tw*. Ministry of the Interior National Immigration Agency Republic of China (Taiwan) A01050000A, 2024. <https://www.immigration.gov.tw/5475/5478/141465/141808/141954/>.

²⁶ Taiwan National Security Bureau, “Analysis of China’s Cognitive Warfare Tactics against Taiwan in 2025,” <https://www.nsb.gov.tw/en/assets/documents/%E6%96%B0%E8%81%9E%E7%A8%BF/3510977a-3c93-4b15-b1f8-246653335a0d.pdf>.

²⁷ The Associated Press. “Taiwan Deports a Chinese Woman for Praising Beijing’s Military Ambitions to Conquer the Island.” *AP News*, March 25, 2025. <https://apnews.com/article/taiwan-china-online-posting-deported-liu-zhenya-2c6a3ef7c125503406c239e1b88f3d90>.

²⁸ Ministry of Education Republic of China (Taiwan). “White Paper on Media Literacy Educational Policy,” <https://english.moe.gov.tw/public/Attachment/2122416591771.pdf>.

²⁹ Hung, Tzu-Chieh. “How China’s Cognitive Warfare Works: A Frontline Perspective of Taiwan’s Anti-Disinformation Wars.” *Journal of Global Security Studies* 7, no. 4 (July 19, 2022). <https://doi.org/10.1093/jogss/ogac016>.

³⁰ Price, Trinity A. *In Defense of Democracy: Taiwan’s Independent Media*. Vols. 43, 29 Oct. 2025, <https://islandora-prod.lib.lehigh.edu/lehigh-scholarship/undergraduate-publications/perspectives-business-economics/perspectives-60-6>.

³¹ Aukia, Jukka. “China’s Hybrid Influence in Taiwan: Non-State Actors and Policy Responses,” 2023. <https://www.hybridcoe.fi/wp-content/uploads/2023/04/20230406-Hybrid-CoE-Research-Report-9-Chinas-hybrid-influence-in-Taiwan-WEB.pdf>.

³² Biberman, John. “E-Governance and Civic Technology: Lessons from Taiwan.” EconStor, 2021. <https://www.econstor.eu/handle/10419/249837>.

³³ Dionis, Yuki. “Taiwan—Exploring Worldwide Democratic Innovations—European Democracy Hub.” *European Democracy Hub*, June 17, 2022. <https://europeandemocracyhub.epd.eu/exploring-worldwide-democratic-innovations-taiwan/>.

³⁴ American Institute in Taiwan (AIT), “Joint Statement on the 10th Anniversary of the Global Cooperation and Training Framework—American Institute in Taiwan,” *American Institute in Taiwan*, May 27, 2025, <https://www.ait.org.tw/joint-statement-on-the-10th-anniversary-of-the-gctf/>.

³⁵ Max Tsung-Chi Yu and Karl Ho, “COVID and Cognitive Warfare in Taiwan,” *Journal of Asian and African Studies*, November 21, 2022, 00219096221137665 <https://doi.org/10.1177/00219096221137665>.

³⁶ Chia, Osmond. “Taiwan to Ban Chinese App RedNote over Fraud Concerns.” *BBC*, December 5, 2025. <https://www.bbc.com/news/articles/c2dz014j9zeo>.

Countering Hostile Chinese Lawfare

An Irregular Warfare-Based Approach

By Crispin M. I. Smith

The People's Republic of China (PRC) is one of the world's premier practitioners of "lawfare," meaning the strategic use of legal systems and principles to achieve strategic, operational, or tactical objectives.¹ Legal warfare plays an important role in the PRC's grand strategy and is employed to restrain strategic competitors, realize territorial claims, limit international criticism, repress overseas critics and dissidents, and shape favorable conditions for potential future conflicts.² Already a capable lawfare user in today's climate of interstate competition, China is also extremely likely to use forms of lawfare during future armed conflict, having built it into military doctrine. This operational lawfare could have significant real-world military and strategic impact, delaying allied third-parties from joining crisis or conflict situations, while attriting combatant willingness to fight, disrupting and dividing anti-Chinese coalitions, and allowing the People's Liberation Army (PLA) to achieve *faits accomplis* on the ground.³

Given the obvious importance of lawfare to PLA and PRC strategy and operations from competition through to conflict, it is imperative U.S. personnel (e.g., lawyers, military and intelligence professionals, public diplomacy and information operations experts) develop and implement effective strategies to combat this form of warfare. This requires a full appraisal of the threat, a raising of awareness of that threat across government departments and within the wider civilian population, and appropriate characterization of lawfare as a form of irregular warfare meriting robust contestation wherever it is deployed by the PRC.

This article briefly outlines the Chinese lawfare threat, highlighting its potential real-world military implications. The article calls for a counter-lawfare strategy, partially grounded in irregular warfare thinking and special operations doctrine, while calling for planners and operators to draw on the irregular warfare community to cohere cross-government teams of military personnel, information operators,

Crispin Smith is a Washington DC-based attorney specializing in national security law. He leads an initiative designed to impose non-kinetic costs against great power competitors and hostile non-state actors and works on issues relating to lawfare and economic warfare. Smith previously served overseas as a British military officer supporting operations in the Indo-Pacific, Middle East, and Europe. He holds a J.D. from Harvard Law School and a B.A. in Oriental Studies from the University of Oxford.

legal practitioners, diplomats, and intelligence professionals.

THE CHINESE VIEW OF LAWFARE

Lawfare is the use of law to achieve strategic, operational, or tactical objectives.⁴ It is also used as a tool to confer legitimacy on state or non-state actions or, conversely, to delegitimize an adversary's actions.⁵ States may deploy lawfare as a strategy to achieve goals in the context of competition and interstate rivalry, as well as during times of conflict.⁶

Non-kinetic military effects are a long-standing and integral component of Chinese strategic thought.⁷ Contemporary PRC foreign policy and military doctrine are demonstrably shaped by the enduring tenets of Marxist-Leninist and Maoist ideologies.⁸ This philosophical grounding, encompassing concepts such as “people’s war,” revolutionary struggle, and political warfare, contributes to a divergence from the more conventional Western delineations between “war”—*i.e.*, periods characterized by overt military violence—and “peace.”⁹ Consequently, the Chinese Communist Party (CCP) and PLA operate with a conceptual framework that inherently blurs these traditional distinctions, a contrast to the prevailing interpretations among Western policymakers, warfighters, and legal scholars. This in turn means that the CCP conceptualizes warfare broadly as a pervasive struggle between competing entities, transcending mere kinetic application of brute force.¹⁰

Within this strategic context, PLA military theorists formally consolidated specific non-kinetic practices under the oft-cited “Three Warfares” which encompass public opinion warfare psychological warfare and legal warfare, or lawfare. Originating in CCP military thinking as early as 1963, this tripartite concept formally integrated into official PLA doctrine in the early 2000s and continues to form an important part of Chinese grand strategy, manifested in strategic competition with

the United States.¹¹ The next sections briefly consider how China uses lawfare today, and how lawfare could be deployed to support Chinese military objectives in the future.

CHINESE LAWFARE IN STRATEGIC COMPETITION

Given CCP blurring of the lines between war and peace and its interest in non-kinetic military effects to achieve state goals, it is unsurprising China uses lawfare to achieve objectives within the context of great power competition that falls below the threshold of active conflict.¹² Indeed, it is well documented that China already uses lawfare as part of its grand strategy within interstate competition.¹³

Lawfare plays an important role underpinning a Chinese grand strategy aimed at gradually displacing the American-led international order. Lawfare is used to impede or delegitimize U.S. and allied operations and influence by asserting novel interpretations of international law, (for example, concerning maritime and aerial transit in contested zones).¹⁴ Beijing frequently challenges the legality of foreign military vessels conducting intelligence, surveillance, and reconnaissance (ISR) activities within its exclusive economic zone (EEZ), arguing such actions are not covered by “innocent passage.”¹⁵ By legally challenging freedom of navigation operations, surveillance activities, and military exercises, Beijing aims to constrain the operational space and increase political and legal risks associated with those operations – undermining the legal justification for U.S. presence and activities in the Indo-Pacific, and potentially leading to self-deterrence or diminished allied support.¹⁶

Lawfare strategies also help consolidate and legitimize the PRC’s own expanding influence. This includes shaping international legal discourses and norms to align with Beijing’s interests. For example, China works hard to influence international organizations and judicial forums to promote its

interpretations of sovereignty, territorial integrity, and non-interference.¹⁷ Meanwhile, initiatives like the Belt and Road Initiative (BRI) allow China to impose legally binding agreements that often favor its own legal frameworks. Beijing also works to shape norms in emerging domains, such as cyberspace and outer space, advocating for principles like “cyber sovereignty” to strengthen state control while codifying domestic laws with extraterritorial reach, further extending Beijing’s legal writ. And by consistently presenting its actions as compliant with international law, China builds a narrative of a responsible global power, even as it pursues revisionist aims.

China’s lawfare during interstate competition is also a valuable tool for achieving unlawful territorial objectives without resorting to overt and kinetic conflict. A well-studied example is the South China Sea, where Beijing has strategically deployed legal arguments, often tied to historical narratives and expansive interpretations of international conventions, to buttress its claims. The construction of artificial islands, followed by their civilian and military development, creates “facts on the ground” that are then reinforced and defended through legal and diplomatic pronouncements. Similarly, regarding Taiwan, Beijing consistently asserts the “One China” principle through legal and diplomatic channels, (successfully) pressuring nations and international bodies to recognize PRC sovereignty over the island, thereby isolating Taipei diplomatically, militarily, and economically without need for direct military intervention, while laying the groundwork to defend against external legal challenges (and potential *casus belli* for foreign intervenors) in the event of an annexation attempt.

Finally, China employs lawfare to set favorable conditions for itself in potential future conflict. By continuously challenging the legal basis of foreign military operations in its vicinity and solidifying its own territorial and legal claims, Beijing seeks

to pre-emptively delegitimize potential military responses to its actions. This includes portraying U.S. or allied military actions as illegal aggression, eroding international legitimacy. Domestic laws related to national security and counterterrorism are also used to justify actions that may be seen as infringements on international norms, creating domestic sovereignty justifications to insulate otherwise unlawful actions from external legal challenge. This pre-conflict conditioning may degrade the willingness to fight of potential Chinese adversaries while isolating them diplomatically. It also ensures that, should kinetic conflict occur, China enters the fight having already won significant battles in the legal and informational domains and having secured real-world military advantages in the physical domain.

CHINESE LAWFARE IN INTERSTATE CONFLICT

Should active conflict break out between China and a third-party state, it is almost certain that the PLA will also use lawfare to support combat operations. This operational lawfare is likely to deliver real-world effects in support of PLA fighters, to the detriment of U.S. combat operations.¹⁸ Some examples of how these effects could be achieved follow.

Shaping and Preparing the Battlespace Ahead of Conflict. China’s lawfare already has the effect of creating favorable conditions from which to fight in the future. In the context of Taiwan, for example, China’s efforts to diminish Taiwan’s diplomatic recognition and promote narratives asserting Taiwan as an inalienable part of the PRC are likely to have the effect of delaying or deterring foreign intervention.¹⁹ Meanwhile, other lawfare efforts may have the effect of weakening the willingness of the Taiwanese population to resist.²⁰ Similarly, in the South China Sea, China has leveraged legal arguments to legitimize its—now entrenched—military presence on artificial islands, creating a *fait accompli* that would be

difficult for adversaries to contest militarily should hostilities begin (while also creating defensive positions that could limit U.S. or allied freedom of action in the South China Sea in times of conflict). In a future conflict, Chinese artificial islands, reinforced with military forces, intelligence sensors, and anti-air and anti-ship systems, could give the PLA a significant edge. Hostile forces could find Chinese presence to be a *fait accompli* not worth contesting should hostilities break out: militarily, an enemy already positioned and holding defensive positions may be difficult and costly to dislodge. Alternatively, military forces (and supply chains) would likely find it challenging to operate in the South China Sea, delaying the passage of forces and materiel around the Indo-Pacific.²¹

Delaying or Deterring Third Parties from Entering an Imminent or Ongoing Conflict. Upon the outbreak of potential crisis or conflict, lawfare could have a devastating impact on the United States's ability to get to and sustain military action within the first and second island chains of the western Pacific. In a Taiwan defense scenario, for example, PLA lawfare operators would be highly likely to use a combination of *jus ad bellum* and *jus in bello* lawfare attacks against any U.S. intervention.²² These narratives would assert that any external intervention is an illegal violation of international law—but the arguments would be primarily directed at third-party countries and their populations, aiming to sway their decision-makers and generate public opposition to supporting U.S. or allied operations. This in turn could cause crucial delays in logistical and operational support, by impacting partner willingness to sign or honor access, basing, and overflight agreements, while eroding domestic U.S. support for military operations and willingness to fight.

Attrititing Willingness to Fight. The PLA may also use lawfare—in combination with the other elements of the “Three Warfares” (*i.e.*, “public

opinion warfare” and “psychological warfare”)—to attrit an adversary's willingness to fight. This may target the morale and willingness of actual combatants to fight or may be intended to weaken support among domestic populations and voting publics. To accomplish this, the PLA may seek out, highlight, or invent adversary violations of international norms, including violations of the Law of Armed Conflict (LOAC) or international humanitarian law (IHL), international human rights law, or an adversary's domestic laws. These violations may be heavily publicized to discredit adversary forces and cast doubt on the morality and legality of their actions and intentions.²³

Dividing Hostile Coalitions of Foreign Nations. China may use operational lawfare to exploit legal and political differences among potential coalition partners.²⁴ This strategy could create interoperability challenges while driving wedges between allies, thereby eroding the legitimacy of any counter-China coalition or alliance during conflict while limiting said coalition's ability to operate as more than the sum of its parts. Concurrently, China is likely to leverage its growing influence within international organizations, like the United Nations, to align them with CCP goals, orchestrate votes to censure adversaries, and amplify Chinese positions, thereby building its own global supporting blocs—while further eroding the international support for and legitimacy of any U.S.-led effort to counter PLA belligerence.

*Achieving Military *Fait Accompli* and Quickly Normalizing Territorial Gains.* In scenarios involving territorial conquest, China might attempt a rapid military *fait accompli*. Lawfare could then be deployed to normalize these newly acquired territories, for example, by framing annexations as the mere reassertion of control over Chinese land while asserting that international laws of belligerent occupation do not apply.²⁵ This strategy would seek to mitigate international criticism, prevent severe

economic sanctions, and limit diplomatic ostracization by portraying the acquisition as a legitimate domestic matter.

At this point it should be clear to readers that PLA operational lawfare has the potential to act as a major force-multiplier in support of Chinese military objectives—with serious ramifications for U.S. operations. It should also be clear that China is already conducting the shaping and preparatory activity needed to maximize the effectiveness of a lawfare-in-conflict strategy. These efforts, conducted by PLA and CCP diplomats, media, and affiliates, shape the legal information environment and include sustained attacks on the United States’s credibility regarding its respect for international law and human rights, as well as pro-PRC narratives on sovereignty issues and interpretations of international law that favor or justify Chinese activity while limiting potential Chinese adversaries. In many cases, these shaping attacks have a basis in real international legal arguments, allowing PLA lawfare operators to spin and promulgate believable accounts claiming the moral and legal high ground. It should also be clear to military audiences that this operational lawfare can (and likely will) be deployed to achieve specific—*i.e.*, military—effects, and the relevant legal narratives will therefore be directed at specific target audiences to achieve those effects. Sometimes those audiences will be American or Western. Just as often, however, they will be decisionmakers and populations in third-party countries. Countering this lawfare-driven information activity, therefore, will require careful and tailored counter-messaging, delivered both overtly and discreetly and at both the strategic level and more locally. The skills, experience, and access required to defend against lawfare should therefore draw, *inter alia*, on the irregular warfare community. The valuable skillset they bring, as well as the broader interests of the irregular warfare when it

comes to countering legal warfare, will be discussed below.

LAWFARE AND IRREGULAR WARFARE

That PRC lawfare—in both strategic competition and during conflict—is a serious threat to U.S. interests is clear. Many scholars and practitioners have observed that there is an urgent need for a Department of War and cross-U.S. government strategy to understand and counter this legal warfare.²⁶ Within any such strategy, however, there is a particularly acute need for the irregular warfare community to step up. In part this is because lawfare can and should be seen as a form of hostile irregular warfare. Irregular warfare specialists must also lean in because they are particularly likely to possess qualities and skills required to intelligently and effectively counter hostile lawfare. Finally, irregular warfare specialists are particularly vulnerable to certain forms of lawfare, which have the potential to significantly harm their freedom of movement and ability to operate on the ground.

LAWFARE AS IRREGULAR WARFARE

As outlined above, lawfare is the purposeful use of law to achieve strategic, operational, or tactical objectives. It may also be used to legitimize a state or non-state actor’s actions or to delegitimize the actions of an adversary.²⁷ States may deploy lawfare as a strategy to achieve goals in the context of competition and interstate rivalry, as well as during times of open conflict. The PRC quite clearly views lawfare as a form of actual warfare, as is made explicit under the “Three Warfares,” other doctrine, and actual practice. The United States’ position, however, is less clear, although there is a growing awareness of the need to address the lawfare threat. For example, combatant commands (most notably,

and perhaps understandably, Indo-Pacific Command) have begun to develop their own counter-lawfare programs.²⁸ But a whole of government position on lawfare (let alone a comprehensive strategy) remains elusive.

Decisionmaker, policymaker, and practitioner focus on this topic could be well served by understanding lawfare for what it is: a form of irregular warfare. Recent developments, as noted below, in U.S. doctrine mean that this should be viewed as a non-controversial position as a matter of doctrine and policy. Historically, U.S. doctrine (including Doctrine for the Armed Forces of the United States, and JP 3–0, Joint Operations) defined irregular warfare as a *violent* struggle among state and nonstate actors for legitimacy and influence over the relevant population(s) [emphasis added].²⁹

More recently, however, irregular warfare has been further defined as “a form of warfare where states and non-state actors *campaign to assure or coerce states or other groups* through indirect, non-attributable, or asymmetric activities, either as the primary approach or in concert with conventional warfare.”³⁰ Or, it is defined as the “overt, clandestine, and covert employment of military and *non-military capabilities across multiple domains* by state and non-state actors through methods *other than military domination* of an adversary, either as the primary approach or in concert with conventional warfare” [emphasis added].³¹ Lawfare, quite clearly, fits comfortably within these definitions. It is a non-military capability able to impact multiple domains. Deployed successfully, it can be (and has been) used to coerce states or other groups without resorting to military domination. And, as outlined above, it is likely that the PLA can and will deploy lawfare to achieve coercive military effects in support of conventional operations, should active hostilities ever arise.

Firmly identifying lawfare as a recognizable form of irregular warfare should help military and

civilian planners and policymakers firmly view the strategy as a tool of warfare—just as the PLA already views it. This could further establish hostile lawfare as not just a problem for lawyers and scholars, but as an effective form of hostile warfare used by adversaries to harm U.S. interests during sub-threshold strategic competition, to shape global and regional conditions to maximize hostile advantages in potential future conflicts and, should those conflicts manifest, to support conventional warfare. Framed this way, hostile lawfare should clearly require and warrant a whole-of-government counterstrategy that draws on a wide range of personnel and policy tools.

IRREGULAR WARFARE PRACTITIONERS AS COUNTER-LAWFARE SPECIALISTS

If hostile lawfare is a form of irregular warfare, irregular warfare specialists are, unsurprisingly, useful subject matter experts able to help meet the threat. Any counter-lawfare strategy would do well to include these specialists both for their experience and capabilities and for their ability to cohere the right people and organizations to meet specific challenges.

An effective lawfare strategy must (among other things) find the right personnel to counter and mitigate adversary lawfare.³² That means building blended teams of specialists and generalists who can find, analyze, and quickly respond to Chinese operational lawfare. But the needed skills are rarely found in a single individual or organization. Instead, these teams must cohere not just legally trained personnel, but also military and civilian intelligence analysts, information-operation and media-engagement professionals, and cultural and linguistic specialists.

Legal personnel should include both lawfare experts and more generalist lawyers, perhaps from the military’s Judge Advocate General’s (JAG) Corps or drawn from agency or department legal advisor

offices. This legal hub would help identify potential lawfare efforts and draft legally sound counter-narratives. Intelligence personnel, meanwhile, will be crucial in drawing on and analyzing classified source material to understand how Chinese lawfare practice may be developing. Intelligence analysts will also be tasked with understanding and predicting likely PLA intentions, the effects needed to achieve those intentions, and how lawfare efforts will be deployed to enable or achieve those effects.

Information and media operators will need to work with the generalist lawyers and lawfare experts to ensure that no Chinese lawfare effort goes uncontested: once lawyers identify lawfare attacks and prepare legal counterarguments and narratives, information operators must then work to deliver those counter-messages to the correct target audience using effective media and in a timely and convincing manner. A legally correct but unconvincing response to a lawfare narrative risks being counterproductive. Likewise, a convincing and legally sound argument delivered days after a target audience has already been persuaded of U.S. malfeasance is likely to be ineffective.

Lastly, cultural experts will be needed to help ensure that lawfare countermeasures are appropriate for their target audiences. The potentially large number of disparate audiences Chinese lawfare may target will likely require drawing on the expertise of numerous cultural and linguistic subject-matter specialists. Individuals with legal expertise related to specific cultural and regional contexts will be particularly helpful for understanding how different legal narratives could “play out.” Such individuals may be rare (and, where found, could be difficult to clear at the highest security levels). Nevertheless, they should be sought out and could include local advisors on host-nation domestic laws—particularly foreign nationals or dual citizens living abroad and willing to support local diplomatic staff. Other groups may be drawn upon for local legal and

cultural expertise, and might include members of U.S. human rights, developmental aid, and legal aid non-government organization (NGO) communities.

Many irregular warfare practitioners will likely immediately feel some familiarity with these requirements. That is because irregular warfare practitioners have often had to build similar teams or joint interagency task forces to achieve their missions and tasks (even if the focus was somewhat different). Irregular warfare operators are also often particularly familiar with the need for—and challenges associated with—working with diverse teams and military and civilian personnel, blending skills sets, and drawing on local nationals, host nation and partner forces, deep subject matter experts, or cultural specialists. Irregular warfare operators are also likely to be particularly familiar with developing creative, unconventional, or completely novel solutions to achieve real-world effects with little or no military or kinetic application of force.

In short, irregular warfare specialists are extremely well placed to lead on counter-lawfare strategy and U.S. departments, agencies, and combatant commands with irregular warfare missions or components should take the lead in understanding, planning for, and countering Chinese hostile lawfare. These organizations and affiliated individuals have the team-building experience to cohere the necessary eclectic skills, and the mindset needed to understand both how adversaries could use lawfare for effect during competition, crisis, and conflict. They are also likely to have experience deploying to countries and locations where hostile lawfare could prove especially effective: peripheral theaters, global swing states, or among foreign partners. Any U.S. counter-lawfare strategy must leverage these advantages.

IRREGULAR WARFARE PRACTITIONERS AS TARGETS OF HOSTILE LAWFARE

As argued above, lawfare and counter-lawfare should be a task wholeheartedly and urgently embraced by irregular warfare practitioners, both because lawfare *is* a form of irregular warfare, and because irregular warfare practitioners are well placed to provide organizational backbone and intellectual heft needed to counter this important tool of Chinese hostile power. But irregular warfare practitioners should also take the lead for another equally important reason: they are particularly vulnerable to hostile lawfare.

Individuals, units, and agencies conducting irregular warfare missions and tasks often necessarily operate in discreet, clandestine, or covert postures. They are also especially likely to conduct operations in a legal “gray zone” – for example, actions conducted under Title 50 of the U.S. Code where the U.S. government may seek to influence foreign conditions without acknowledging its role. Irregular warfare practitioners may also take on liaison roles, working closely with foreign partners or out of embassies around the world, requiring consent and a degree of trust from local authorities in-country.

These roles may be particularly vulnerable to hostile lawfare. Since irregular warfare is often undertaken by elite military units or others operating in particularly hostile environments, but from behind a veil of secrecy or obfuscation, there is a particular vulnerability that kinetic engagements will be exploited for allegations of war crimes or other human rights abuses. Western populations rightly take these allegations extremely seriously, but special forces units or other practitioners may find defending their actions especially challenging due to the difficulty of presenting operational (but classified) evidence to legal courts or to the “court”

of public opinion. Special forces units belonging to U.S. Five Eye partners have faced allegations of war crimes from Afghanistan in recent years, resulting in convictions and jail time for offenders, terminations, losses of public confidence, parliamentary and public scrutiny, and loss of operational freedoms, and loss of trust with host nations and partner forces.³³ In many cases the allegations proved to be real—warranting serious legal punishment—but the military impact can be severe. For example, elite operators go through long and expensive training pipelines and can be difficult to replace. Meanwhile, in many cases, Chinese information operators have sought to exploit these cases for strategic advantage.³⁴

While it is already the case that irregular warfare operators are vulnerable to legal warfare, it is likely that the cost of deploying hostile lawfare against them may also be falling thanks to advances in generative artificial intelligence (GenAI). This could make lawfare a particularly cost-effective way for hostile states to deal with irregular warfare personnel. Specifically, advances in GenAI may make fabricating or embellishing evidence of legal violations ever easier and more convincing.³⁵ Units operating in military or legal gray zones or under covert and clandestine postures could be particularly vulnerable to such fabrications due to public and host-nation uncertainty about their role and activities. Concerns over the sensitivities of irregular warfare activities could also cause a reluctance to publicly comment on or quickly engage with hostile lawfare, resulting in a ceding of the narrative and information environment. Regardless of the truth of any given incident, this type of faked evidence could result in a breakdown in local trust between operators and partner forces or host nations, loss of permissions, legal action or convictions, and so on—all to the detriment of the mission and to U.S. and allied interests.

IRREGULAR WARFARE WITHIN A COUNTER-LAWFARE STRATEGY

As I have outlined throughout this paper, Chinese lawfare is a serious challenge to U.S. interests both in strategic competition, through sub-threshold conflict, and into conventional warfare. It is a form of Chinese warfare conducted against the U.S. and other countries to their detriment and to the benefit of PRC grand strategy and as part of theatre-setting for future conflict.³⁶ It is, by Department of War (DOW) definitions, arguably a form of “irregular warfare” and should be treated as a major priority by the irregular warfare community.³⁷

To counter the threat, there is an urgent need for a whole-of-government U.S. counter lawfare strategy. Several scholars and practitioners have put forward ideas for what such a strategy should involve.³⁸ Broadly, however, U.S. government departments and agencies must work together to comprehensively understand Chinese lawfare strategies and techniques, using this understanding to develop intelligence driven approaches to preempt and predict likely lawfare lines of attack.³⁹ As outlined above, effective counter-lawfare teams should also be stood up. These will necessarily draw on an array of personnel with diverse skillsets, including legally trained personnel, military and civilian intelligence analysts, information-operation and media-engagement professionals, and cultural and linguistic specialists.⁴⁰ These teams should be embedded in operational-level military commands and included in wargames, exercises, and planning sessions. They should identify potential Chinese operational lawfare campaigns now and research and prepare effective counterarguments and narratives accordingly. Where necessary, these teams should identify preparatory activities needed to counter Chinese narratives seeded in advance of conflict to enable future lawfare, or to lay the groundwork to improve friendly U.S. counternarrative success against prospective arguments.

U.S. and allied governments should also consider placing lawfare specialists in embassies, particularly in the Indo-Pacific and tasking them with identifying and coordinating responses to locally targeted Chinese lawfare. They should work with local legal professionals and embassy cultural specialists to identify potential Chinese lawfare operations at an early stage. They should also provide advice on the most appropriate ways to counter-message in their respective local contexts.⁴¹ These teams should then be empowered to actively contest inaccurate and misleading legal analyses and narratives, as well as the capture of judicial and legal bodies wherever identified. Wherever possible, defensive lawfare operators should be permitted to quickly respond to counteract falsehoods and institutional influence campaigns. Meanwhile, to enable speedy counter-messaging the teams should work to preemptively detect active or likely legal attacks, allowing lawyers and information operators to craft responses proactively instead of reactively.

Within this context, irregular warfare operators should support and lead the development of the broader strategy. As outlined above, organizations engaged in irregular warfare are especially likely to have access to personnel with relevant skills and expertise and, moreover, are well placed to cohere complex blended teams. In particular, counter-lawfare operators should draw on lessons from “foreign internal defense” (FID) missions, as well as “military information support operations” (MISO). The DOW defines FID as “the participation by civilian agencies and military forces of a government or international organization in any of the programs or activities taken by a host nation government to free and protect its society from subversion, lawlessness, insurgency, violent extremism, terrorism, and other threats to its security.”⁴²

As outlined above, Chinese lawfare may be deployed to coerce or influence governments or populations of foreign countries. Where encountered in

countries in which the U.S. already has military ties, counter-lawfare might be deployed independently or as part of wider FID programs. This could mean including counter-lawfare efforts in existing security force assistance programs (for example, by training law enforcement personnel to help identify and counter legal warfare), or through direct support—for example, through intelligence sharing, funding of judicial systems and rule of law programs, wider counter lawfare trainings, and other engagements. This should be done to help harden foreign governments and populations to Chinese lawfare campaigns—making it more costly for the PLA to shape global operating environments or coerce third-party countries.

MISO operations, among other U.S. government information capabilities (including, for example, information activities led by other parts of the intelligence community or State Department), should also play an important role in an irregular warfare-led counter-lawfare strategy. In many cases, Chinese lawfare is a particularly potent form of hostile information operation, targeting foreign governments and populations in order to boost PRC legitimacy or weaken the legitimacy of the United States and allies (that the PRC views lawfare as closely related to information operations should be clear, given legal warfare's close association with information warfare and psychological warfare in the context of the "Three Warfares"). Countering lawfare will therefore often require timely and coordinated information activity. This plays to MISO operators' strengths, given their experience identifying appropriate target audiences and conducting strategic messaging for real-world effect and in support of national objectives.

Irregular warfare specialists should also ensure their relevant experience is fed in to support wider government counter-lawfare strategies. In some cases, employment of irregular warfare personnel may be inappropriate (for example, where purely

civilian and law enforcement departments are better placed to counter hostile narratives or actions). Nevertheless, as wider lawfare strategies and capabilities are developed, irregular warfare specialists should be consulted and should offer training support to the wider counter-lawfare community.

CONCLUSION

Lawfare is already delivering results for the PRC as part of interstate competition and will likely play an important role should the PLA go to war. This hostile lawfare is a form of irregular warfare and poses a clear threat to U.S. interests and operations and requires the development and implementation of a whole-of-government counterstrategy. At a minimum, this must involve building operational counter-lawfare teams comprising government lawyers, intelligence personnel, information operators, public diplomacy experts, and cultural specialists. These teams must work to understand and preempt hostile legal efforts and narratives and must counter those attacks in a manner that speaks effectively to the foreign audiences especially likely to be targeted and influenced by Chinese efforts.

In support of this strategy, lawfare should be classified as a form of irregular warfare. Lawfare comfortably fits current U.S. doctrinal definitions of IW as a non-military capability used to coerce states or groups through indirect, non-attributable, or asymmetric activities. By classifying lawfare this way, U.S. policy understanding of lawfare would be brought in line with how the PLA already views legal warfare, helping military and civilian planners to recognize its significance and plan effectively against it.

Meanwhile irregular warfare practitioners and operators can and should play a leading role in operationalizing the counter-lawfare strategy. Irregular warfare specialists possess the experience needed to build the required blended teams and are well placed to support the development of

creative countermeasures that achieve military and strategic effects without resorting to kinetic force drawing, for example, on existing irregular warfare missions and tasks. By taking the lead, the irregular warfare community can drive forward and support U.S. contestation of the legal “domain,” protecting U.S. interests while maintaining the legitimacy of the international system. **PRISM**

Notes

¹ Crispin Smith, “Chinese Lawfare in Conflict: the Threat to U.S. Operations,” *Harvard National Security Journal*, vol. 16, no. 2, (2025); see also Jill Goldenziel, “Law as a Battlefield: The U.S., China, and the Global Escalation of Lawfare,” *Cornell Law Review*, vol. 106, (2021): 1094-97; see also Orde F. Kittrie, “Lawfare, China, and the Grey Zone,” in *Hybrid Threats and Grey Zone Conflict: The Challenge to Liberal Democracies* 209 (Mitt Regan & Aurel Sari eds., 2024); See also Jordan Foley, “Multi-Domain Legal Warfare: China’s Coordinated Attack on International Rule of Law,” *Lieber Inst. Articles War* (May 28, 2024), <https://lieber.westpoint.edu/multi-domain-legal-warfare-chinas-coordinated-attack-international-rule-law/> [https://perma.cc/8WE6-9F9G] (noting that use of law in gray zone conflict is “most pronounced in the Indo-Pacific where the People’s Republic of China (PRC) remains the United States[’s] pacing challenge and continues to engage in controversial lawfare”). For a discussion of lawfare definitions, see Dunlap, *Lawfare Today* (“[lawfare] is the strategy of using—or misusing—law as a substitute for traditional military means to achieve an operational objective”); Kittrie, *Lawfare: Law as a Weapon of War* (lawfare comprises “compliance-leverage disparity lawfare,” meaning the use of an adversary’s own compliance with domestic or international law and rules of engagement to constrain that adversary and so obtain battlefield advantage; and “instrumental lawfare,” or using legal tools in place of conventional military action to achieve a military objective); Goldenziel, *Law as a Battlefield* (lawfare includes “the purposeful use of law to bolster the legitimacy of one’s own strategic, operational, or tactical objectives toward a particular adversary, or to weaken the legitimacy of a particular adversary’s particular strategic, operational, or tactical objectives”).

² Smith, “Chinese Lawfare in Conflict: The Threat to U.S. Operations.”

³ Smith, “Chinese Lawfare in Conflict: The Threat to U.S.

Operations.”

⁴ Charles J. Dunlap, Jr., “Lawfare Today: A Perspective,” 3 *Yale Journal of International Affairs*, vol. 3, (2008): 146; Orde F. Kittrie, *Lawfare: Law as a Weapon of War* 18–25 (2016); Goldenziel, “Law as a Battlefield.”

⁵ Goldenziel, “Law as a Battlefield.”

⁶ Smith, “Chinese Lawfare in Conflict.”

⁷ In the *Art of War* (c. 5th Century BCE), Sun Tzu noted that “defeating an enemy without fighting is the acme of skill.” “The Art of War” chapter 3; see also Steven Halper et al., “China: The Three Warfares” (2013): 32, <https://cryptome.org/2014/06/prc-three-wars.pdf> [https://perma.cc/U5LD-KLHT] (noting that, while the idea of the Three Warfares is a relatively new concept in PLA manuals, the role of perception management has been a staple of PLA activities since at least the 1930s and that the “Three Warfares” are “entirely congruent with Chinese strategic culture”).

⁸ “Formulation of Foreign Policy of New China on the Eve of its Birth,” *Ministry Foreign Affairs of the People’s Republic of China*, (last visited Mar. 14, 2025), https://www.mfa.gov.cn/eng/zy/wjls/3604_665547/202405/t20240531_11367589.html [https://perma.cc/SN67-P2KN]; see also Julia Lovell, “Maoism: A Global History,” (2019) (noting that “in the context of a global great-power vacuum...early evidence suggests that the [CPC] is deploying strategies developed under Mao...to increase its influence abroad”).

⁹ Dean Cheng, “Winning Without Fighting: Chinese Legal Warfare,” (2012), <https://www.heritage.org/asia/report/winning-without-fighting-chinese-legal-warfare> [https://perma.cc/N9WP-E56L]; see also Elsa Kania, “The PLA’s Latest Strategic Thinking on the Three Warfares,” *Jamestown Foundation China Brief*, vol. 16, no. 13, (Aug. 22, 2016), <https://jamestown.org/program/the-plas-latest-strategic-thinking-on-the-three-warfares/>.

¹⁰ Seth G. Jones et al., “Competing Without Fighting: China’s Strategy of Political Warfare” (2023): 2–4, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-08/230802_Jones_CompetingwithoutFighting.pdf?VersionId=Zb5B2Le0lf0kk7.QH7E0meA9phGqQEzf [https://perma.cc/LK5F-UL8B] (discussing the CPC’s view of “political warfare,” or power politics short of conventional war, and noting that China views warfare as a struggle between competing entities and not just the use of brute force).

¹¹ Peter Mattis, “China’s ‘Three Warfares’ in Perspective,” *War on the Rocks* (Jan. 30, 2018), <https://warontherocks.com/2018/01/chinas-three-warfares-perspective/> [https://perma.cc/2AS3-NLPU]; Cheng, “Winning without Fighting;” Halper et al., “China: The Three Warfares.”

¹² Joint Chiefs of Staff, Joint Doctrine Note 1-19, Competition Continuum v, 2-3 (2019) (“Competition is a fundamental aspect of international relations. As states and non-state actors seek to protect and advance their own interests, they continually compete for diplomatic, economic, and strategic advantage.” The DoD sees “Competition Below Armed Conflict” as encompassing “[s]ituations in which joint forces take actions outside of armed conflict against a strategic actor in pursuit of policy objectives. These actions are typically nonviolent and conducted under greater legal or policy constraints than in armed conflict but can include violent action by the joint force or sponsorship of surrogates or proxies.” Activities may include “diplomatic and economic activities; political subversion; intelligence and counterintelligence activities; operations in cyberspace; and the information environment, military engagement activities, and other nonviolent activities to achieve mutually incompatible objectives, while seeking to avoid armed conflict.”)

¹³ Goldenziel, “Law as a Battlefield.” See also Rush Doshi, “The Long Game: China’s Grand Strategy to Displace American Order” (2021) (though Doshi does not address lawfare directly, he describes PRC efforts to limit U.S. influence within global institutions while building up Chinese influence in existing and new institutions). See also Jamil N. Jaffer’s testimony before the U.S. House Select Committee on the Chinese Communist Party on “How the CCP Uses the Law to Silence Critics and Enforce its Rule” noting that Xi Jinping the case for China to seek control of the “rule of law” system built by the Western powers and to actually has called for China to “shape the system in China’s interests by actively participat[ing] in the formulation of international rules and be a participant, promoter, and leader in the process of global governance reform” available at <https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/Jaffer%20House%20Select%20Committee%20on%20the%20CCP%20-%20Testimony%20on%20the%20CCP%20Use%20of%20Law%20to%20Enforce%20Its%20Rule%20-%20Circulation%20%289.17.24%29%20%28002%29.pdf>. See also “China’s Extraterritoriality: A New Stage of Lawfare,” noting that Xi Jinping sees lawfare as a means to achieve foreign policy goals, to manage global competition and to defend China from the reach of foreign extraterritorial norms. In a speech given during a 2022 collective study session of the Party’s Politburo, focusing on the “construction of the socialist rule of law system with Chinese characteristics” Xi underscored the importance of “using rule of law means to conduct international struggle”. These words are coded: the term

“rule of law” closely aligns with the notion of law-fare, while the term “struggle” constitutes Xi’s favored Marxist terminology for describing competition in international politics. In his speech, Xi first advocates for building legislation to defend China against “sanctions, [foreign] interference, and long-arm jurisdiction.” Second, he calls for “prioritizing urgent needs by strengthening law in foreign-related fields”, indicating that China should be prepared to use extraterritorial norms to assert China’s interests abroad.” <https://www.institutmontaigne.org/ressources/pdfs/publications/chinas-extraterritoriality-new-stage-lawfare.pdf>.

¹⁴ Justin Malzac, “A Special Operations Approach to Lawfare,” *Naval War College Review*, (2024). Goldenziel, “Law as a Battlefield.” Smith, “Chinese Lawfare in Conflict.”

¹⁵ Halper et. al., “The Three Warfares.”

¹⁶ For a discussion of Chinese lawfare in the South China Sea, see Justin Nankivell, China’s Use of Lawfare in the South China Sea Dispute, in Halper et. al., “The Three Warfares.”

¹⁷ Malzac, “A Special Operations Approach to Lawfare.”

¹⁸ Smith, “Chinese Lawfare in Conflict: The Threat to U.S. Operations.”

¹⁹ Smith, “Chinese Lawfare in Conflict: The Threat to U.S. Operations.”

²⁰ Smith, “Chinese Lawfare in Conflict: The Threat to U.S. Operations.”

²¹ Smith, “Chinese Lawfare in Conflict: The Threat to U.S. Operations.”

²² Michael J. West & Aurelio Insisa, “Reunifying Taiwan with China through Cross-Strait Lawfare,” *China Quarterly*, vol. 257, (2024): 186-201.

²³ Smith, “Chinese Lawfare in Conflict: The Threat to U.S. Operations.”

²⁴ Smith, “Chinese Lawfare in Conflict: The Threat to U.S. Operations.”

²⁵ Smith, “Chinese Lawfare in Conflict: The Threat to U.S. Operations.”

²⁶ Goldenziel, “Law as a Battlefield;” Malzac, “A Special Operations Approach to Lawfare;” Smith, “Chinese Lawfare in Conflict;” Orde Kittrie, “Lawfare, China, and the Grey Zone,” in *Hybrid Threats and Grey Zone Conflict: The Challenge to Liberal Democracies* (Mitt Regan & Aurel Sari eds., 2024).

²⁷ Goldenziel, “Law as a Battlefield.”

²⁸ U.S. Indo-Pacific Command Counter-Lawfare Center One Pager, available at <https://www.pacom.mil/Portals/55/Documents/Legal/Counter-Lawfare%20One%20Pager.pdf?ver=KlcakpJTSPGp5L5DZH8wIQ%3D%3D> <https://www.pacom.mil/Contact/Directory/10/106-Staff-Judge-Advocate/>; See also, Timothy Boyle, “U.S.

Indo Pacific Command Charts a Course for Countering China's Legal Warfare" (2024) at <https://lieber.westpoint.edu/us-indo-pacific-command-charts-course-countering-chinas-legal-warfare/>. The closest to a whole of government strategy came last year when Section 1284 of the Senate's draft for the Fiscal Year 2025 National Defense Authorization Act (NDAA) included a direction for the U.S. Department of Defense (DoD) to submit a report on "hostile legal operations." Unfortunately, this provision did not make it into the final law.

²⁹ DOD JP 3-05 II-1.

³⁰ DOD JP 1, II-7.

³¹ DOD Field Manual 3-0, I-40.

³² Smith, "Chinese Lawfare in Conflict: The Threat to U.S. Operations."

³³ Inspector General of the Australian Defence Force, Afghanistan Inquiry Report (2020) <https://afghanistaninquiry.defence.gov.au/> (the "Brereton Report"). See also, Matthieu Aikins, How War-Crime Accusations Against Green Berets Were Denied and Buried, New York Times (Sept. 30, 2025) <https://www.nytimes.com/2025/09/30/magazine/green-beret-war-crimes-afghanistan.html>; Douglas Guilfoyle, Alleged UK War Crimes in Afghanistan, Lieber Articles of War (June 21, 2022), <https://lieber.westpoint.edu/alleged-uk-war-crimes-afghanistan/>.

³⁴ "China Demands Justice for Civilians Killed by U.S. Military: FM Spokesperson," *Xinhua* (Dec. 14, 2021), http://www.news.cn/english/2021-12/14/c_1310372391.htm (available via the Wayback Machine at https://web.archive.org/web/20221225133803/http://www.news.cn/english/2021-12/14/c_1310372391.htm) (drawing attention to PRC foreign ministry statements condemning "barbaric military interventions by the United States in Afghanistan, Iraq, Syria and other countries under the banner of 'democracy' and 'human rights,' and [calling] on the international community to investigate the war crimes committed by the U.S. military of killing innocent civilians around the world") [<https://perma.cc/WQ69-7DG8>]; Yu Ning, "How US Evades Responsibility for War Crimes in Afghanistan," *Global Times* (Sept. 27, 2021), <https://www.globaltimes.cn/page/202109/1235240.shtml> [<https://perma.cc/L4MM-QTHB>] (a daily tabloid newspaper under the CPC's official newspaper, the People's Daily (Renmin Ribao), discussing allegations of U.S. and Australian war crimes); Alex Ward, "China and Australia Are in a Nasty Diplomatic Spat over a Fake Tweet — and Real War Crimes," *Vox* (Dec. 2, 2020), <https://www.vox.com/22021226/australia-china-afghanistan-tweet> [<https://perma.cc/FE98-MYNG>] (discussing a diplomatic spat between Australia and China relating to Chinese

propaganda relating to real war crimes committed by Australian special forces).

³⁵ George Bellas, "Deepfakes in the Courtroom: Problems and Solutions," <https://www.isba.org/sections/ai/newsletter/2025/03/deepfakesinthecourtroomproblemsandsolutions> noting that "the ease with which deepfakes can be created poses significant problems for courts in handling video and image evidence. We can no longer assume a recording or video is authentic when it could easily be a deepfake." This concern is perhaps magnified outside of closed courtrooms and on the international legal stage where issues are particularly emotive and controversial images and footage are likely to be widely shared beyond directly involved parties, making authorship and origin of materials especially hard to verify.

³⁶ Crispin Smith, "Chinese Lawfare in Conflict: the Threat to U.S. Operations," *Harvard National Security Journal*, vol. 16, no. 2, (2025): 169-184. disrupting enemy operations by imposing strategic costs – for example by limiting access, basing, and overflight or by forcing elongated supply chains.

³⁷ DOD Field Manual 3-0, I-40.

³⁸ Smith, "Chinese Lawfare in Conflict;" Goldenziel, "Law as a Battlefield;" Malzac, "A Special Operations Approach to Lawfare;" Orde Kittrie, "Lawfare, China, and the Grey Zone," in *Hybrid Threats and Grey Zone Conflict: The Challenge to Liberal Democracies* (Mitt Regan & Aurel Sari eds., 2024).

³⁹ Smith, "Chinese Lawfare in Conflict: The Threat to U.S. Operations."

⁴⁰ Smith, "Chinese Lawfare in Conflict: The Threat to U.S. Operations."

⁴¹ Smith, "Chinese Lawfare in Conflict: The Threat to U.S. Operations."

⁴² DOD JP 3-22.

From Saguntum to Taipei

The Hazards of Strategic Ambiguity

By Robert Boudreau and James L. Johnsen

Strategic ambiguity is not a modern invention, and neither are the risks that attend the practice. More than two millennia ago, the Second Punic War started after Rome remained outwardly ambivalent as to whether it would aid a client state called Saguntum against Carthaginian aggression.¹ Not wanting to antagonize Carthage, Rome failed clearly to state or demonstrate how it would respond to an attack on Saguntum. The Carthaginian leader Hannibal interpreted this irresolution as an invitation to attack. He launched what history would come to call the Second Punic War with an attack on the city, catching the Romans flat-footed. Rome not only lost Saguntum, but it also critically undermined its credibility with numerous other client states throughout the Mediterranean region.

Applying principles of prospect theory to the current U.S. policy of strategic ambiguity towards Taiwan, we demonstrate that the lesson from Saguntum is that *ambiguity invites offense*.² For deterrence to succeed, the adversary must clearly understand which causes will trigger which actions, and the adversary must act (or abstain from acting) out of fear of the response. Ambiguity about the response to an adversary attack introduces risk analysis into its decision. Rather than certainty about a defensive response to aggression, the adversary must consider the possibility that it could attack without a response. In the first instance, the adversary must weigh the risk of losses if it attacks. In the second, the adversary must consider the risk of lost opportunity if it does not attack. If the adversary intuits at all that there is a possibility of attacking without drawing a response, it is more likely to pursue that option.

Strategic ambiguity attempts to maintain the “initiative” with respect to an adversary and preserve options for action. But that flexibility can come at a great cost. For the Romans, the cost was a 17-year war

Robert Boudreau, Lieutenant Colonel, is a student in the U.S. Army War College’s Master of Strategic Studies program and has served in the Marine Corps Reservist as a judge advocate and civil affairs officer in a variety of positions. In his civilian career, he works as an Enforcement Attorney for the U.S. Securities and Exchange Commission in Fort Worth, Texas.

James L. Johnsen, Major, is pursuing a Master of Arts in Defense and Strategic Studies through the U.S. Naval War College and is a U.S. Marine Corps Reserve manpower officer and civil affairs officer assigned to 3d Civil Affairs Group. As a civilian, he is a foreign service officer currently posted as the General Services Officer for the American Embassy in Niamey, Niger. This article represents the personal opinions of its authors and does not reflect any official position of any agency of the United States Government.

that saw the invasion of the Italian peninsula. In the present, it remains to be seen what the price will be for the United States' policy of strategic ambiguity with respect to Taiwan and the People's Republic of China (PRC). With China's posture constantly shifting towards increasingly open aggression against Taiwan, now is the time for the United States to confirm its commitment to Taiwan's security and direct its policy from the realm of ambiguity into a zone of strategic clarity.

AN ANCIENT EXAMPLE

At the close of the First Punic War, Rome and Carthage reached a treaty in 226 B.C. under which Carthage agreed not to advance north of the Iber River in modern day Spain. The agreement contained a latent ambiguity because the Roman client city of Saguntum lay to the south of the Iber. As a result, Carthage could arguably advance and conquer any territory south of the river, including Saguntum, a Roman client state.

Rome attempted to avoid antagonizing its Carthaginian rivals by obscuring its intentions towards Saguntum. This left the Carthaginians guessing as to whether Rome would act to limit Carthage's expansionist aims. Rome's attempt at balancing its relations with Saguntum *vis-à-vis* Carthage ultimately failed, placing Hannibal and the Carthaginians at a significant advantage. Carthage was able to attack Saguntum without Roman intervention. Rome professed loyalty to Saguntum but did not clearly come to the city's aid as Hannibal threatened to attack. In this posture of strategic ambiguity—ostensibly holding to the treaty with Carthage, while also backing Saguntum, and yet being unwilling either to declare a breach with Carthage or to bolster Saguntum's defenses—Rome lost the strategic gamble, and nearly two decades of war ensued.³

Before the attack on Saguntum, the city served as a proxy for the escalating conflict between Rome

and Carthage. Around 221-220 B.C., a dispute broke out between Roman and Punic factions in Saguntum; the Roman faction prevailed, and the Punic leaders were executed.⁴ On the heels of this defeat Rome continued to pressure Carthage and sent ambassadors with a clear message: stay out of Saguntum. But they failed to reinforce that message by making equally clear what the response would be if Hannibal attacked the city anyway. Even while maintaining the narrative that Saguntum was to remain free of Carthaginian control, Rome still did not send its own troops to support the city. Hannibal, unconvinced of Rome's good intentions, saw Saguntum as strategically important both as the base of operations for a future Roman campaign against Carthage, as well as a prize launching point for a Carthaginian assault against Roman aggressors.

At the point of Hannibal's attack in 218 B.C., Carthage could claim both maltreatment at the hands of Rome, its more powerful competitor, as well as a threat to Carthage's security which necessitated immediate action. Rome's failure to clearly warn Carthage of what would happen in response to an attack on Saguntum, combined with the Carthaginians' outrage over the killing of their agents in Saguntum at the hands of Rome's devotees, set the stage for the Carthaginian attack on Saguntum. Carthage's response cut through Rome's fluctuating attitudes towards Saguntum and ultimately left Rome with no choice but to fight anyway from a position of significant disadvantage.

In these circumstances, Carthage was placed in the unenviable position of relying on Rome's good graces for a continued peace or attacking Saguntum and facing devastating losses. Neither presented a good chance of success for Carthage. In a full-scale conflict over control of Saguntum with Rome, a numerically much-superior force, Carthage would likely be crushed; however, attempting to maintain the status quo by not attacking the city also did

not bode well for Carthage, as the rising tensions between the two empires would probably eventually have led to a flare-up in another place. Viewed through the lens of “prospect theory” – where Carthage was faced with probable “loss” outcomes either by launching an attack or maintaining the status quo – Carthage’s risk aversion, corresponding to an increased likelihood of attack, is predicted to be reduced.⁵ And that is ultimately how the scenario played out; Carthage took the initiative and attacked Saguntum, and won.⁶

Rome’s embarrassment at Saguntum resonated throughout the region. After Rome’s failure to defend the city, Rome attempted to unite other Spanish cities against Saguntum. A leader of the Volciani people retorted that they would prefer the friendship of Carthage to Rome, citing specifically the way the Romans had betrayed their purported allies at Saguntum.⁷

TODAY’S GREAT POWER PARALLEL

In current affairs, the United States finds itself in an analogous position with respect to Taiwan as Rome did with Saguntum. The United States supports the “One China” policy and rejects Taiwanese independence.⁸ At the same time, it supports Taiwan’s right to self-govern but without consistently promising to reinforce that right with the use of American military forces.⁹ Four decades into the United States’ pattern of deliberately ambiguous policy decisions regarding Taiwan, this deterrence strategy against Chinese invasion may soon fail unless a hard shift is made to strategic clarity.

While the United States ostensibly still adheres to the One China policy, then-U.S. President Joe Biden stated several times in recent years that the United States will defend Taiwan against a Chinese attack.¹⁰ Taiwan’s small size belies its strategic importance to the United States and the world. Taiwan’s advanced technology sector is a critical

component of defense production, electronics manufacturing and other parts of global industry. It lies in a strategic location along a major international shipping route. Further, Taiwan stands as a beacon of democratic success for the international community; the symbolic nature of its ability to self-govern deserves unwavering support from the free world. For the PRC, on the other hand, Taiwan as an “unsinkable aircraft carrier” is indispensable to the PRC’s vision for the future, as it looks to expand its military presence and hegemonic influence across the Western Pacific.¹¹

The present predicament is not new. Decades before the Carter administration recognized the PRC as the sovereign government of China, President Eisenhower maintained a stance of solidarity with Taiwan, and against the PRC, that rivaled U.S. commitment to its NATO partners against Russia.¹² Times have changed, and the balance of power has shifted substantially in the competition landscape. But American leaders must resist the anachronistic charm of a “that was then, this is now” attitude and instead view Taiwan with the 2,000-year mind that the PRC does.

Taiwan represents far more to the United States and to the free world than just a reliable source of semiconductors. The Cold War between the United States and the Soviet Union was fought to prove that democracy is a powerful force for peace which could win out over communism. Following the fall of the Soviet Union, the U.S. “victory” in the Cold War seemed clear. But Russian leadership under Putin has returned the country to an imperialist mindset, and the ideological war has resumed.¹³ And this mindset is not only in Russia, but in the Far East as well. While the PRC, as the world’s second largest economy, can potentially offer attractive economic opportunities to the developing world and others, engaging with the PRC may also bring unintended consequences such as increased debt, greater vulnerability to economic shocks, and enhanced PRC

influence in domestic affairs. One need look no further than the massive Belt and Road Initiative (BRI) development spending campaign which the PRC has leveraged to gain access to and control over nations on every continent in its quest for global preeminence, despite some mixed success.¹⁴ By contrast, a free and prosperous Taiwan, a key player in global supply chains and sitting in a strategic location, represents a stark contrast against the veiled authoritarianism of the Xi regime. For the United States to restore credibility with its partners in the Pacific and elsewhere, it must clarify its support for Taiwan.

Perhaps because of decades of hot-and-cold U.S. policy towards Taiwan, there is no consensus view among the Taiwanese people that U.S. signals of support improve Taiwanese security. A 2023 Brookings Institution poll indicated that a majority of Taiwanese respondents felt U.S. Speaker of the House Nancy Pelosi's 2022 trip to Taiwan weakened Taiwan's security.¹⁵ According to the study's authors, the data suggested that the Taiwanese people fear "entrapment," i.e. being brought unwillingly into an escalating rivalry between the United States and the PRC, as U.S. actions may trigger more aggressive responses from the PRC.

THE THEORY OF DETERRENCE

Military deterrence, a high-stakes international game of chicken, presents a state with two options: first, "to support the status quo through cooperation;" and second, "to overrun the status quo through military action."¹⁶ For nuclear powers, the spectrum of possible actions is endlessly nuanced between strategically ignoring aggressor actions and preparing to use the nuclear codes.

Convincing an adversary that the United States will use its military power to defend a third-party state, an act of policy rather than immediate survival, is much more challenging. The key to success is credibility.¹⁷ But engaging in "dual-deterrence" — that is, taking a position of trying to deter

two other states from acting against each other by maintaining an ambiguous stance as to how the one state engaging in deterrence will respond to each other state's actions, infinitely compounds those challenges. A policy of strategic ambiguity straddles two positions simultaneously — one which seeks to deter states from taking action against the other, and the second which remains deliberately vague as to actual commitments or intentions.¹⁸ Thus, ambiguity in deterrence introduces key complications to policymaking and implementation. First, the actor engaging in deterrence may not clearly identify "red lines" or particular aggressor actions which the actor "has defined as a *causus belli*," an act of war to which it will react.¹⁹ Second, the actor engaging in deterrence may avoid clarity as to what its response will be if any red lines were to be crossed.²⁰

THE AMBIGUOUS ONE CHINA POLICY HAS REACHED ITS EXPIRATION DATE

When the United States first embraced the One China policy during the Carter years, the PRC wielded a fraction of the global influence that it exercises today.²¹ At the time, the policy aimed to deter PRC communist expansion over a democratic Taiwanese population, and given that Taiwan still flies an independent flag, the policy has arguably been fairly effective. However, the symbolic line-in-the-sand that Taiwanese democratic self-governance once represented to the PRC is now just one roadblock in the path of Beijing's expansionist goals. Through maritime operations in the East and South China Seas, BRI investments on every continent, and an international charm offensive, the PRC has been able to achieve a nearly unmatched sway over other nations and accomplish many of its national aims without firing a shot.²²

Today's international posture is much changed from the China-Taiwan dispute of the 1970s, as the potential for reunification with Taiwan offers more

than just an opportunity for the PRC to bring the Chinese people under a single political system. If China can execute a swift combined-arms invasion and seize control of Taiwan, it would send a powerful message to the world that China's military has fully modernized and is able to compete with any opponent. Taiwan's proximity to the Chinese mainland allows for this "experiment" to be carried out in China's backyard, and depending on any potential U.S. response, at a lower risk than, for example, attempting to seize control of disputed features of the Philippine archipelago.

The stakes are substantially different for the United States if it is to continue asserting positive influence around the world because Taiwan is perhaps just one steppingstone for the Chinese along a path to much broader control of the Pacific. Meanwhile, the United States' support for other countries has arguably been expressed in incongruous policy positions, with support for the Ukraine, Israel, and the Afghanistan governments evolving with the Trump Presidency.²³ If the United States is to maintain credibility with Taiwan and key allies and partners regarding its 45-year position that the Taiwanese people have a right to govern themselves democratically, then it is time to solidify its position.

PERCEPTIONS SHAPE DECISIONS

Prospect theory, a classic model of decision-making which argues that cognitive factors must be considered beyond the mechanical cost-benefit analysis of classic rationality, posits that states are generally risk averse and will be less likely to seek a change in the status quo where the outcomes are perceived to be gains rather than losses.²⁴ For an actor seeking to deter another party from particular actions, then the actor undertaking deterrence will be more likely to succeed where it shapes the other party's perceptions to frame a change in the status quo as a gamble between expected gains, rather than expected losses.

In the case of Taiwan and the PRC, according to prospect theory, each party will be less likely to make a strategic move – Taiwan towards independence and the PRC towards invasion – if either party perceives that its move is from one beneficial position to another (i.e., "this might make us better off") versus escaping further losses (i.e., "we don't have much left to lose"). From the U.S. perspective, the worst outcome would be where both Taiwan and the PRC perceive that they are each already facing strategic losses, and that they can potentially cut those losses by breaking from the status quo. For Taiwan and PRC to frame potential consequences in the right light, the United States must be seen as credible both in terms of (i) whether and under what circumstances it will intervene, and (ii) whether its intervention will be effective.

As Beijing considers its options, with the benefit of 40-plus years' hindsight as to how the United States' ambiguous One China policy has been implemented, it is likely to hold a risk-averse position. If the PRC breaks the status quo and attacks Taiwan, it has a significant chance of success, though perhaps at a very high cost. Using the recent Russia-Ukraine war as a model for how a potential PRC seizure of Taiwan might play out, it would be nearly impossible for the United States to respond quickly with kinetic force, and U.S. support would most likely be relegated to providing arms for a prolonged guerilla fight; in short, this places a PRC attack into a "gains" frame with a corresponding increased willingness to accept the risk. On the other hand, China has experienced transformative growth which has brought it to the front of the world stage in the 21st Century, and there is no indication that the trend is slowing. However, if the PRC were to attack Taiwan, it could expect to face immediate sanctions and other consequences from much of the developed world, which could substantially curtail its growth trajectory and international respect it has built through a strong export economy and the BRI. Accordingly,

maintaining the status quo would also be viewed as a “gains” prospect for the PRC, and thus, according to this theory, Beijing should hold a risk-averse stance regarding this choice. Overall, Beijing would hold a risk-averse position to attacking Taiwan and breaking the status quo, and so a shift by the United States from strategic ambiguity to clarity could have an enhanced deterrent effect.

On the other hand, it may be countered that if the United States moves from a position of strategic ambiguity to one of greater clarity regarding Taiwan, the move could increase the PRC’s dissatisfaction with the status quo and incentivize Beijing to speed-up its reunification plans. But the PRC is not the only actor here. Polling data from 2024 indicated that the vast majority of the Taiwanese people are not looking for an imminent declaration of independence.²⁵ With strengthened support from the United States, Taiwan’s calculation of the gains to be had by breaking from the status quo and declaring independence should be reduced, and correspondingly, the potential costs of keeping with the current independent governance structure should be reduced. If the PRC takes the Taiwanese response to a favorable U.S. policy position into account, that should offset, or at least mitigate, the PRC’s dissatisfaction with the status quo.

CREDIBILITY MATTERS

Political and military leaders often succumb to the temptation to keep the broadest menu of options open to retain the initiative under a variety of circumstances. They seek to sacrifice definiteness for perceived flexibility. While retaining the initiative can be helpful if it buys time for new ideas, it will result in failure if it merely masks indecision. In the latter case, preserving the initiative undermines credibility and makes deterrence impossible.²⁶ To convince the adversary that the deterring power has red line conditions under which it will act, the deterring power must persuasively and clearly

communicate which adversary actions will draw which potential responses. This is the foundation of effective, credible deterrence. The deterring power cannot simply communicate its intention—it must make the adversary believe in the actions that will back up that intention.²⁷

The most credible threat often comes after having purposefully and obviously demolished any off-ramps. The adversary cannot suspect the deterring power will retreat from an attack if it has no avenue for retreat. Indeed, by sacrificing the initiative, the deterring power places the onus of decision on the adversary. In modern international politics, where aggression is almost universally reviled, a power seeking to deter another can gain an advantage by placing the final decision to attack or refrain from attacking on the adversary. By forcing an adversary to take that final politically unseemly step, the deterring power can maintain its own international prestige and take advantage of the inherent strengths of a thorough, intentionally planned defense.

Furthermore, in the absence of explicitly stated red lines, the United States may project power, using its physical presence within a potential conflict zone, as a proxy for clearly articulated red lines. Specifically, by sending U.S. troops to partner with Taiwanese forces, for example through training missions, the United States strongly signals to the PRC that an attack on Taiwan will, in effect, also be an attack on the United States. If public reporting is correct, U.S. Army specialists may already be training on a rotational basis with Taiwanese soldiers in the region of the Taiwan Strait.²⁸ The United States may also bolster its support of Taiwan by openly engaging with the Taiwan military in additional ways, such as through periodic exercises during which it may invite other partners’ participation.²⁹

Turning next to whether the United States can effectively support the Taiwanese in defending against a PRC invasion, a recent study by the

Center for Strategic International Studies (CSIS) suggests that the United States and its allies would succeed, though at a very high cost.³⁰ Nevertheless, the United States has not been shy about describing China as its primary “pacing challenge” in defense preparation.³¹ If the United States is to be taken seriously as a military partner for Taiwan, then policymakers should be consistent both in word and deed to prepare for a large-scale conflict in support of Taiwan’s democratic freedom.

HISTORICALLY, STRATEGIC CLARITY CONTRIBUTED TO COLD WAR SUCCESS

The United States often found it useful and even necessary to make its strategic stance clear to the Soviet Union during the Cold War. The U.S.-led alliance’s posturing and maneuvering during the Berlin Airlift offers an example where strategic clarity led to a positive outcome.³² In the Soviet sector of Germany after the Second World War, Stalin’s regime set out to destroy the social roots of fascism by “bolshevizing” the East German people and economy.³³ Stalin recognized that the American-British-French force in West Berlin represented a threat to this effort and decided in March 1948 to establish a ground blockade of the exclave with the end in mind of forcing Western powers out of the city.³⁴

While Allied policy leading up to the blockade was not a model of cohesion and definiteness, the success of the initial airlift effort led them to rally around supporting West Berlin as a check against further Soviet expansion in Central Europe.³⁵ The first overt signal sent was the deployment of some 60 B-29 bombers to bases within striking distance of the Soviet Union.³⁶ At the same time, American and Allied leaders overruled the local commander’s desire to break the blockade by launching an armored convoy through Soviet-occupied East Germany.³⁷ This tempered signaling supported

public comments from U.S. Secretary of State George C. Marshall confirming that the Western powers would not be coerced into abandoning West Berlin.³⁸ The United States ultimately committed an enormous portion of its airlift capacity to provide relief supplies to West Berlin between June 1948 and May 1949. This commitment of significant kinetic and non-kinetic military resources, which substantiated the United States’ public comments committing to the defense of West Berlin, ultimately broke the Soviet willingness to subsume the Western-occupied sectors of the city into the larger East German zone.³⁹ The Soviets thought they could remove the Westerners cheaply but demurred when presented with clear messaging supported by tangible action.

Several parallels exist between the Berlin Airlift and the present-day China/Taiwan rift. First, the dispute is fundamentally rooted in ideological differences between the PRC’s communist regime and Taiwan’s democratic government. Second, China’s threat of using armed force to achieve reunification with Taiwan, whose military will be unable to match the PRC’s forces head-on, is similar to the Soviet Union’s threat of invading West Berlin and eliminating the separate administrative regions. Third, the United States is again at odds with a powerful peer competitor, which has inevitably led at various times to saber-rattling and suggestions that all options are on the table. But, as the Cold War example shows, the United States’ and its western allies’ consistent strategic posture led to a positive result ultimately dissuading the Soviet Union from escalating the conflict into a shooting war.

PROLONGED U.S. AMBIGUITY INVITES OFFENSE

The United States, by keeping its intentions with respect to both the PRC and to Taiwan ambiguous, hopes to avoid goading the PRC into attacking the island while also communicating some level of non-specific support for its democratic partner.⁴⁰ In

support of this approach, some may argue that the United States' non-specific commitment towards Taiwan creates incentives for Taiwan to invest in its own defense capabilities. This in turn frees-up resources for the United States to focus in other areas of international competition. But without a reliable support commitment, Taiwan is left to speculate as to how a change in the status quo – for example, by declaring independence – will impact its future prospects.⁴¹

For decades, the PRC has periodically made threatening overtures, and therefore, it is easy for Taiwan to assume that the current environment is inevitably leading to conflict. Applying prospect theory's principles to Taiwan's predicament, it is foreseeable that Taiwan would frame its options in terms of *losses*, i.e. that the PRC will invade at some point, and it cannot do any worse by making a break for independence on its own. Accordingly, the United States' ambiguity invites Taiwan to take action to bridge the gap between rhetoric and readiness. More specifically, the lack of U.S. clarity towards Taiwan, instead of fostering indecisiveness, may actually be signaling to Taiwan that it is better to prepare on its own against an invasion than to wait on any potential U.S. support at some future moment of need. Complicating this point, U.S. policy towards Beijing continues to embrace a spectrum of vital issues beyond Taiwan, from the PRC's dealings with Iran, North Korea, and Russia to halting the proliferation of fentanyl throughout local communities.⁴² In addition, the United States views China as its military capability pacing threat, and is thus preoccupied with developing hypersonic missiles, improving space defense and conventional naval and aeronautical assets, and preventing international hacking.⁴³ From Taiwan's perspective, given the breadth of U.S. interests with regard to China beyond its status, any actions – whatever they may be – undertaken by Taiwan to change the status quo

and improve its defense may in turn trigger military responses by the PRC.

Similarly, the United States' policy of strategic ambiguity invites China to take offense at a vast array of U.S. or Taiwanese actions.⁴⁴ As China's economy grows and it continues to expand its military capabilities, it is a bit Pollyannaish to view the PRC as satisfied with its current position on the international stage.⁴⁵ As long as the United States remains ambiguous as to how it will translate the One China policy into practice, the PRC likewise may easily frame its options to disrupt the status quo in terms of losses, rather than gains, leading to an increased likelihood that it will choose aggression. But the United States' current approach ignores the Romans' lesson. Like Hannibal at the doorstep of Saguntum, the PRC can use any number of pretexts for invading Taiwan. While the United States tries to keep China guessing as to its intentions regarding Taiwan's defense, only future hindsight will show whether this was clever policy or too clever by half.

Some question whether a U.S. move away from ambiguity and towards clarity will have any meaningful deterrent effect against PRC aggression. According to U.S. Senator Chris Murphy, the PRC has already “priced-in” the cost of anticipated U.S. intervention into its operational plans; accordingly, under this view, “strategic ambiguity is largely irrelevant to whether [the PRC] decides to attack Taiwan.”⁴⁶ However, this perspective seems to pay short shrift to the spectrum of options available to the United States, and instead stifles policymakers from finding creative deterrence solutions. Assuming it is true that the PRC has priced in *some* cost of a U.S. response, an effective deterrence strategy should seek to maximize the price that the PRC will pay for actions leading up to and including an attack on Taiwan.

ESTABLISH DEFENSIBLE RED LINES

As discussed above, the problem of ambiguity is twofold — not only does it fail to articulate what actions will trigger a response, but it also fails to provide notice as to what the likely response will be. Learning from the experiences of two World Wars, the Cold War, and the Global War on Terrorism, the United States is no stranger to fostering alliances and building military coalitions throughout the world with the aim of deterring various threats and improving international stability.

Above all, any action by the PRC to degrade the Taiwanese military should trigger U.S. intervention, at least in the form of providing arms. PRC military incursion should lead to additional support across operational domains. But short of these more drastic military actions by the PRC, the ongoing cycle of aggressive military drills in and around Taiwan should lead the United States to demonstrate that it supports a prepared Taiwanese military, ready to engage a PRC invasion head-on, and to wage a protracted insurgency, should initial resistance fail.

As a sign of its commitment, and as it has done in many other instances, the United States could openly send its troops to Taiwan, perhaps on a periodic schedule for bilateral training activities. Placing U.S. troops alongside Taiwanese forces would resemble the United States' very effective partnerships with any other number of countries—from the Air Force base on Okinawa to the Army garrison in Bavaria to Marine Corps deployments to Australia. And in these latter examples, U.S. commitments can hardly be called ambiguous. Indeed, the United States' presence in those countries makes clear and credible the U.S. intention to deter aggression against these countries. Implicit with embedding troops with a partner nation's forces is the notion that an attack on one is an attack on all, thereby creating a *de facto* red line that any form

of attack will trigger some response. Short of open declarations of its intentions, the United States can, through repetition of exercises with the Taiwanese for example, communicate what it is preparing for. That is, what the United States' likely response will be to an attack. Thus, a simple commitment of a modest number of troops, in conjunction with inviting Taiwan into the United States' Pacific exercise cycle, could provide an outsized strategic impact. An added benefit would be to demonstrate to Taiwan that the United States is committed to a long-term defense relationship and reduce the likelihood that Taiwan will feel the need to follow a path on its own.

CONCLUSION

What, then, is to be done? Thankfully, the United States' posture with Taiwan has significant differences from Rome's with Saguntum. The United States is not recovering from a traumatic war with our Great Power rival. If anything, the United States and China enjoyed a significant rapprochement late in the 20th Century, and perhaps those days are not beyond the point of no return. Also, unlike the Romans in Spain, the United States is not looking to expand its territorial reach into East Asia.

Notwithstanding these favorable distinctions, the lesson for American policymakers is simple and should be accepted—strategic ambiguity invites offensive, adversarial actions. If the United States will fight for Taiwan, it should say so without equivocation and then act to make those statements credible. By doing so, the United States can burden China with the onus of a difficult decision. If China acts, it should do so knowing exactly what consequences it will elicit with that action.

Continued ambiguity invites the PRC to escalate its current “salami-slicing” incremental-encroachment approach to Taiwan into more direct acts of aggression. For Taiwan, the United States' failure to express clear commitment may at some point color Taiwan's willingness to rely on

U.S. support. As Congressman Mike Gallagher has repeatedly stressed, “strategic clarity is necessary but not sufficient;” the United States “must follow it up with the decisive action that will be required to deter a Chinese Communist Party invasion of Taiwan within the next five [(now, two)] years.”¹⁷ Before the window of opportunity is closed, the United States’ watchword must be consistent, committed clarity. **PRISM**

Notes

- ¹ Donald Kagan, *On the Origins of War and the Preservation of Peace* (New York: First Anchor Books, 1996), 232–280.
- ² Berejikian, Jeffrey D. and John S. Dryzek, “Reflexive Action in International Politics,” p. 198 and following. *British Journal of Political Science*, Vol 30: No. 2 (Cambridge University Press, Apr. 2000), 193-216.
- ³ Kagan, *On the Origins of War*, 256-274.
- ⁴ Kagan, *On the Origins of War*, 262.
- ⁵ Jeffrey D. Berejikian, “A Cognitive Theory of Deterrence,” p. 168. *Journal of Peace Research*, Vol. 39: No. 2 (Sage Publications, Mar. 2002), 171-72.
- ⁶ Kagan, *On the Origins of War*, 266-267.
- ⁷ Aubrey de Sélincourt, trans., *The War with Hannibal* (London: Penguin Books, 1965), 43, cited in Schelling, 66n15.
- ⁸ Boon, Hoo Tiang and Hannah Elyse Sworn, “Strategic Ambiguity and the Trumpian Approach to China-Taiwan Relations,” 1487. *International Affairs* 96: No. 6 (Oxford University Press, June 2020).
- ⁹ Ibid.
- ¹⁰ David Cohen, “Biden hasn’t changed U.S. policy on Taiwan, Jake Sullivan says.” Politico (Apr. 4, 2023).
- ¹¹ Boon and Sworn, 1497.
- ¹² McKinney, Jared M. and Peter Harris, Report: “Deterring China: 1949 to Present,” 14-15 (Strategic Studies Institute, U.S. Army War College (2024)).
- ¹³ Norman M. Naimark, “Putin in Stalin’s Mirror.” *Defining Ideas* (Hoover Institution, May 1, 2023).
- ¹⁴ Michael Mazarr, “U.S.-China Relations in the Tank—A Handbook for an Era of Persistent Confrontation,” pp. 5-6 (Center for Strategic and International Studies (CSIS) (2022)). But see also discussions of BRI project failures by Elaine Dezenski and Josh Birenbaum, Research Memo: “Tightening the Belt or End of the Road? China’s BRI at 10” (Foundation for Defense of Democracies, February 27, 2024); and by Nadia Clark, “The Rise and Fall of the BRI,” *Asia Unbound* blog (Council on Foreign Relations April 6, 2023).
- ¹⁵ Alastair Iain Johnston, Tsai Chia-hung, and George Yin, “Commentary: When might US political support be unwelcome in Taiwan?” The Brookings Institution (April 5, 2023).
- ¹⁶ Berejikian, 165-183.
- ¹⁷ Thomas C. Schelling, *Arms and Influence*, pp. 35-36 (Yale University Press, 2020).
- ¹⁸ Boon, 1489.
- ¹⁹ Van Jackson, “Tactics of Strategic Competition,” *Naval War College Review*, Vol 70: No. 3, Article 4 (U.S. Naval War College Digital Commons, 2017), 3.
- ²⁰ Van Jackson, “Tactics of Strategic Competition,” p. 3. *Naval War College Review*, Vol 70: No. 3, Article 4 (U.S. Naval War College Digital Commons, 2017), 4.
- ²¹ Richard C. Bush, “A One China Policy Primer.” Brookings Center for East Asia Studies (March 2017).
- ²² Kerry K. Gershaneck, “To Win without Fighting – Defining China’s Political Warfare,” 14-15. Marine Corps University Press (April 2024).
- ²³ Jeffrey C. Higgins, “Strategic Clarity: An Argument for Effective Deterrence,” pp. 5-7. *Security Nexus* (Daniel K. Inouye Asia-Pacific Center for Security Studies 2023).
- Aluf Benn, “America and Israel Follow the Same Old Script,” *Foreign Affairs* (June 5, 2025).
- ²⁴ Jeffrey D. Berejikian, “A Cognitive Theory of Deterrence,” p. 168. *Journal of Peace Research*, Vol. 39: No. 2 (Sage Publications, Mar. 2002), 171-72.
- ²⁵ Lorenzo Lamperti, “Taiwan’s National and Political Identities Put To the Test by the Vote.” Italian Institute for International Political Studies, Commentary (January 11, 2024).
- ²⁶ Schelling, 44.
- ²⁷ “Peter George, Dr. Strangelove or How I Learned to Stop Worrying and Love the Bomb (London: Prion, 1999).
- ²⁸ John Feng, “US Army Special Forces Train Taiwan Troops Near China’s Coast.” *Newsweek* (February 8, 2024).
- ²⁹ Jerry Doyle and Subhranshu Sahu, Editors, “Exclusive: U.S. and Taiwan navies quietly held Pacific drills in April.” *Reuters*, (May 14, 2024).

³⁰ Mark F. Cancian, Matthew Cancian and Eric Heginbotham, “The First Battle of the Next War.” A Report of the Center for Strategic and International Studies (CSIS Jan. 2023).

³¹ Mike Pompeo and Bryan Clark, “A new strategic concept could be useful in the US military’s defense of Taiwan.” *The Hill*, Opinion (April 2, 2024).

³² Harrington, D. F., *Berlin on the Brink: The Blockade, the Airlift, and the Early Cold War*, pp. 27–46 (University Press of Kentucky, 2012).

³³ Harrington, D. F., *Berlin on the Brink: The Blockade, the Airlift, and the Early Cold War*, pp. 27–46 (University Press of Kentucky, 2012).

³⁴ Harrington, D. F., *Berlin on the Brink: The Blockade, the Airlift, and the Early Cold War*, pp. 27–46 (University Press of Kentucky, 2012), 44.

³⁵ Harrington, D. F., *Berlin on the Brink: The Blockade, the Airlift, and the Early Cold War*, pp. 27–46 (University Press of Kentucky, 2012), 30–44.

³⁶ Harrington, D. F., *Berlin on the Brink: The Blockade, the Airlift, and the Early Cold War*, pp. 27–46 (University Press of Kentucky, 2012), 119–22.

³⁷ Harrington, D. F., *Berlin on the Brink: The Blockade, the Airlift, and the Early Cold War*, 27–46 (University Press of Kentucky, 2012), 128.

³⁸ Harrington, D. F., *Berlin on the Brink: The Blockade, the Airlift, and the Early Cold War*, 27–46 (University Press of Kentucky, 2012), 134.

³⁹ Miranda Priebe, et al. Research Report: Anticipating Allies’ Responses to U.S. Retrenchment, 30–32 (Santa Monica: Rand Corporation, 2025).

⁴⁰ Raymond Kuo, “‘Strategic Ambiguity’ Has the U.S. and Taiwan Trapped.” *Foreign Policy* (January 18, 2023).

⁴¹ Jeffrey C. Higgins, “Strategic Clarity: An Argument for Effective Deterrence,” *Security Nexus* 24, no. 1 (2023): 12.

⁴² David Pierson and Olivia Wang, “China and the U.S. are Talking, but their Détente Has Limits.” *The New York Times* (February 2, 2024).

⁴³ See generally U.S. House Committee on Oversight and Accountability report, *CCP Political Warfare: Federal Agencies Urgently Need a Government-Wide Strategy* (October 24, 2024).

⁴⁴ China reacted aggressively to U.S. Speaker Pelosi’s 2022 visit to Taiwan, for example by engaging in its largest-ever military exercises in the region. Robert Plummer, “Taiwan braces as China drills follow Pelosi visit.” *BBC News* (August 4, 2022).

⁴⁵ Steven Tsang, “What Xi Jinping Really Thinks.” *Time* Ideas section (May 11, 2024).

⁴⁶ Kuo, “‘Strategic Ambiguity.’”

⁴⁷ Wisconsin Representative Mike Gallagher, May 23, 2022. *Strategic Clarity on Taiwan is Necessary but not Sufficient* [Press Release].

Mapping the BRICS Plus Cryptocurrency Ecosystem

Is the BRICS Plus Bloc Effectively Using Cryptocurrency to Avoid Sanctions?

By Kathleen Cassedy, Anne Walton, and Ian Conway

This paper examines the question: What is the current state of the use and viability of cryptocurrency within BRICS Plus members as an effective tool for bypassing G7-aligned control of financial systems and thereby sanctions? The focus is on how BRICS Plus members employ indirect financial methods, rather than overt funding lines, to advance collective strategic objectives. It evaluates U.S. economic sanctions on relevant states and designated persons listed by the Office of Foreign Assets Control (OFAC) on the Specially Designated Nationals and Blocked Persons (SDN) list.¹ Findings aim to support irregular warfare (IW) practitioners, especially those engaged in counter-threat finance (CTF) and counter-threat networks (CTN). The study provides contextual understanding of how cryptocurrency facilitates state-level strategic aims and enables individuals and organizations to evade sanctions and designations.

The study employs a case study of observable cryptocurrency transactions between Russian entities and entities based in the United Arab Emirates (UAE), two members of BRICS Plus whose relationship illustrates emerging financial dynamics. By mapping these transactions through blockchain forensics and commercial analytic tools, the research assesses whether cryptocurrency use within BRICS Plus

Kat Cassedy is an IWC Researcher, a commercial analyst, and a national security expert with more than 20 years of experience across the public, academic, and private sectors. She is recognized for her deep expertise in open-source intelligence (OSINT), political and economic warfare, and threat analysis at strategic, operational, and tactical levels.

Anne Walton is an IWC Researcher with over 12 years of experience in anti-money laundering, intelligence, and risk analysis. Her investigative experience includes supporting multi-year independent monitorships and analyzing complex money flows involving wire transfers and cryptocurrency. Ms. Walton has produced intelligence reports for the U.S. government and provided analytical support to law enforcement on criminal money laundering investigations.

Ian Conway is an IWC Researcher with nearly 30 years of analytical, investigative, and programmatic experience in national security analysis, private intelligence, and commercial investigations. He is currently focused on developing methods and technology to expose adversary clandestine commercial infrastructure that facilitates political warfare and gray zone activities.

meaningfully enables sanctions circumvention and the development of settlement systems outside the Society for Worldwide Interbank Financial Telecommunications (SWIFT).²

For this article, IW follows the definition in U.S. Department of War (DOW) *Joint Publication 1*: “a form of warfare where states and non-state actors’ campaign to assure or coerce states or other groups through indirect, non-attributable, or asymmetric activities.”³ Cryptocurrency can facilitate such activities by masking resource mobilization and obscuring attribution. Irregular warfare operations typically unfold within the broader context of Great Power Competition (GPC), where the environment contains a dense mix of actors—development organizations, extractive industries, private security companies (PSCs), private military companies (PMCs), and religious missions. The ruble-backed stablecoin A7A5, launched in late 2024 by a firm jointly connected to a sanctioned Russian bank and a designated Moldovan-Russian national, exemplifies this mix of actors in the cryptocurrency context.⁴ In its first seven months of operation, A7A5 recorded over \$40 billion in transactions, the vast majority of which occurred outside U.S. financial oversight.⁵ An entire financial settlement ecosystem independent of the U.S. dollar—and thus immune to sanctions actions—further complicates efforts to correlate these actors to their benefactors, obscuring state proxies and malign networks.

The paper examines three core questions:

- Are BRICS Plus members engaged in sanctions-evasion behavior using cryptocurrency?
- If so, can commercial chain-analysis tools and equity-chain mapping methods reliably detect this behavior? If not, could cryptocurrency nevertheless serve as a sanctions-avoidance mechanism for BRICS Plus?
- Does this behavior reflect individual state actions, or can researchers identify coordinated bloc-level activity?

Russia, the world’s most-sanctioned state in 2022–2024, and the UAE form the central case, offering a representative view of BRICS Plus dynamics.⁶

BRICS AND BRICS PLUS

Brazil, Russia, India, and China formed BRIC in 2009 in response to the 2008 global financial crisis.⁷ South Africa joined in 2011, creating BRICS.⁸ For more than a decade, the group maintained a stable membership, meeting regularly to discuss development, alternative financial systems, and reduced reliance on the U.S. dollar. In 2024, Iran, Egypt, Ethiopia, and the UAE acceded, followed by Indonesia in 2025.⁹ Today, the bloc refers to itself as BRICS Plus, acknowledging its expanded membership.¹⁰

BRICS Plus members, like most global financial actors, remain dependent on SWIFT to settle international payments. SWIFT’s dominance renders sanctions that restrict network access particularly costly.¹¹ Building a viable alternative multilateral economic system—especially one capable of settling cross-border trade without the U.S. dollar—has become a core BRICS Plus objective.¹² Efforts include exploring BRICS Pay (discussed below), experimenting with cryptocurrencies, and operationalizing the New Development Bank (NDB) as a development-finance counterpart to the World Bank, without Western political conditionality.

These developments intersect directly with the research focus on cryptocurrency’s role in sanctions evasion and alternative financial architectures.

WHY THE UAE?

To select an appropriate case-pair for Russia, we identified a BRICS Plus state with:

- a prominent crypto ecosystem,
- government support for digital-asset innovation, and

- significant transactional inflows from BRICS members.

The UAE meets all criteria. It has positioned itself as a global center for blockchain, Web3, and artificial intelligence development.¹³ Dubai launched its Blockchain Strategy in 2018, created the Virtual Assets Regulatory Authority (VARA) in 2022, and established the Dubai Multi-Commodities Centre (DMCC) Crypto Centre, now home to more than 25,000 companies and multiple accelerator programs.¹⁴

CRYPTOCURRENCY

Cryptocurrency is a form of digital or virtual currency that employs encryption and other cryptographic techniques (e.g., digital signatures, hash functions, and proof-of-work algorithms) to ensure the security and integrity of transactions. Cryptocurrency relies on the *blockchain* as a digital ledger that immutably and securely records all transactions.¹⁵ Users manage their cryptocurrency holdings in digital wallets, utilizing public and private encryption keys for the transfer and receipt of funds. Certain cryptocurrencies are generated via *mining* (solving advanced mathematical problems to create the currency), while others are acquired through *staking* (locking coins to support network operations).¹⁶

A defining feature of blockchain systems is *immutability*, the principle that recorded data cannot be altered retroactively without altering all subsequent blocks and gaining majority control of the network. Each block contains a unique cryptographic hash of the previous block, so changing even a single transaction would invalidate the entire chain. This immutability creates a permanent audit trail that is beneficial for ensuring trust and accountability.

Key features of cryptocurrencies include decentralization, security, transparency, and globalized

nature. *Decentralization* refers to the fact that most blockchains function on distributed computer networks (nodes), which enable resistance to censorship and central control. Cryptocurrencies offer security because the blockchains on which they conduct transactions are protected through robust cryptographic algorithms, rendering them extremely difficult to alter or counterfeit. Transparency is achieved because all transactions are recorded on a public ledger (the blockchain), accessible to anyone for verification and review.

Although blockchain ledgers are transparent, alphanumeric addresses serve to both depict ownership and provide pseudonymity to transactions. Thus, cryptocurrency transactions are *pseudonymous*, not fully anonymous. Each participant is represented by a 26-character alphanumeric address rather than a personal identity. While all transactions are publicly visible on the blockchain, they are not directly linked to named individuals or entities in the absence of supplemental information. Lastly, cryptocurrencies may be transmitted and received globally, often with lower fees and more rapid processing compared to traditional banking systems. These benefits allow certain types of cryptocurrencies to function as a form of international remittance. Such transactions are performed on a peer-to-peer basis, without a centralized intermediary, e.g., traditional banking systems.

Cryptocurrency is increasingly used in criminal activities. Its speed and pseudonymous nature make it an attractive vehicle to enable illicit transactions such as money laundering, ransomware payments, and dark web trade. While blockchain records are public, criminals often use obfuscation tools like mixers and privacy coins to conceal their tracks from investigators.¹⁷

INTEGRATIVE LITERATURE REVIEW

For this paper, an integrative approach to reviewing the literature was used. The common foundation—and the connective tissue tying this project to IW—lies in Farrell and Newman’s work on *weaponized interdependence*, particularly as it relates to global economic networks.¹⁸ Farrell and Newman explore a case study of SWIFT as an example of what they term *chokepoints*:

*The weaponization of SWIFT... demonstrates how globalized networks can indeed be used to exercise “power over,” both by gathering enormous amounts of data that can then be employed for security purposes and by systematically excluding states from participation in the world financial system. Exactly because the SWIFT organization was a crucial hub in global economic exchange, it allowed those states that had jurisdictional sway over it to employ the panopticon and chokepoint effects.*¹⁹

Building on that foundation and extrapolating the weaponized interdependence concept from counterterrorism to the GPC environment, this review was organized around three specific elements of the global economy: 1) sanctions, designations, and cryptocurrency; 2) BRICS Plus financial approaches (NDB and BRICS Pay); and 3) the UAE as a strategic nexus. By weaving these three elements together with Farrell and Newman’s *weaponized interdependence* and *chokepoints*, a foundational context for this paper was established. Further, this foundation provides clear linkages to the practice of IW and provides greater generalizability for the selected pairing in the case study. This section concludes with the identification of intersections and gaps in the literature across the three elements above and closes with observations affirming the utility of this study.

SANCTIONS, DESIGNATIONS, AND CRYPTOCURRENCY

Scholarly work increasingly explores cryptocurrency as a mechanism for sanctions and SDN evasion. Ahari et al. analyze Russian attempts to obscure assets through crypto exchanges after the 2022 invasion of Ukraine, concluding that while individuals can successfully evade detection, large-scale systemic evasion remains constrained by volatility and compliance controls.²⁰ O’Neill and Wick argue that enforcement lags behind technological innovation, leaving crypto infrastructures vulnerable to misuse.²¹

Ungboriboonpisal documents North Korea’s pioneering adoption of cryptocurrency in state-level evasion through mining, ransomware, and exchange hacks.²² Wronka assesses how regulatory gaps enable major powers, notably China and Russia, to incorporate digital currencies into sanctions-resistant strategies, linking this trend to Beijing’s ambition to steer developing nations—including BRICS members—into yuan-linked financial ecosystems.²³ Across these studies, crypto’s utility in sanctions evasion is well established, but most research focuses on single states rather than multilateral blocs.

BRICS PLUS FINANCIAL APPROACHES (NDB AND BRICS PAY)

Parallel literature assesses the bloc’s attempts to reduce dollar reliance. The NDB offers development financing without Western policy conditions. Emerging signals—such as Ethiopia’s reconsideration of crypto bans and exploration of a national Bitcoin reserve—suggest some BRICS members may integrate digital assets into national economic strategies.²⁴ Whether the NDB will incorporate cryptocurrencies remains uncertain.

BRICS Pay exemplifies aspirational bloc-level financial sovereignty. Analysts differ on feasibility:

some see transformative potential while others note persistent operational delays. Helmy frames BRICS Pay as a precursor to a supranational digital currency tied to central bank digital currencies (CBDCs).²⁵ Otorbaev emphasizes its value as a sanctions-resistant settlement mechanism.²⁶ Much of the literature, however, originates from Russian and Chinese sources, where academic writing often blends analysis with strategic messaging.

THE UAE AS A STRATEGIC NEXUS

The UAE occupies a pivotal position in crypto-enabled networks associated with BRICS Plus. VARA and DMCC have made Dubai a magnet for digital-asset ventures. Cooper and Cannon argue that Emirati officials view BRICS and the NDB as platforms for expanding geopolitical influence.²⁷ Russia's support for Emirati accession to the NDB—and subsequently to BRICS Plus—reflects this alignment, particularly given the UAE's pattern of declining to enforce Western sanctions.

U.S. government assessments indicate that sanctioned Russian and Iranian actors have transacted through exchanges with UAE footprints.²⁸ Congressional correspondence also highlights stablecoins, especially Tether, as possible vectors for Russian sanctions evasion with the UAE functioning as a facilitator.²⁹

INTERSECTION AND GAPS

Three themes emerge from the literature:

- Cryptocurrency enables sanctions and SDN evasion, though scalability to the bloc level remains unresolved;
- BRICS Plus actively seeks alternative financial mechanisms, including the NDB and BRICS Pay, but implementation lags rhetoric; and
- The UAE serves as a critical financial and technological hub, linking sanctioned actors to

global markets through permissive digital-asset regulations.

Major gaps persist. No scholarship systematically examines BRICS Plus as a coordinated actor in crypto-enabled sanctions evasion. Research overwhelmingly isolates individual states—Russia, China, Iran—rather than analyzing bloc-level strategic behavior. Further, source bias is substantial: Western literature focuses on risks, while BRICS-aligned texts often serve ideological or aspirational purposes.

In conclusion, current scholarship demonstrates strong linkages among cryptocurrency, sanctions evasion, and BRICS Plus financial strategies but lacks integrative analyses of the bloc as a coherent actor. By combining blockchain forensics with equity-chain mapping, future work can evaluate whether BRICS Plus operationalizes cryptocurrency as part of broader strategic competition with the West. Such insights are crucial for practitioners in irregular warfare, sanctions enforcement, and financial intelligence.

METHODOLOGY

Research Design

The research to support this paper employed an exploratory case study design to examine how BRICS Plus members employ cryptocurrency to facilitate sanctions evasion and advance the bloc's economic objectives.³⁰ The analysis centers on the Russia-UAE pairing—Russia being a heavily sanctioned state globally and the UAE a recent BRICS Plus entrant and major cryptocurrency hub.

This paper integrated blockchain analytics with qualitative open-source and commercial investigative research. We also analyzed publicly available and subscription-based datasets using commercial blockchain analysis platforms, financial intelligence tools, and open-source intelligence (OSINT)

techniques. Additionally, data was collected, monitored, and analyzed data between 21 July 2025 and 12 September 2025, incorporating both historic and current blockchain activity.

Data Collection and Metrics

The initial task involved selecting OFAC-sanctioned or -designated entities with presence in Russia or the UAE, which had been sanctioned in part or full for activities involving using cryptocurrency to evade previous sanctions and designations. The associated sanctions announcements needed to include one or more associated public cryptocurrency wallets, to provide an anchor point from which to begin the blockchain analysis, using Anchain.AI and Arkham Intel.³¹ Desirable entities had a high level of historical or ongoing transactional activity, providing opportunities for larger and more varied data samples. These criteria led researchers to the selection of Garantex (Russia), Grinex (Russia, and the successor entity to Garantex), and Bitpapa (UAE).³²

Data selection emphasized breadth and methodological rigor. Key components included:

- Three sanctioned exchanges—Garantex (Russia), Bitpapa (UAE), and Grinex (Garantex successor);
- More than 4,000 transactions analyzed across those entities;
- From a sample of 451 Bitcoin transactions from Garantex to Bitpapa between 2021 and 2023, 27 transactions involved a Garantex address directly sending or receiving crypto from a Bitpapa address;
- 11 transactions from 2021 and 2022 in which Garantex sent crypto to a Bitpapa address
- 16 transactions from 2022 and 2023 in which a Bitpapa address sent crypto to a Garantex address;³³
- 625 transactions involving three Bitpapa

wallets linked to high-risk addresses associated with malware and illicit finance; and

- 3,100 transactions detected during one observation period from a non-Know Your Customer (KYC)-compliant hot wallet (FixedFloat) one hop from Grinex.

Analytical Framework

Three principal lines of inquiry were followed as noted earlier. Each question guided iterative rounds of data collection and analysis using process tracing to identify linkages between state-linked actors, intermediaries, and financial flows.³⁴ Quantitative transaction data was visualized through deterministic and heuristic clustering to identify wallet ownership and flow-of-funds patterns. Qualitative enrichment involved mapping these findings to corporate networks, shell entities, and ultimate beneficial owners (UBOs) through equity-chain analysis.

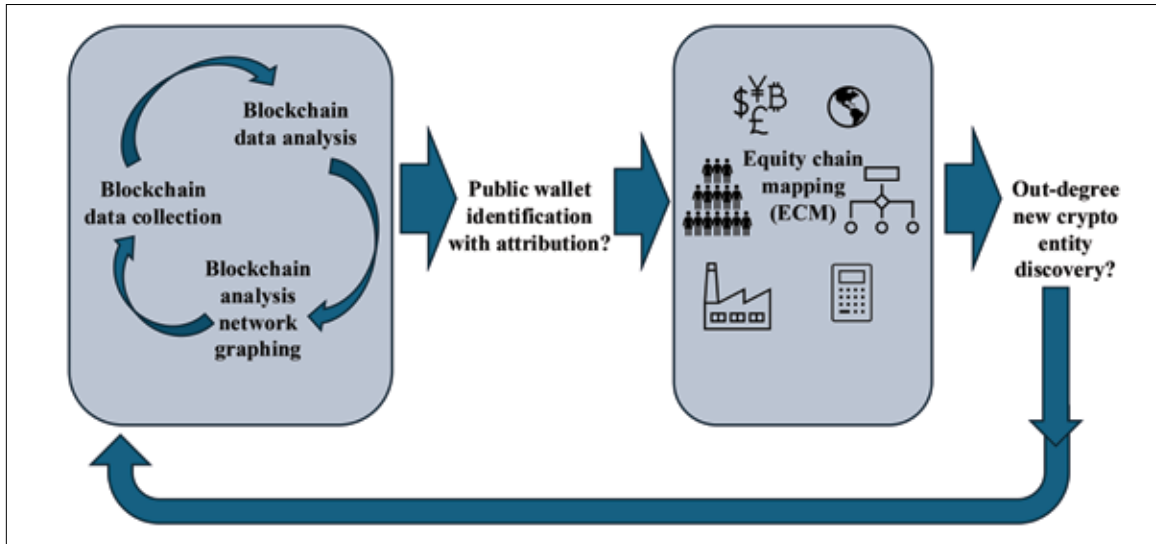
Process Tracing and Triangulation

Process tracing facilitated the identification of key actors, financial intermediaries, and transactional linkages indicative of sanctions-avoidance behavior. Findings were compared against established counter-threat finance (CTF), anti-money laundering (AML), and KYC frameworks to assess alignment with known illicit finance methods. Triangulation across commercial analytics, open-source databases, corporate filings, and government reporting strengthened the validity and reliability of the results.

Limitations

Several methodological limitations are inherent in the design. First, correlation should not be conflated with causation. Single-case studies lack the control conditions necessary to establish causal inference.³⁵ Second, generalizability is limited, as findings are context-specific and may not represent the

Figure 1. Process: Combining Blockchain Forensics with ECM, for Entity Attribution



Source: authors.

broader BRICS Plus network.³⁶ Third, the absence of comparative analysis restricts the ability to detect macro-level patterns across BRICS Plus.³⁷ Finally, bias and limited reproducibility are inherent risks in interpretive study designs.³⁸

Despite these constraints, the exploratory case study design allowed deep insight in context and contributes to the knowledge base methodological guidance for future analyses of cryptocurrency use in sanctions evasion. It further advances understanding of the capabilities and limitations of commercial blockchain analytic tools in assessing state-level irregular warfare and financial operations.

CASE STUDY ANALYSIS

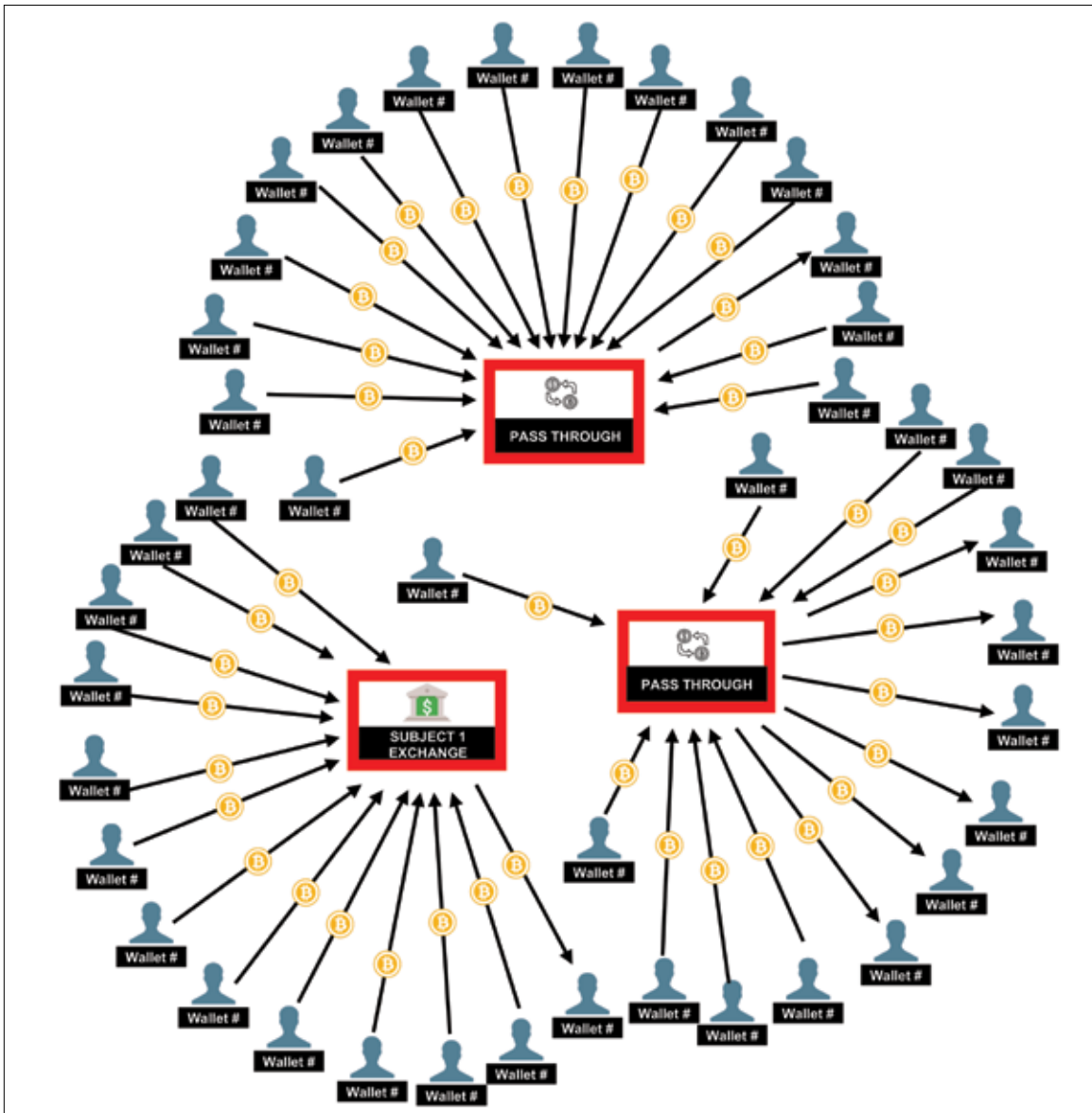
Historical and live blockchain data was collected and analyzed from the selected entities between 21 July and 12 September 2025. Transactions were examined for patterns indicating direct or indirect relationships between the entities and high-risk services, including mixers and exchanges known for weak AML/KYC compliance. When notable activity

was identified, network graphs were generated to visualize transactional relationships.

Each entity then underwent equity chain mapping (ECM) to support attribution of blockchain activity to identified people or organizations³⁹ Graphs derived from blockchain data typically included one known subject interacting with a network of unattributed wallet addresses. This limitation is inherent to blockchain analysis: without prior intelligence or platform-provided attribution, most counterparties remain unidentified. Available data include transaction time, value, and interaction patterns but not verifiable identity.

Applying ECM to known public wallets occasionally revealed associated ownership structures and related entities, allowing analysts to identify additional networks. Newly identified entities were then subjected to further blockchain analysis to discover linked public wallets, creating an iterative cycle of analysis and attribution (Figure 1). While this process could continue indefinitely in an operational intelligence setting, time and resource constraints limited the study to two analytical cycles.

Figure 2. Subject 1 Exchange Interacting with High Risk Addresses.



Source: authors.

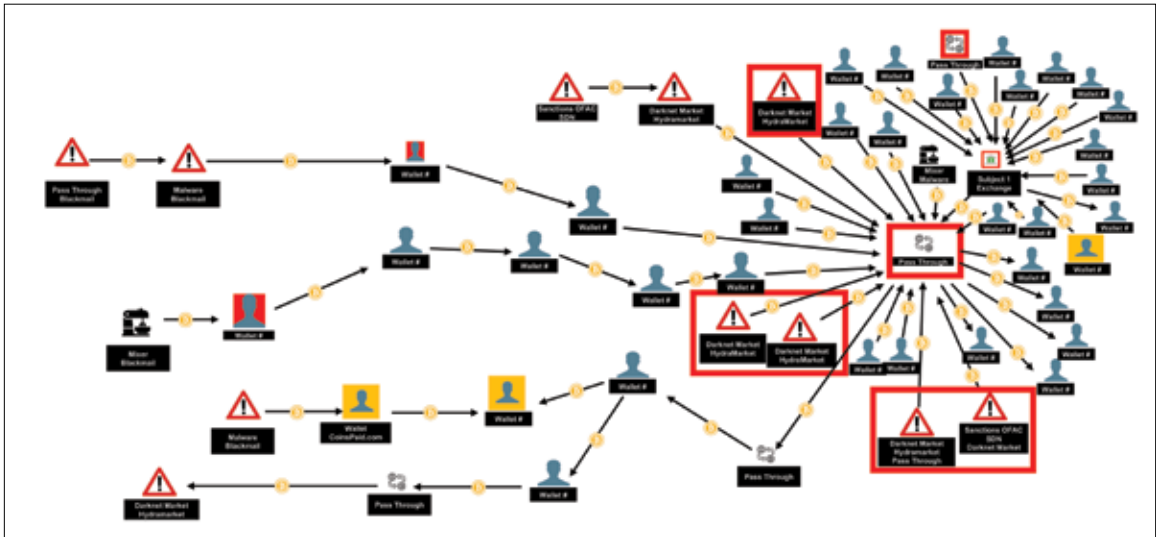
Network Graphing

Ten network graphs were selected to illustrate both the key questions and the broader complexity of the cryptocurrency ecosystem. Each graph includes at least one known entity interacting with addresses associated with malware, darknet markets, mixers,

sanctioned entities, or other high-risk services⁴⁰ Such activity is considered evidence of potentially evasive or illicit behavior, including sanctions avoidance.⁴¹

Graph nodes can be expanded to reveal additional counterparties, dramatically increasing network complexity. Commercial platforms also ingest

Figure 3. High Risk Addresses Only Two Hops From Subject 1 Exchange



Source: authors.

open-source data to support attribution, creating a persistent cat-and-mouse dynamic exploited by threat actors.⁴² The graphs represent snapshots of activity, not complete networks. Each subject controls multiple wallets: only a representative sample is shown. Wallet addresses are abbreviated to the first five characters for readability, consistent with industry practice.

Subject 1 Exchange, Pass Throughs, and High-Risk Addresses

Subject 1 Exchange (Garantex, wallet address: *bc1qw*) was analyzed for interactions with high-risk addresses. Two addresses which interacted directly with the Subject 1 Exchange wallet, both labeled *Pass Through* (see Figure 2), have direct suspicious activity with sanctioned, darknet market, mixer and malware addresses, according to data analysis and high-risk tracer functionality resident in the An-chain.AI platform. *Pass through* refers to an address that provides access to other services, systems, or accounts. Figure 1 shows transactions in Bitcoin (BTC, shown here as yellow circles with a stylized “B”). (Note: the underlying cryptocurrency in

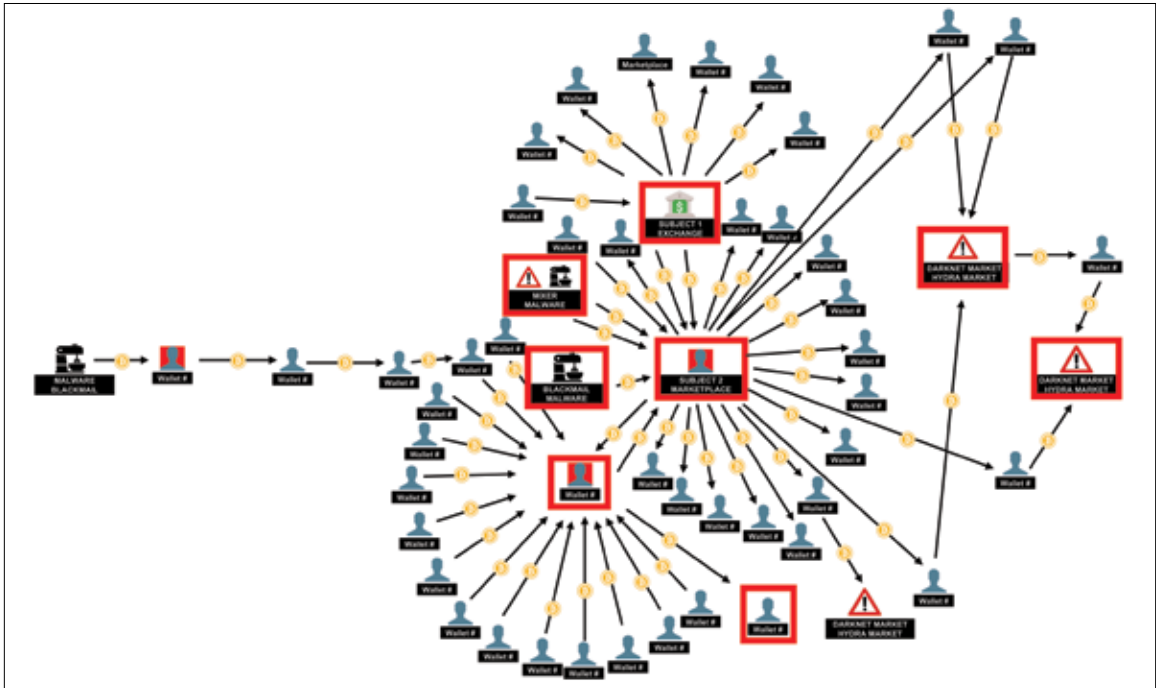
transactions in the remaining figures in this section are all in BTC, unless otherwise noted.)

In exploring the data shown in Figure 2, one of the pass-through addresses (wallet address: *33AGb*) was found within one to five hops from malware, sanctions, darknet markets and blackmail addresses. This can be seen in Figure 3, moving from right to left. Subject 1 Exchange (not highlighted) is the center of the right-hand hub, with the pass through down and to the left slightly. The interactions with concerning addresses continue to the left of the pass-through wallet, some moving in-bound and some out-bound. Red boxes to the left of and below the pass-through show direct interaction with concerning addresses. Red triangles denote additional suspicious activities at two or more levels removed from the pass through.

Subject 2 Marketplace Interaction with Potentially High-Risk Marketplace

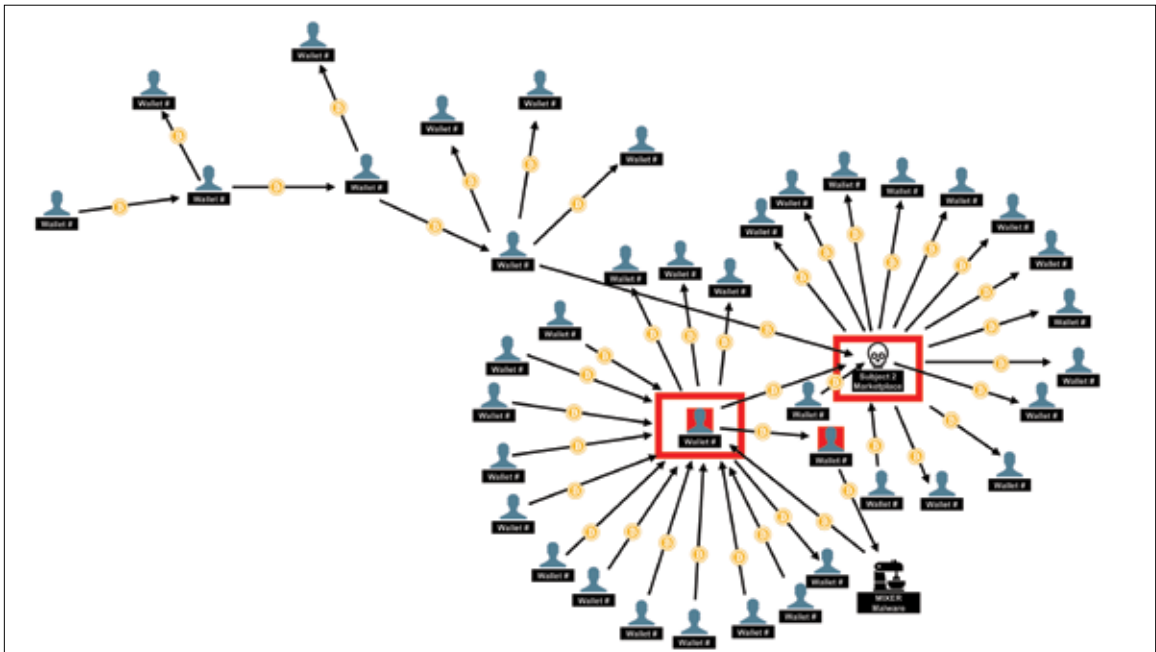
In Figure 4, Subject 1 Exchange (top center) interacts with Subject 2 Marketplace (Bitpapa, wallet address: *bc1qx*, center below Subject 1 Exchange). Subject 2 Marketplace in turn interacts with high-

Figure 4. Subject 2 Marketplace Interaction with High Risk Addresses



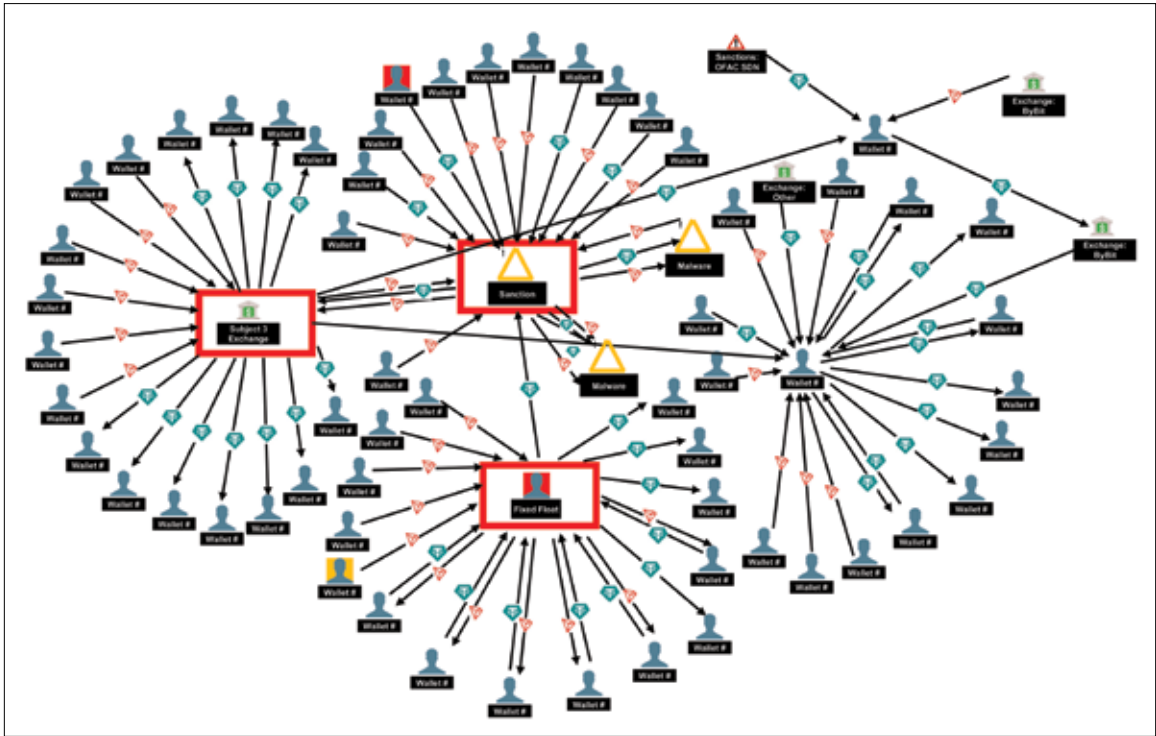
Source: authors.

Figure 5. Exposure of Subject 2 Marketplace to Malware and Mixer Addresses



Source: authors.

Figure 6. Subject 3 Exchange Interaction with Active High Risk Counterparty



Source: authors.

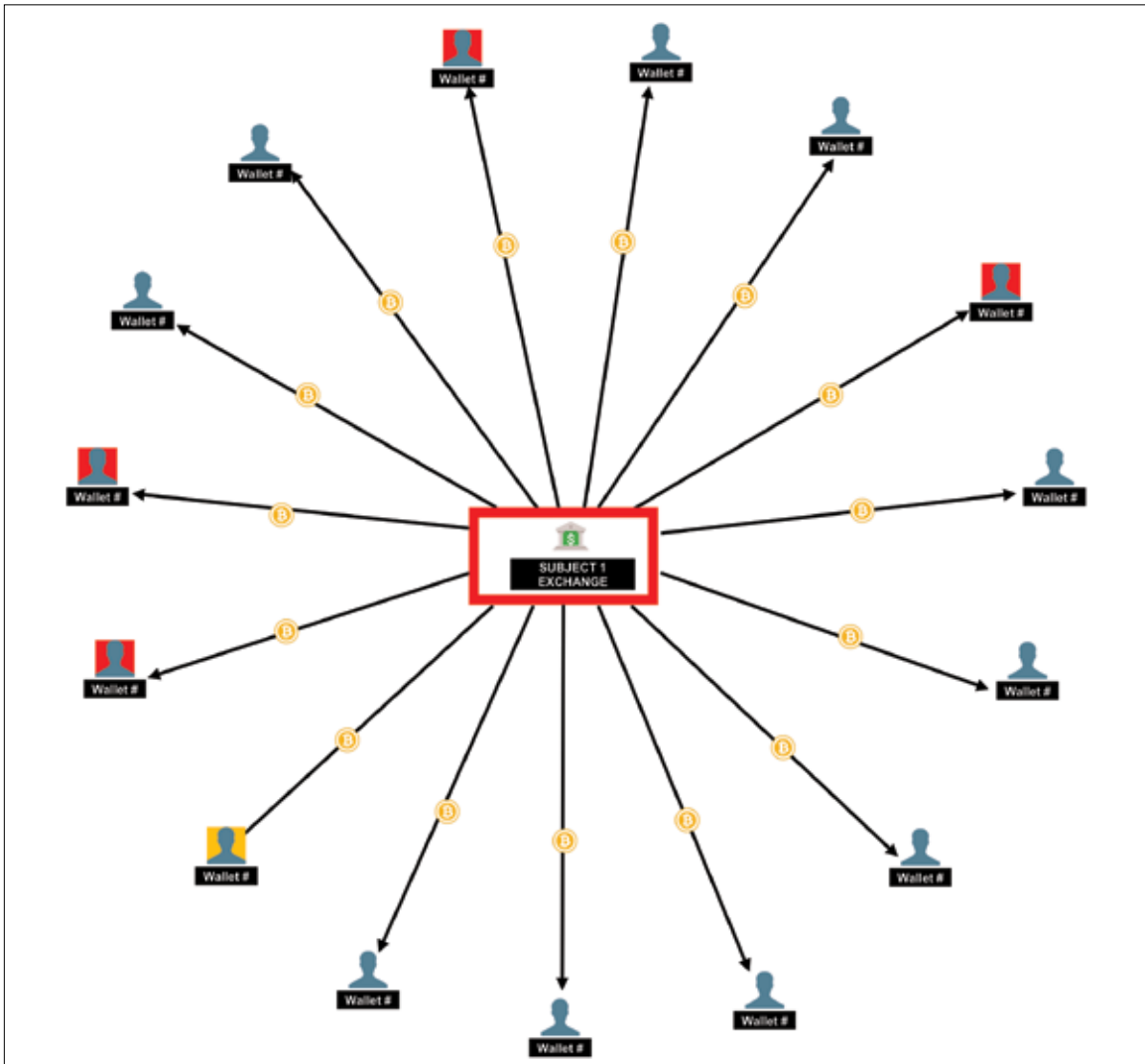
risk wallets (remaining red boxes) which have a high volume of transactions with mixer and malware addresses. The bottom center wallet address was identified as one from the KuCoin exchange. The KuCoin exchange has been in the crosshairs of regulators in the U.S. and the Netherlands for poor or non-existent compliance, and in January of 2025, the company pled guilty in the U.S. to operating an unlicensed money-transmitting business. The guilty plea included a \$300 million fine and two years absence from the U.S. market.⁴³

Subject 2 Marketplace was observed interacting with high-risk address *INffV*, an address which has a high volume of transactions with mixer and malware addresses. This creates indirect exposure of Subject 2 Marketplace to malware addresses, both incoming and outgoing, within 1-2 hops, as illustrated below in Figure 5.

Subject 3 Exchange Activities

In Figure 6, Subject 3 Exchange (Grinex, left hand red box, wallet address: *TL1k1*) directly interacts with address *TJXqR* that in turn has direct interaction with FixedFloat (bottom center red box, address: *TDoXU*). FixedFloat is considered an active high-risk counterparty, according to supplemental data from AnChain.AI. Subject 3 Exchange also interacts with addresses that interact with offshore exchanges. Currency in Figure 6 activity involves Tether (green symbols with a T) and Tron (red three-dimensional triangle shapes).

Figure 7. Hub View of Subject 1 Exchange Direct Interaction With High Risk Parties



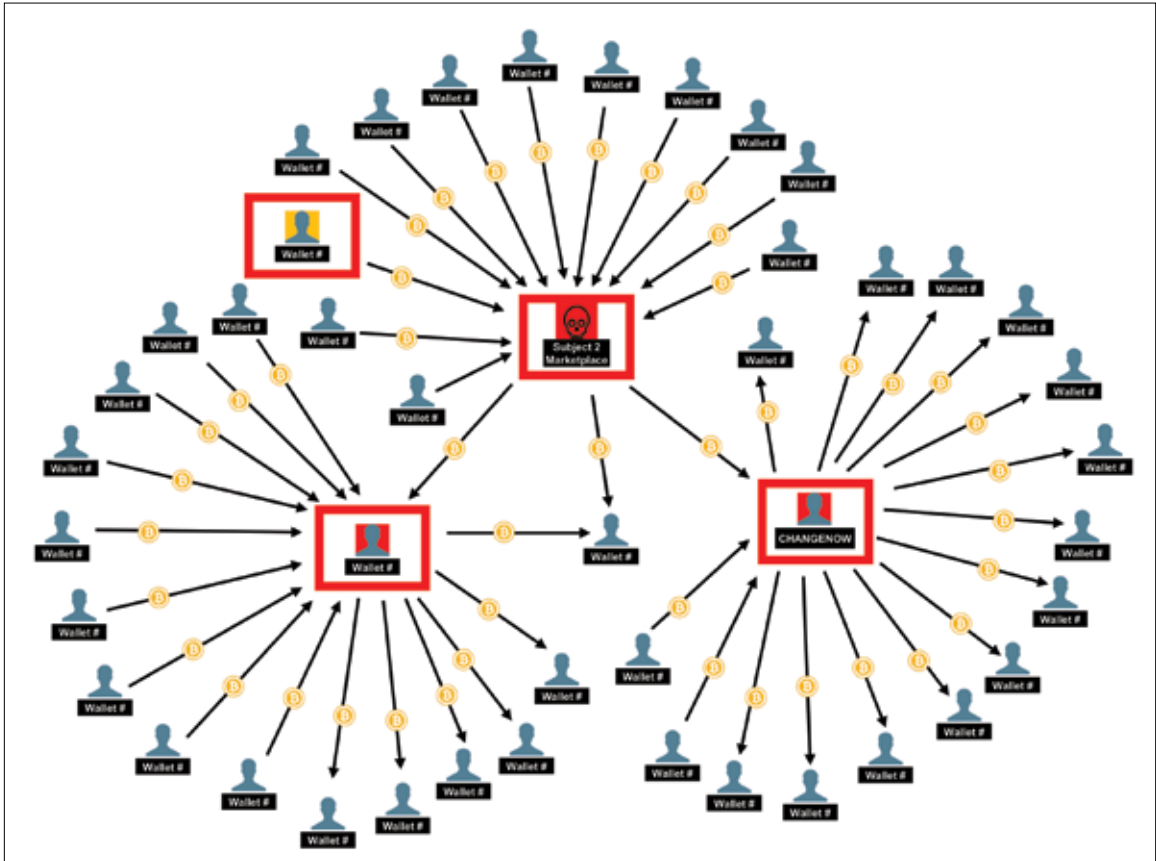
Source: authors.

Subject 1 Exchange (Hub Center) is Shown Directly Interacting with High-Risk Addresses (Red Icons) in Figure 7.

Figure 8 (below) illustrates that sanctioned entity Subject 2 Marketplace (second red box from top) interacted with high-risk addresses ChangeNOW (right hand red box, hot wallet address: *bc1qq*) and an unidentified wallet address: (*bc1qt*). ChangeNOW is identified in AnChain data as

having direct high-volume transactions with malware, mixer, sanction, blackmail, hacker, scam, wallet, ransomware, darknet market and scam addresses over time, thus earning ChangeNOW itself a high-risk entity identity, per AnChain data. ChangeNOW’s *Bc1qq* address specifically had interactions with darknet market and malware addresses previously (not visible in Figure 7), also according to AnChain data.

Figure 8. Subject 2 Marketplace Interaction with ChangeNOW Hot Wallet and Others



Source: authors.

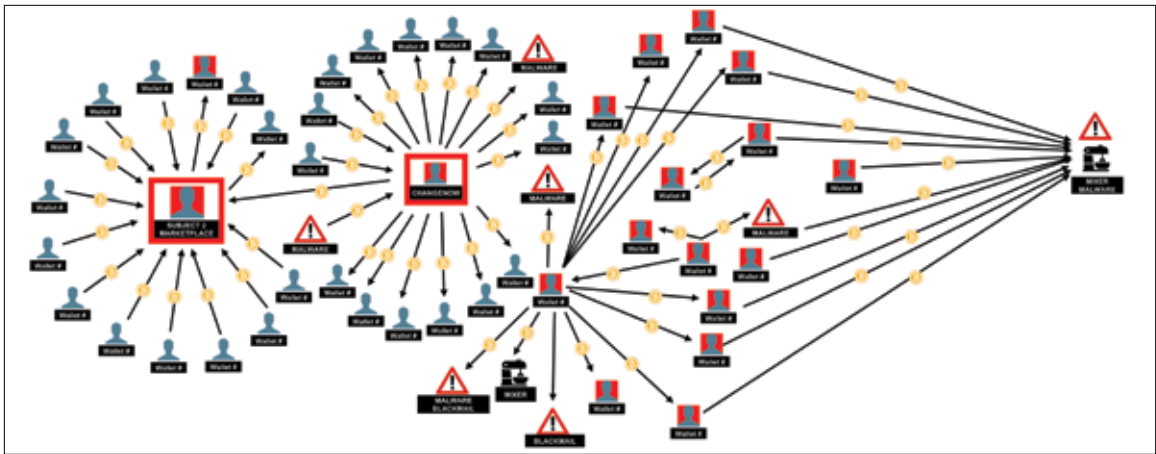
Subject 2 Marketplace further had direct interaction with *bc1qs*, which was separately observed engaged in low volume transactions with a dark-net market address (not included in Figure 8 but included in the underlying data).

Figure 9 shows an expanded view of Subject 2 Marketplace’s interaction with ChangeNOW and ChangeNOW’s high risk activity. According to its website, ChangeNOW indicates users in the US and UK are required to process transactions through its partner, Guardarian. This is an example of nested crypto activity whereby ChangeNOW operates *through* Guardarian to service customers in jurisdictions in which it is not permitted or chooses not to operate directly. The contact information on

the ChangeNOW website directs inquiries to CHN Group LLC, incorporated in Saint Vincent and the Grenadines, address: Euro House, Richmond Hill Road, Kingstown. The mailing address, however, is Newtonlaan 115, Utrecht, 3584 BH, Netherlands. The partner company, Guardarian, is based in Estonia. These entities are discussed later, in the context of ECM.

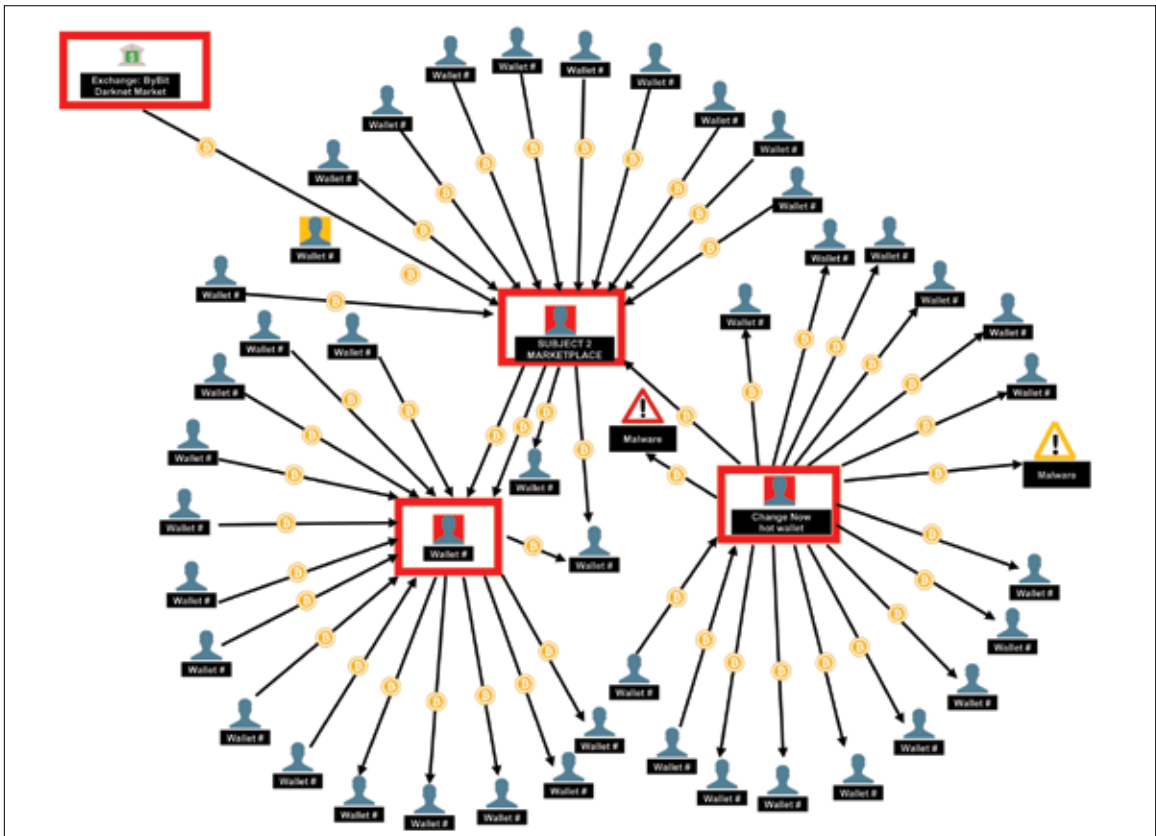
Figure 10 depicts a Subject 2 Marketplace wallet (second red box from the top) interacting with a ChangeNOW hot wallet (right hand red box) and an unknown high-risk wallet (bottom left red box, address: *Bc1qq*). Subject 2 Marketplace in this figure is two hops from Bybit exchange (top left red box), a *potential* exit point or offramp to fiat currency.

Figure 9. Subject 2 Marketplace Interaction with ChangeNOW Hot Wallet, and Other High Risk Addresses



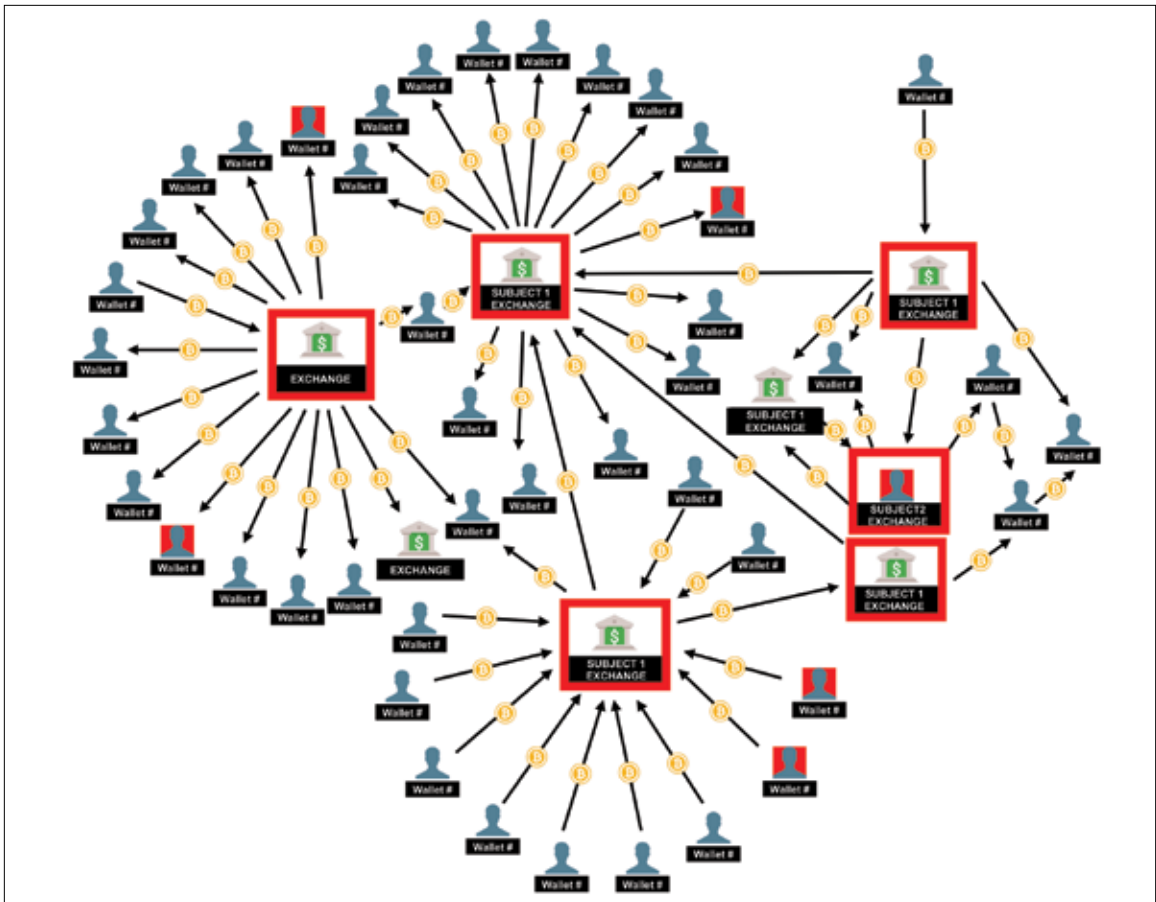
Source: authors.

Figure 10. Subject 2 Marketplace within Two Hops of Off-ramp to Fiat Currency



Source: authors.

Figure 11. Subject 1 Exchange and Subject 2 Marketplace, Interacting with Each Other and with High Risk Addresses



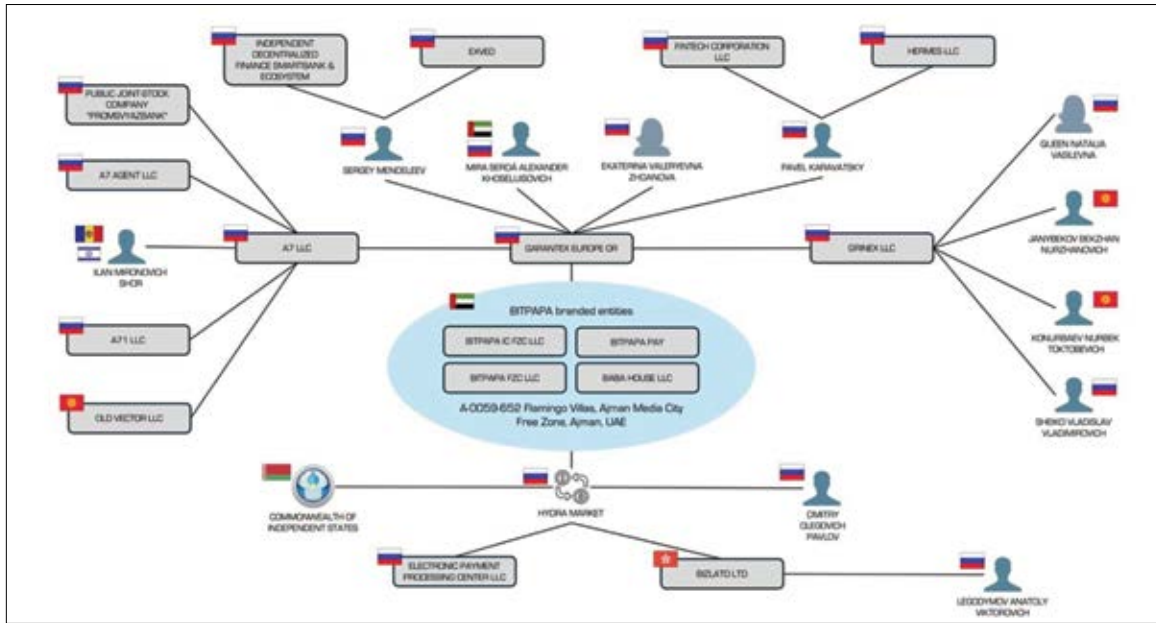
Source: authors.

Off-ramps are an important part in compliance and AML-based analysis of cryptocurrency, as they indicate opportunities to revert to traditional financial systems, after having laundered funds through multiple exchanges, marketplaces, and mixers. It is at these exit points where there is a greater likelihood of detecting ownership (through subpoena or other legal means), due to more stringent compliance regulations associated with conversion to fiat currency.

Finally, Figure 11 shows Subject 2 Marketplace interacting with both Subject 1 Exchange and Subject 3 Exchange addresses, plus a fourth unknown high-risk address (left center node). The unknown address

interacts with a centralized exchange. The target addresses are the core/center of each node. This final figure demonstrates the interaction over time of the subject entities with each other, despite sanctions. The effectiveness of sanctions in cryptospace is at present highly reliant on the willingness of other nations to enforce said sanctions. However, the amoeba-like shifting of the blockchain and its population make it extremely difficult to conduct said enforcement. This ambiguity provides fertile ground for U.S. adversaries – including groups such as BRICS Plus – to establish global financial systems outside the reach of G7-aligned financial controls.

Figure 12. ECM of Subject 1 Exchange, Subject 2 Marketplace, and Subject 3 Exchange



Source: authors.

Equity Chain Mapping

Mapping the corporate relationships between and amongst UAE-based Subject 2 Marketplace, Russian-based Subject 1 Exchange and the related Subject 3 Exchange proved challenging. Outside of the detailed work performed by OFAC, little commercially available information was found to support the ECM process. However, once the three entities were fully assessed in commercial software, the relational network graph appears as follows, in Figure 12.

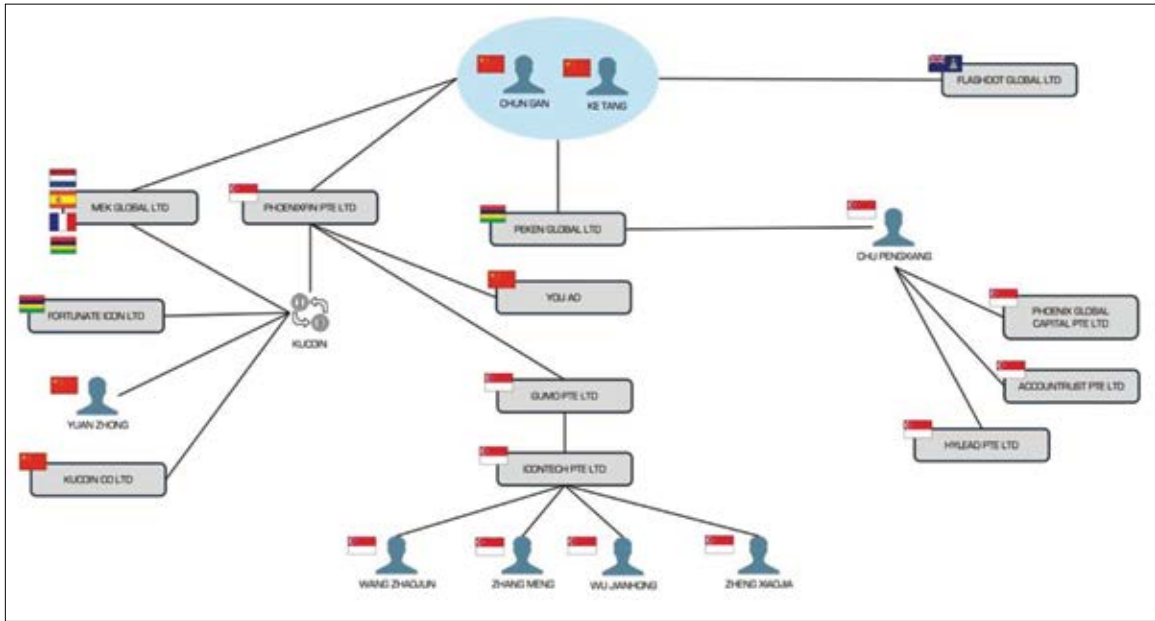
As discussed above, the evidence to support linkages between icons on the graph lie mostly with the narrative in the sanctions and designations issued by OFAC, as well as commercial adverse media aggregators. Nonetheless, the ECM process reveals positive correlation to two individuals and one corporate entity operating in Kyrgyzstan, as well as five previously obfuscated but related Russian entities, and one previously unknown firm in Hong Kong. Should further research be necessary in the future, the process has resulted in multiple

investigative leads. Further, this graphing exercise serves to underscore the centrality of the UAE to Russia’s use of cryptocurrency – even between Russian entities.

Mapping the relational entities associated with *Subject 2 Marketplace interactions* also proved challenging. Notably, the revolving trademark ownership of KuCoin proved key to associating the apparent branding ownership during western enforcement actions. Details of enforcement activities elicited in commercial software aggregators revealed the challenges associated with correctly resolving similarly branded KuCoin entities by several state regulators, including South African authorities. As such, the Figure 13 graph (below) omits many KuCoin branded entities (including many in Germany) which could not be verifiably resolved as associated with this network in the scope on this research.

Unlike the above, in which the center of gravity weighed heavily towards Russia and UAE, the

Figure 13. Applying ECM to Out-degree Entity KuCoin Reveals New Geography



Source: authors.

KuCoin network’s center of gravity lies in China, Singapore, and Mauritius – the latter a privacy and tax haven jurisdiction favored by Southern African countries – including the state of South Africa.

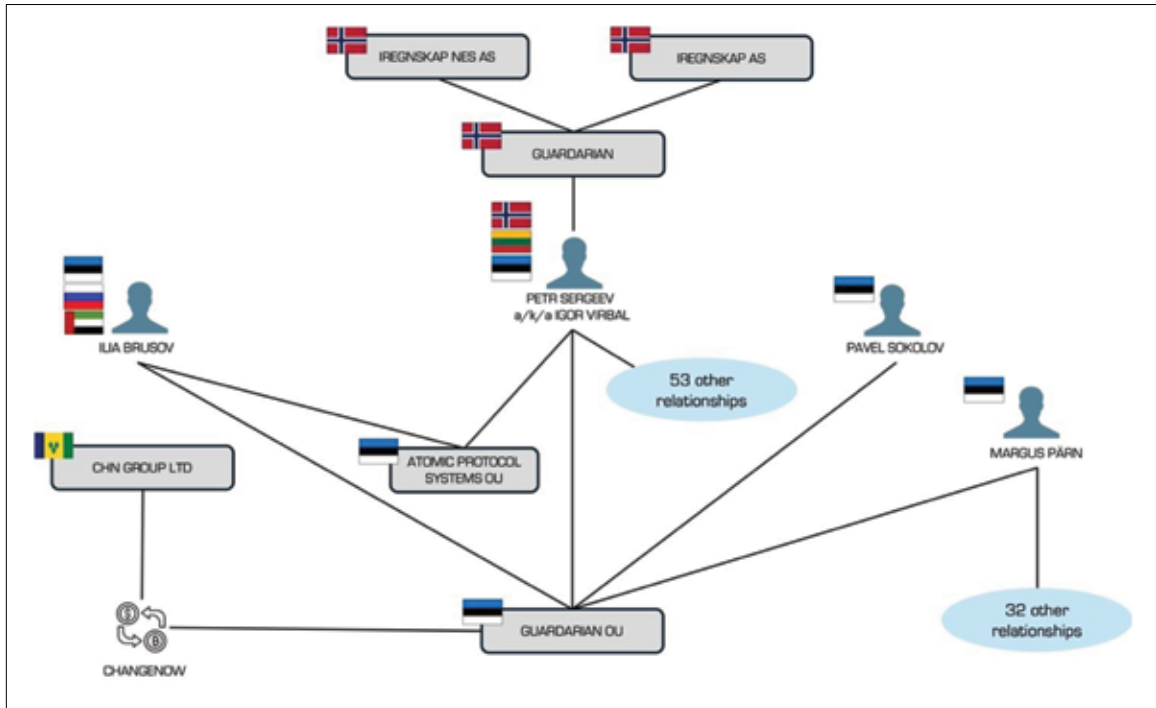
Phoenixfin appears to have undergone ownership changes since western regulators conducted enforcement actions and litigation. Currently Phoenixfin appears to be beneficially owned by Icontech PTE LTD via Gumotech PTE LTD, both domiciled in Singapore. The outsized presence of Chinese surnames appearing in Icontech’s ownership structure is not especially noteworthy, as slightly more than 75% of Singapore’s population is ethnically Chinese. Substantiating actual Chinese ownership in Icontech requires a deeper look at the corporate formation documents above, which the Singapore government has monetized and thus researchers did not access in this study. Finally, the modest similarity in branding between Mauritius-based Fortunate Icon and Singapore-based Icontech provides a potential investigative lead for further research.

The assessment of Subject 2 Marketplace’s interaction with ChangeNOW and Guardarian (mostly) reveals a departure from the geographic centers of gravity identified to this point, in Figure 14. The Guardarian network appears based in Baltic and Nordic countries – especially Estonia – although one of Guardarian’s former key principals (an Estonian national) does maintain residency permits in both Russia and the UAE.

While none of the above ECM work products reveal evidence of state sponsorship or a coordinated BRICS Plus effort, the outsized presence of Russia, China, and Emirati individuals and entities – as well as tax and privacy jurisdictions favored by BRICS Plus nations, is suggestive of tacit state involvement, at a minimum.

Perhaps most notable, however, is the consistent presence of known Russian and Chinese commercial obfuscation tradecraft. In practice, the operational asset may be offshored, then buried in another system as a sub-processor. Conversely, the asset may simply

Figure 14. ChangeNOW ECM Reveals Baltic and Nordic Connections



Source: authors.

nest under an offshore partner relationship. Often this tradecraft is paired with a revolving door of ownership layered over the asset and/or the partner system. Variants of this pattern can be observed in all three ECM graphs, again, suggesting organized state-level efforts to hide in plain sight as legitimate corporate entities in the global financial system.

RESPONSES TO RESEARCH QUESTIONS

Are BRICS Plus Members Engaged in Sanctions Evasion Behavior Using Cryptocurrency?

Yes. Using the case study of OFAC-sanctioned or -designated entities, citizens, and residents of Russia and the UAE, this project analyzed cryptocurrency transactions, on the Bitcoin, Tron, and Tether

blockchains. These transactions involved wallets controlled by sanctioned cryptocurrency exchanges with known physical addresses in UAE and Russia. The transactions took place both prior to and in the time following the sanctions or designation of these entities by OFAC. The identification of these activities required evaluation of on-chain and off-chain data and public or commercial information to elucidate the findings.

If so, can Commercial Chain-Analysis Tools and Equity-Chain Mapping Methods Reliably Detect this Behavior? If not, Could Cryptocurrency Nevertheless Serve as a Sanctions-Avoidance Mechanism for Brics Plus?

This behavior can be analyzed using blockchain forensics combined with off-chain data from public and commercial sources through the review of

historical and current transactions. Open-source reporting and OFAC sanctions notices confirm that Russian exchanges Garantex and Grinex, the UAE-based marketplace Bitpapa, and other platforms demonstrated or supported obfuscation tradecraft to enable sanctions and designation evasion.

On-chain analysis shows that Garantex, designated by OFAC in 2022, transacted with Bitpapa during 2021–2022. Bitpapa presents itself as a peer-to-peer marketplace facilitating buyer–seller crypto trades but relies on escrow smart contracts to intermediate and settle transactions. The platform also enables ruble-to-cryptocurrency exchange through transfers via sanctioned Russian banks, including Sberbank and Tinkoff. Additionally, Bitpapa deployed a Telegram bot to automate buyer–seller connections, reducing friction and increasing transaction scale.⁴⁴

Following its designation in 2022, Garantex’s operators shifted operations to Grinex, which OFAC designated in August 2025. According to criminal indictments, Garantex routinely rotated operational wallets to obfuscate activity.⁴⁵ Because this tactic is commonly used by illicit actors, it is reasonable to assess that Bitpapa employs similar tradecraft. Consequently, the transaction volumes observed through the selected analytics platform likely represent only a subset of total activity.

ECM, when paired with blockchain analysis, strengthens attribution and contextual understanding.⁴⁶ Applying ECM to sanctioned platforms often reveals ultimate beneficial ownership, which can surface additional exchanges, facilitators, and services involved in sanctions evasion within the crypto ecosystem. These findings demonstrate how attribution efforts can expose broader networks rather than isolated platforms.

This analysis also highlighted structural constraints. The privacy model underlying blockchain architecture inherently limits attribution absent external identifiers. Government investigators often rely on technical collection and dark web

exploitation to overcome these barriers. However, when exchanges or individuals appear in public records, legal filings, or regulatory notices, ECM proved effective in identifying broader relationships and previously unreported actors. As commercial analytics capabilities improve, particularly in public-wallet attribution, the value of ECM will continue to increase. Further expansion of this analysis could yield additional networks and insights if pursued in future research.

Does this Behavior Reflect Individual State Actions, or can Researchers Identify Coordinated Bloc-Level Activity?

By tracing observable behaviors both off chain and on-chain, it is clear that proxies of at least two *members* of BRICS Plus are engaging in state-supported sanctions avoidance via the cryptocurrency economy, which largely lies outside of Western financial controls. Although these activities are suggestive of coordination and cooperation between individual states who have BRICS Plus membership, there is insufficient data at present to draw conclusions about whether these are systematic actions of *the bloc as a whole*. The continual increase in variety of tactics, techniques, and procedures used by bad actors in the crypto ecosystem – e.g., *chain hopping* to further obscure transactions trails and evade detection by monitoring platforms – creates further challenges.⁴⁷ Illicit actors are incentivized to build private or *permissioned* blockchains, use *bridges* to move and swap currencies, or to use *mixers* to further obfuscate their transactions.⁴⁸

There are, however, rapidly increasing volumes of data on such observable behaviors – and available tools with which to uncover those behaviors—which suggests that further research, particularly more quantitative research over a broader period, may be warranted to better understand this emerging area of concern. There are benefits to observing evolving transaction behaviors over time, as a snapshot at

any given moment doesn't reveal activities outside that window of time, and historical data may not include emerging capabilities, relationships, and tradecraft. Extended observation may lead to uncovering new techniques, platforms, and behaviors amongst illicit actors.

CONCLUSION

This analysis sought to answer: *What is the current state and viability of cryptocurrency within BRICS Plus as a tool for bypassing G7-aligned financial controls and sanctions?* Although the findings indicate that cryptocurrency is increasingly being used by several BRICS Plus members as part of broader efforts to reduce reliance on Western financial systems, the collective effectiveness of crypto as a sanctions-avoidance backbone for the bloc remains inconclusive.

While this paper focused primarily on Russia and the United Arab Emirates (UAE), analysis suggests that other BRICS Plus members are also exploring cryptocurrency as a mechanism for advancing financial sovereignty and reducing exposure to U.S. dollar-dominated systems.⁴⁹ More developed BRICS Plus economies are attempting to balance domestic oversight frameworks with growing interest in local-currency trade settlement and digital payment systems. Fiat-backed stablecoins are being developed across the bloc as part of this effort. However, cryptocurrencies and stablecoins have not yet demonstrated sufficient reliability or stability to function as a mature, bloc-wide trade settlement system. Their current role is better understood as supplementary rather than transformative.

The evolving U.S. regulatory environment may further complicate BRICS Plus efforts in this domain. The 2025 passage of the U.S. GENIUS Act—particularly if it results in stablecoin backing by U.S. Treasury bonds—could strengthen dollar dominance within the crypto ecosystem and undermine BRICS Plus objectives to decouple settlement

U.S. GENIUS Act: Implications for BRICS Plus

Treasury-backed stablecoins enabled by the U.S. GENIUS Act could extend dollar dominance into crypto settlement layers—turning digital assets into a new channel for U.S. monetary and regulatory power.

Dollar Reinforcement: Stablecoins collateralized with U.S. Treasuries would embed the dollar at the core of on-chain payments, collateral, and trade finance.

Demand Increase: Global stablecoin adoption would translate into sustained foreign demand for U.S. government debt.

Jurisdictional Reach: On-chain activity would increasingly fall under U.S. compliance, surveillance, and enforcement influence—even outside the banking system.

BRICS Constraint: Competing BRICS Plus settlement initiatives risk being outcompeted on liquidity, trust, and scalability rather than blocked politically.

Strategic Paradox: Crypto, framed as a tool of de-dollarization, may instead consolidate U.S. financial primacy by default.

Bottom Line: *Regulated stablecoins could quietly achieve what sanctions and diplomacy cannot—locking in dollar centrality across the next generation of global settlement infrastructure.*

systems from U.S. financial influence.⁵⁰ This development warrants continued monitoring.

Globally, the cryptocurrency market is estimated at approximately \$4 trillion, a significant portion of which flows through offshore and lightly regulated jurisdictions. These environments can foster regulatory arbitrage and create incentives for sanctions evasion, whether opportunistically or by design. The BRICS Plus bloc has publicly stated its intention to construct alternatives to Western-dominated financial infrastructure, and Russia and the UAE have emerged as particularly active in leveraging

cryptocurrency toward that end, albeit for different strategic reasons.⁵¹ Russia’s objective is largely defensive, aimed at mitigating the impact of economic sanctions imposed following its 2022 invasion of Ukraine.⁵² The UAE, by contrast, has sought to expand its role as a global financial center through cryptocurrency adoption, integrating digital assets into its broader economic strategy and positioning itself as a hub for Web3 and financial innovation.⁵³

This project examined transactions between Russian and UAE-based crypto platforms to identify observable sanctions-evasion behavior. Blockchain analysis combined with open-source intelligence indicates sustained interaction between sanctioned Russian entities and UAE-based platforms, demonstrating that cryptocurrency facilitates sanctions-resistant financial activity at the bilateral level. Broader open-source data also allow partial quantification of these flows. While some cryptocurrency platforms nominally restrict U.S. user access, these controls can generally be circumvented through basic anonymization measures.

Interagency Opportunity

This fragmentation highlights a significant capability gap for practitioners engaged in irregular warfare and counter-threat finance. A coordinated interagency effort between the intelligence community and the Department of Treasury could support development of integrated analytic platforms incorporating artificial intelligence to fuse blockchain analytics, sanctions data, and corporate intelligence. Such a capability would represent a major advance in addressing the persistent challenge of cryptocurrency attribution.

Attribution remains a core analytic challenge. Blockchain data alone are insufficient to reveal the identity of the individuals and organizations behind wallet activity. Effective analysis requires integration of on-chain and off-chain data, including corporate records, sanctions disclosures, adverse media, and legally obtained investigative data. Yet no single commercial platform provides comprehensive coverage across these domains. As a result, practitioners

Table 1. Addressing Project Limitations & Exposed Vulnerabilities with Future Research.

Limitation	Potential Follow-on Research
Project examined only one BRICS Plus member country pair	Extend longitudinal analysis across all BRICS Plus states
Tools used for blockchain analysis revealed gaps in coverage	Benchmark blockchain analytics tools for coverage and accuracy
Proliferation of stablecoins as means for FOREX outside of traditional (monitored) banking systems	Assess stablecoins—particularly A7A5—as potential settlement mechanisms
Private and permissioned blockchains not included in data – may mask even greater vulnerabilities	Expand investigative analysis of private and permissioned chains
Ownership/control attribution generally possible only at KYC/AML-compliant exchanges or when exiting blockchain to fiat currency	Model sanctions interdiction strategies targeting exchanges and off-ramps
Absence of China’s influence on dollar-alternative financial systems, including crypto	Repeat this study’s methodology and framing, using China and Brazil as the case study pair

Source: authors.

must rely on layered analytic approaches using multiple tools in parallel.

An additional blind spot exists in the realm of private and permissioned blockchains, which remain almost entirely opaque to commercial analytic tools. Surveillance of these systems will likely require a combination of legal authorities and human intelligence capabilities, as technical collection alone is insufficient.

Current analytic models largely presume that illicit actors intend to convert cryptocurrency into fiat currency through exchanges, making off-ramps a critical point of investigative focus. However, the strategic implication of widespread stablecoin adoption is that reliance on fiat may itself diminish over time. Should BRICS Plus members succeed in establishing functional crypto-denominated settlement mechanisms, existing sanctions (which depend on control of fiat-based chokepoints) could lose effectiveness.

Finally, this work did not touch upon China's evolving attitudes towards and role in dollar-alternative settlement systems or its development of a digital yuan. China's roles in BRICS and in the greater global economy (traditional and crypto) demand closer examination, using the lens presented in this study. A comparable pairing such as the Russia/UAE set, exploring China and perhaps Brazil, could provide valuable insight into the broader strategic alignment-or lack thereof-of the BRICS Plus members states.

This analysis presents a snapshot in time. Continued research is necessary to determine whether cryptocurrency will mature into a strategic financial instrument for BRICS Plus or remain primarily tactical. Future research should:

Absent sustained investment in analytic capacity, the national security community risks losing visibility into an evolving domain of global finance where adversaries increasingly operate beyond the reach of traditional controls. **PRISM**

Notes

¹ "Sanctions List Search" (U.S. Department of Treasury, Office of Foreign Assets Control, updated as needed), <https://sanctionssearch.ofac.treas.gov/>.

² *Society for Worldwide Interbank Financial Telecommunications (SWIFT)*: A vast messaging network used by financial institutions to quickly, accurately, and securely send and receive information, such as money transfer instructions. The system powers most international money and security transfers. ("What is Swift?," Swift, *Who we are*, accessed October 15, 2025.) <https://www.swift.com/about-us/who-we-are/what-swift>.

³ *Joint Publication-1, Vol 1, Joint Warfighting* (Joint Chiefs of Staff, U.S. Department of Defense, August 27, 2023).

⁴ "Stablecoins are digital assets issued by private companies as tokens on a blockchain, typically pegged to a fiat currency like the US dollar, and backed by reserves such as cash or highly liquid securities." (*What is a stablecoin?* McKinsey & Company, September 2, 2025), <https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-a-stablecoin>.

⁵ Elliptic Research blog, "The rise of A7A5: the Ruble stablecoin now transfers \$1 billion per day" (Elliptic, July 28, 2025), <https://www.elliptic.co/blog/the-rise-of-a7a5-the-ruble-stablecoin-now-transfers-1-billion-per-day>.

⁶ Hume, Eleanor and Rutter, Kyle, "Sanctions by the Numbers: 2024 Year in Review" (Center for New American Studies, March 11, 2025), <https://www.cnas.org/publications/reports/sanctions-by-the-numbers-2024-year-in-review>.

⁷ Goldman Sachs' then-Chief Economist, Jim O'Neill, first used the term BRICs in 2001. The group adopted the moniker when it first met in June 2009 in Yeketerinaberg, Russia. Molavi, Afshin, "The BRICS Expansion Is A New World Order of Strategic Multialignment" (*Forbes*, August 31, 2023) <https://www.forbes.com/sites/afshinmolavi/2023/08/31/the-brics-expansion-is-a-new-world-order-of-strategic-multialignment/>.

⁸ "BRICS Previous Summits" (BRICS Brazil website, January 20, 2025), <https://brics.br/en/about-the-brics/brics-previous-summits>.

⁹ Strangio, Sebastian, "Indonesia Officially Becomes First Southeast Asian Member of BRICS" (*The Diplomat*, January 8, 2025), <https://thediplomat.com/2025/01/indonesia-officially-becomes-first-southeast-asian-member-of-brics/>.

¹⁰ Alternatively, BRICS+. The group itself on its website, infobrics.org, is not consistent in this regard. This article uses "BRICS Plus" throughout, for consistency.

¹¹ Cipriani, Marco; Goldberg, Linda S.; and La Spada, Gabriele, “Financial Sanctions, SWIFT, and the Architecture of the International Payments System” (*Staff Reports No 1047*, Federal Reserve Bank of New York, January 2023), https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr1047.pdf?sc_lang=en.

¹² Dasgupta, Saibal, “BRICS’ de-dollarization agenda has a long way to go” (*VOA*, October 26, 2024) <https://www.voanews.com/a/brics-de-dollarization-agenda-has-a-long-way-to-go/7840686.html>.

¹³ Web3 is a concept in technology circles for the next iteration of the Internet. The key concept here is that Web3 will be blockchain-based and decentralized. “What is Web3?” (McKinsey & Company, October 10, 2023), <https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-web3>.

¹⁴ Heaver, Irina, “Building Dubai’s Crypto Hub, The Story Of DMCC’s Leadership” (*Forbes*, December 3, 2024), <https://www.forbes.com/sites/irinaheaver/2024/12/03/building-dubais-crypto-hub-the-story-of-dmccs-leadership/>; “Dubai Blockchain Strategy” (Government of Dubai, published in 2018), <https://www.digitaldubai.ae/initiatives/blockchain>; “World’s premier business destination | DMCC” (Dubai Multi Commodities Centre (DMCC), accessed November 6, 2025), <https://dmcc.ae/>; “DMCC ecosystem: Crypto” (DMCC Ecosystems, accessed November 6, 2025), <https://dmcc.ae/ecosystems/crypto-and-blockchain>.

¹⁵ “Blockchain is a decentralized digital database or ledger that securely stores records across a network of computers in a way that is transparent, immutable, and resistant to tampering. Each ‘block’ contains data, and the blocks are linked in a chronological ‘chain.’” (Hayes, Adam, “Blockchain Facts: What Is It, How It Works, and How It Can Be Used,” Investopedia, September 4, 2025), <https://www.investopedia.com/terms/b/blockchain.asp>.

¹⁶ Coursera Staff, “How Does Cryptocurrency Work? A Beginner’s Guide” (Coursera, July 15, 2025), <https://www.coursera.org/articles/how-does-cryptocurrency-work>.

¹⁷ Human, Kiernan B D, “A Systematic Review of Cryptocurrencies Use in Cybercrimes” (*Graduate Thesis and Dissertation*, University of Central Florida, 2023), <https://stars.library.ucf.edu/cgi/viewcontent.cgi?article=1110&context=etd2023>.

¹⁸ Farrell, Henry and Newman, Abraham, “Weaponized Interdependence: How Global Economic Networks Shape State Coercion” (*International Security*, vol. 44, no. 1, Summer 2019), <https://direct.mit.edu/isec/article/44/1/42/12237/Weaponized-Interdependence-How-Global-Economic>.

¹⁹ *Ibid*, p. 71.

²⁰ Ahari, Armin et al, “Is it easy to hide money in the crypto economy? The case of Russia.” (*Focus on European Economic Integration Q4/22*. Oesterreichische Nationalbank, Legal Division. 2022), https://www.oenb.at/dam/jcr:e5c5af39-daf7-4863-8e33-064e260898b6/04_PB_feei_Q4_22_Is-it-easy-to-hide-money-in-the-crypto-economy.pdf.

²¹ O’Neill, Alex, and Amanda Wick, “Digitally Enabled Sanctions Evasion” (*Journal of Financial Crime Studies*, 2023).

²² Ungboriboonpisal, Ticha, “Efficacy of Economic Sanctions in the Face of Cryptocurrency” (*Journal of International Security and Policy*, 2022).

²³ Wronka, Christoph, “Digital Currencies and Economic Sanctions: The Increasing Risk of Sanction Evasion” (*European Review of International Studies*, 2023).

²⁴ *Africa Intelligence Online*, “Ethiopia Revises Cryptocurrency Regulation amid BRICS Plus Membership,” 2025; Ekanem, Samuel, “Ethiopia Moves Toward Crypto Adoption with Proposed Bitcoin Reserve” (*Business Insider Africa*, 2025).

²⁵ Helmy, Nadia, “BRICS Pay and the Future of Supranational Cryptocurrency” (*Journal of International Political Economy*, 2025).

²⁶ Otorbaev, Djoomart, “Building BRICS Pay: Toward a Sanctions-Resistant Global Payment System” (*BRICS Plus Official Website*, 2025).

²⁷ Cooper, Andrew, and Cannon, Brendon. *The UAE’s Role in BRICS Plus and the New Development Bank*. 2024.

²⁸ Office of Foreign Assets Control (OFAC), *Treasury Sanctions Russian-Based Hydra and Related Entities* (Washington, DC: U.S. Department of the Treasury, 2024); U.S. Department of the Treasury, *National Proliferation Financing Risk Assessment* (Washington, DC, 2024).

²⁹ Warren, Elizabeth and Marshall, Roger, “Letter to U.S. Department of Defense and Department of Treasury on Cryptocurrency and Sanctions Evasion,” U.S. Senate, April 2024.

³⁰ Mills, Albert J., Durepos, Gabrielle, and Wiebe, Elden “Instrumental Case Study” (*Encyclopedia of Case Study Research*, Sage Publications, Inc., Vol. 0, pp.474-475, 2010), <https://doi.org/10.4135/9781412957397.n175>.

³¹ Anchain.AI (<https://ciso.anchainai.com/>) and Arkham (<https://intel.arkm.com/>).

³² Office of Foreign Assets Control (OFAC), “Sanctions List Search: Garantex” (Department of Treasury, 05APR2022), <https://sanctionssearch.ofac.treas.gov/Details.aspx?id=36025>; OFAC, “Sanctions List Search: Grinex” (Department of Treasury, 14AUG2025), <https://sanctionssearch.ofac.treas.gov/Details.aspx?id=55045>; and OFAC, “Sanctions List Search: Bitpapa” (Department of Treasury, 25MAR2024), <https://sanctionssearch.ofac.treas.gov/Details.aspx?id=48096>.

³³ In almost all instances the addresses were distinct on both ends of the transaction. This tactic aligns with the high-risk typology and techniques used by Garantex and other high risk exchanges and marketplaces to obfuscate transactions by continuously moving or using different operational wallets and addresses to transact.

³⁴ Beach, Derek and Pedersen, Rasmus Brun, *Process-Tracing Methods: Foundations and Guidelines* (University of Michigan Press, 2019).

³⁵ Creswell, John W, and Creswell, J. David, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (Sage Publications, Sixth Edition, p.13-15, 2023).

³⁶ Yin, Robert K. *Case Study Research and Applications: Design and Methods*. (Sage Publications, Sixth edition, 2018), <https://ebooks.umu.ac.ug/librarian/books-file/Case%20Study%20Research%20and%20Applications.pdf>.

³⁷ Flyvbjerg, Bent, “Five misunderstandings about case-study research” (*Qualitative Inquiry*, Vol. 12, no.2, 2006, 219–245), <https://arxiv.org/pdf/1304.1186>.

³⁸ Baxter, Pamela and Jack, Susan, “Qualitative case study methodology: Study design and implementation for novice researchers” (*The Qualitative Report*, 13(4), 544-559, 2008); George, Alexander L. and Bennett, Andrew, *Case Studies and Theory Development in the Social Sciences* (MIT Press, 2005), https://www.academia.edu/19264308/Case_Studies_and_Theory_Development_in_the_Social_Sciences.

³⁹ *Equity chain mapping (ECM)*. ECM is both a process and a product. The ECM process leverages AML/CFT and business compliance and analysis tools in an iterative manner, developing a traceable evidentiary chain of information using primary source information, which can then be mapped into a data visualization product, referred to as an *equity chain map*. Conway, Ian and Cassedy, Kathleen, “Equity Chain Mapping: Adapting Counter Threat Finance for Great Power Competition” (submitted for potential publication to *PRISM*, JUL2025).

⁴⁰ “What Is a High-Risk Wallet? Risks & Protection Tips” (Cryptoscam Defense Network, February 25, 2025), <https://cryptoscamdefensenetowork.com/what-is-a-high-risk-wallet/>.

⁴¹ Carlisle, David, “Crypto mixers and privacy protocols: the sanctions compliance implications” (Elliptic blog entry, March 1, 2023), <https://www.elliptic.co/blog/analysis/crypto-mixers-and-privacy-protocols-the-sanctions-compliance-implications>.

⁴² “The Growing Landscape of Seizable Crypto Assets: On-Chain Balances Linked to Criminal Activity Exceed \$75 Billion” (Chainalysis, October 9, 2025), <https://www.chainalysis.com/blog/landscape-of-seizable-crypto-assets-2025/>.

⁴³ Press Release, “Kucoin Pleads Guilty To Unlicensed Money Transmission Charge And Agrees To Pay Penalties Totaling Nearly \$300 Million” (U.S. Department of Justice, Southern District of New York, January 27, 2025), <https://www.justice.gov/usao-sdny/pr/kucoin-pleads-guilty-unlicensed-money-transmission-charge-and-agrees-pay-penalties>.

⁴⁴ Ahari, Armin et al, “Is it easy to hide money in the crypto economy? The case of Russia.” (*Focus on European Economic Integration Q4/22*. Oesterretschtsche Nationalbank, Legal Divison. Pp. 83, 2022), https://www.oenb.at/dam/jcr:e5c5af39-daf7-4863-8e33-064e260898b6/04_PB_feel_Q4_22_Is-it-easy-to-hide-money-in-the-crypto-economy.pdf.

⁴⁵ “United States of America v. Aleksej Besciokov and Aleksandr Mira Serda” (U.S. District Court, Eastern District of Virginia, Case 1:25-cr-00039-CMH, February 27, 2025), <https://www.justice.gov/opa/media/1392316/dl>.

⁴⁶ Conway, Ian and Cassedy, Kathleen, “Equity Chain Mapping: Adapting Counter Threat Finance for Great Power Competition” (submitted for potential publication to *PRISM*, JUL2025).

⁴⁷ “Chain Hopping: The Future of Crypto Money Laundering” (Merkle Science, July 6, 2023), <https://knowledge.merklescience.com/security-risk/chain-hopping-the-future-of-crypto-money-laundering>.

⁴⁸“A permissioned blockchain is a distributed ledger that is not publicly accessible. It can only be accessed by users with permission.” (*Permissioned Blockchain: Definition, Examples, vs. Permissionless*. Investopedia, July 25, 2024), <https://www.investopedia.com/terms/p/permissioned-blockchains.asp>; “A blockchain bridge is a tool for moving crypto assets from one blockchain to another.” (Huffman, Eric, *What Is Bridging in Crypto? A Complete Overview*.w” CryptoNews Academy, December 6, 2024), <https://cryptonews.com/academy/what-is-bridging/>; and “Mixers and tumblers are cryptographic facilities or services that mix different streams of potentially traceable crypto funds concealing the trail leading back to the fund’s original source.” (*Mixers and Tumblers Primer: Overview, Types, Pros and Cons, Legal Status and How They Work*. Merkle Science, August 25, 2022), <https://www.merklescience.com/blog/mixers-and-tumblers-primer-overview-types-pros-and-cons-legal-status-and-how-they-work>.

⁴⁹ Africa Intelligence, “Ethiopia: Government fine-tunes its Bitcoin strategy with an eye on Trump’s announcements” (*Africa Intelligence Online*, April 24, 2025), <https://www.africaintelligence.com/eastern-africa-and-the-horn/2025/04/24/government-fine-tunes-its-bitcoin-strategy-with-an-eye-on-trump-s-announcements.110439246-art>.

⁵⁰“Fact Sheet: Donald J. Trump Signs GENIUS Act into Law” (The White House, July 18, 2025), <https://www.whitehouse.gov/fact-sheets/2025/07/fact-sheet-president-donald-j-trump-signs-genius-act-into-law/>.

⁵¹ Otorbaev, Djoomart, “BRICS Plus: The Emerging Alternative to Western Economic Dominance” (BRICS portal, June 23, 2025), <https://infobrics.org/en/post/49433>.

⁵² O’Neill, Alex and Wick, Amanda, “Sounding the Alarm on Digitally Enabled Sanctions Evasion” (*Lawfare Media*, October 16, 2024), <https://www.lawfaremedia.org/article/sounding-the-alarm-on-digitally-enabled-sanctions-evasion>.

⁵³ Heaver, Irina, “Building Dubai’s Crypto Hub, The Story Of DMCC’s Leadership” (*Forbes*, December 3, 2024), <https://www.forbes.com/sites/irinaheaver/2024/12/03/building-dubais-crypto-hub-the-story-of-dmccs-leadership/>.

Equity Chain Mapping

Adapting Counter Threat Finance for Great Power Competition

By Ian Conway and Kathleen Cassedy

In the economic statecraft that underpins Great Power Competition (GPC), hostile adversary states exploit the seams and gaps in global financial systems and commercial competition to circumvent the U.S. dollar-based trading system, acquire export restricted weapons systems components, conduct influence operations at scale, and otherwise erode U.S. hegemony. Activities in this space invariably fall short of western definitions of war, thus creating a gray zone that concurrently exceeds normal peacetime competition and avoids kinetic response. Capabilities to identify and action such non-kinetic GPC activities sometimes reside outside the U.S. Department of War (DoW) and instead with interagency partners.

The DoW-centric Counter Threat Finance (CTF) tools and techniques that were so successful in the Global War on Terrorism (GWOT) were not designed to pursue nation states and their corporate infrastructure – they were designed to pursue people and associated networks. In GPC, the successful execution of the hostile economic statecraft described above is predicated on the establishment and control of clandestine commercial infrastructure, and the tools and techniques to uncover such infrastructure may reside in the private sector.

The purpose of this article is to contribute to the sparse body of knowledge involving fusing CTF and Counter Threat Network (CTN) methodologies with commercially available tools, technologies, and capabilities to form an operational framework with the doctrine, regulations, and standards that, as of this writing, have not been codified. This article presents one such private sector-developed method: equity chain mapping. This case study demonstrates how commercial tools and techniques can effectively provide insights into answering critical questions such as “Who is the ultimate beneficial owner?” and “Who or what entities exert influence and control?” Like CTN and CTF doctrine, the results using commercial tools take analysis

Ian Conway is an IWC Researcher with nearly 30 years of analytical, investigative, and programmatic experience in national security analysis, private intelligence, and commercial investigations. He is currently focused on developing methods and technology to expose adversary clandestine commercial infrastructure that facilitates political warfare and gray zone activities.

Kat Cassedy is an IWC Researcher, a commercial analyst, and a national security expert with more than 20 years of experience across the public, academic, and private sectors. She is recognized for her deep expertise in open-source intelligence (OSINT), political and economic warfare, and threat analysis at strategic, operational, and tactical levels.

only to a point providing indicators; hard definitive evidence requires more robust and often classified capabilities. However, the concepts discussed here are not just theory – they are effective investigative techniques applicable to sifting through the myriads of corporate structures used by state and non-state actors to target the United States, and U.S. partners and allies.

These methods may provide a roadmap for the CTF community to reframe its tradecraft towards GPC competitors and evolve this work to adapt their valuable capability to address a more enduring problem set.

BACKGROUND

Scholarly research suggests legacy tactics, techniques, and procedures (TTP) developed during the GWOT (especially CTF/CTN) should be adapted to state-level competition and conflict.¹ However, the difference in adversaries and environments requires different approaches. Issues that constituted strategic problems in a counterterrorism context (such as state involvement or six-figure fund transfers)

are relatively insignificant in a GPC environment. The strategic level issues of GPC might include millions – or possibly even billions – of dollars moving through venture capital, private equity, and sovereign wealth funds, through offshore privacy jurisdictions to clandestine commercial infrastructure established to field nation-state level weapons systems. Effectively investigating the latter is more akin to the financial sector's Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) and Know Your Customer/Know Your Business (KYC/KYB) diligence processes, that is, if these processes were designed for investigations rather than regulatory compliance.²

One such process that was specifically designed for commercial investigations is *equity chain mapping (ECM)*. The ECM process leverages AML/CFT and business compliance and analysis tools iteratively, developing a traceable evidentiary chain of information from primary sources, which can then be mapped into a data visualization product referred to as an *equity chain map*. The ECM process is described in detail in the methodology and case

Figure 1. Autopilot hardware component from a downed Russian Orlan-10 UAV.⁵

This is the component containing the software assessed in this report.

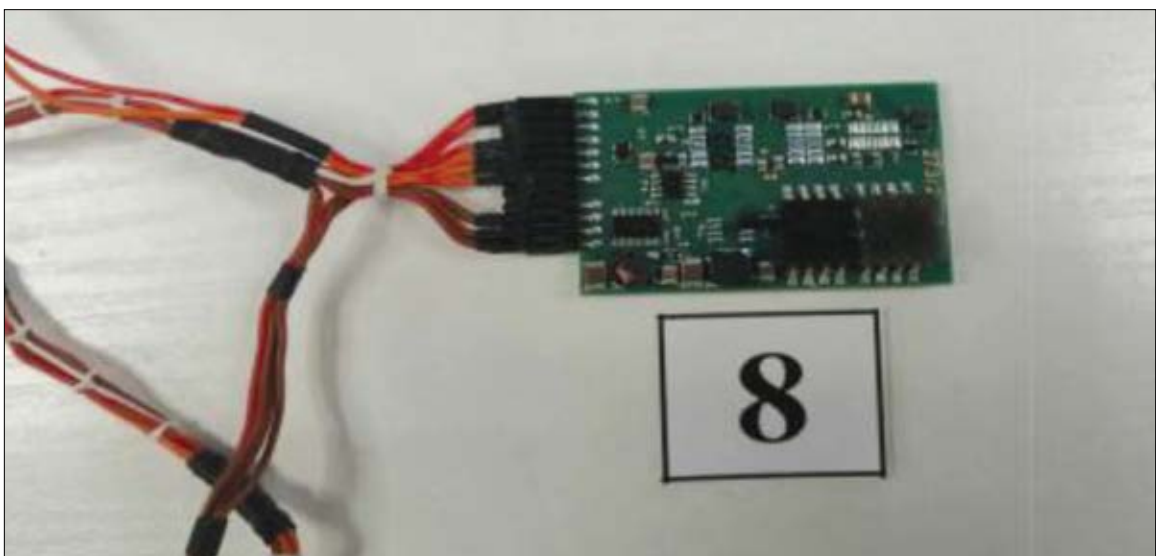
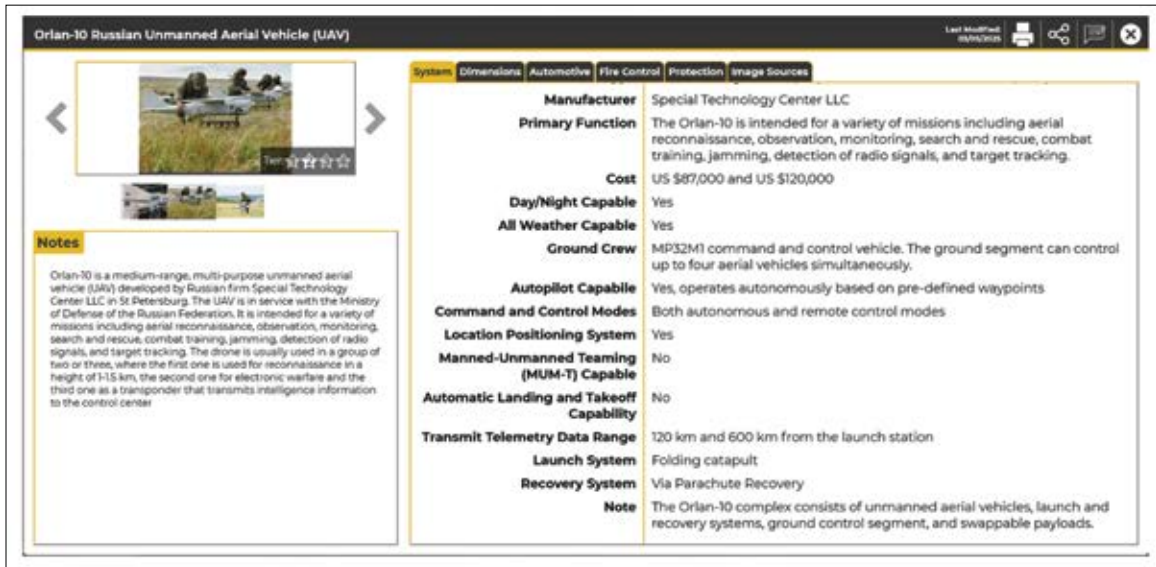


Figure 2. Russian Orlan-10 UAV.⁷
 General description of the airframe and its use.



study sections of this article. Iterative equity chain maps are included throughout those discussions as more is learned about the network at hand during respective methodological steps. The narrative component of the graphic ECM depictions is equally valuable, as what was *not* discovered can be equally important as what *was* discovered.

A case study approach demonstrated the utility of using ECM to uncover the ownership and control structure behind the manufacturer of the autopilot software in a Russian Orlan-10 unmanned aerial vehicle (UAV).³ While the illicit proliferation of U.S. manufactured, export restricted electronics and technology destined for Russia’s ORLAN-10 UAV is well documented in legal cases, commercially sourced intelligence originating in Ukraine provided the technical basis for the UAV components used in this analysis.⁴ The autopilot software component (see *Figure 1*) was selected for this project because it effectively illuminates and validates the approach.

Limited scholarly research addresses the application of GWOT-era CTF and CTN using

commercial software and databases to a GPC strategic environment. There is no evidence in unclassified sources that the national security community has embraced such an idea. Nor is there any indication in open sources that organizations have attempted to operationalize such an approach. There is, however, a body of doctrine, regulations, and established standards that must be considered when addressing this research challenge, given the differences in scale, scope, and environment between the GWOT and strategic competition. Little of the identified doctrinal material has been applied to perform CTF/CTN in a GPC environment. Finally, there is some scholarly research and investigative reporting examining hardware elements of this challenge from a supply chain perspective but equity chain analysis of the auto-pilot software element of the Orlan 10 platform (see *Figure 2*) has not yet been performed.⁶

While the joint doctrine governing CTF and CTN is operationally focused, these disciplines are at their essence intelligence functions – meaning they involve educated guesses and the

instincts that come with experience. Dr. Moyara Ruehsen, Professor at the Middlebury Institute of International Studies described the qualities of the CTF investigator (and by extension, the disciplines themselves) in this passage:

It is also important to be able to recognize whether something is out of the ordinary and be motivated to dig further to find out more information. Of course, sometimes you won't have time to dig deeper, and that is where strong general knowledge about the world—international geography, economics, business, culture—comes into play.

Due to the time-sensitive nature of threat financing and combined with the vast amounts of harmless financial transactions that occur every day, forensics professionals rely on an educated sense of instinct to fish out possible transactions. Knowledge of foreign shipping ports can help investigators recognize whether a shipping route is unnecessarily convoluted. A large shipment of advanced technology exported from a country with little manufacturing base or a shipment of wine from Saudi Arabia will jump out instantly to an investigator working to counter threat finance.⁸

What Dr. Ruehsen has described is the “art” component of intelligence analysis. Forensic accounting, big data analytics, scrutiny of invoices and balance sheets (among other activities) constitute the “science” component.

Many of these qualities are difficult to teach or train. In the analysis that follows, both elements are portrayed in an integrated manner, as they cannot effectively be decoupled. The experienced analyst is under no illusion they will find hard evidence to support their instincts. However, CTF methodologies can leverage ECM to generate focused and

narrow collection priorities for other classified intelligence assets, thus serving as a force multiplier.

INVESTIGATIVE METHODOLOGY: EQUITY CHAIN MAPPING (ECM)

The ECM investigative methodology involves a multi-step, recursive process for developing a 360-degree look at a corporate network. As the process evolves, the ECM methodology uncovers information that allows the user to develop a network map – a construct familiar to CTF professionals. The equity chain map lets the user visualize the methodology’s findings, both during the investigation (or research) and at the conclusion. The equity chain map can reveal centers of gravity, outliers, and areas for further investigation/research. In the intelligence context, equity chain maps (accompanied by an amplifying narrative assessment) developed at an unclassified level can identify focused collection priorities or, alternatively, redirect work to other, more promising areas.

Critically, the ECM process is not a checklist. Undertaking any diligence problem with a compliance or checklist mindset all but guarantees insufficient outcomes. Further, commercial internet search engines are not designed for diligence, and rarely index the deep web data necessary to perform effective diligence.⁹ Search engines are also susceptible to optimization tradecraft and advertising revenue algorithms designed to skew and mis-prioritize search returns in favor of vendors’ wares. These circumstances create the conditions which require the employment of third-party commercial tools (discussed in the appendix of this article) to circumvent the algorithms and filters and zero in on the required primary source data.

The following provides a narrative description of the steps involved with associated ECM task descriptions and requirements.

Perform Entity Resolution. There might be hundreds of companies named XYZ LLC worldwide,

and many of them may be part of the same family of companies. Depending on the business purpose, these may be registered as branch offices, limited partnerships, holding companies, or other structures. Entity resolution involves ensuring that analysts (a) properly identify the correct XYZ LLC for the targeted research, and then (b) identify the remainder of this resolved firm's corporate network. To effectively execute this process, it is critical to understand which information is available to the public and which is not, in each jurisdiction. As Dr. Ruehsen accurately claims, it is also important for the analyst to have a general sense of what "normal" structures look like in various industry sectors.

Determine Ownership and Control. The next step is to validate the ultimate beneficial owner (UBO) and controlling parties. Ownership and control are separate and distinct issues and should not be conflated. Depending on the jurisdiction in which the entity is domiciled and the structure of the corporation, these questions may or may not be possible to answer without inside knowledge. Experienced investigators can make educated guesses using data derived from the entity resolution process, but in many cases, definitive answers are not openly obtainable.

Perform Out-Degree Searches. Gaining a picture of the business activities of identified key management personnel and shareholders at one degree from the resolved entity is critical. This process can greatly help overcome the myopia of consistent branding and reveal in-network business platforms with shared personnel that are not readily apparent due to branding and/or jurisdictional variances. All individuals identified in the ownership and control phase above should be isolated and searched for other corporate affiliations.

Check for Sanctions, Embargos, and Exclusions. Every entity identified in the entity resolution process and every person identified in the ownership and control determination must be checked for

exposure to sanctions, etc. This does not just mean the U.S. Treasury Office of Foreign Assets Control (OFAC) Specially Designated Nationals (SDN) list, as there are multiple U.S. government agencies, and dozens of countries and multinational institutions that issue sanctions, embargos, etc.¹⁰

Check for Political Exposure. The Financial Action Task Force (FATF) defines the term Politically Exposed Person (PEP) and publishes guidance on how these issues should be handled by financial institutions. However, FATF definitions and protocols were designed for anti-money laundering and countering the financing of terrorism (AML/CTF) and are insufficient to address the challenges associated with irregular warfare (e.g., adversarial capital and foreign malign influence.¹¹ Every entity and person identified above must be checked for political exposure.

Check for Wanted Fugitives and Persons of Interest. Every person identified above must be checked against these lists to determine if they are subject to international arrest warrants or are wanted for questioning by authorities. While the International Criminal Police Organization (INTERPOL)'s red notice list is the best known and perhaps most important, some financial markets also publish persons of interests lists for suspected securities fraud and other malfeasance.

Check for Financial Regulatory Authority Enforcement Actions. Every entity and person identified above must be checked for exposure to this kind of derogatory information. While the U.S. Securities and Exchange Commission (SEC) is perhaps the most prominent domestic regulator, this organization does not regulate all types of companies or market participants. Individual markets like the NYSE and NASDAQ may conduct their own enforcement activities. Further, Japanese companies can trade on the S&P 500 just as a Malaysian firm can trade securities on a German market. All relevant databases and sources must be checked.¹²

Check for Criminal Litigation, Civil Litigation, and Arbitration. Litigation checks are critical to the diligence process, and every entity and person identified above must be checked for exposure to this litigation. It is important to note that litigation is not inherently derogatory, and each identified case must be examined to determine adverse exposure. Many jurisdictions (including the U.S. Federal court system) have monetized this data, and while identifying that a research subject has been party to litigation is often achievable in most jurisdictions, obtaining the actual case files may come with additive costs.

Check for Tax Delinquency, Bankruptcies, Liens, and Judgements. Every entity and person identified above must be checked for exposure to financial delinquency, distress, and irresponsibility. Much like litigation records, this data is often monetized or difficult to openly obtain.

Check for Patents, Trademarks, and Intellectual Property. Patent and trademark data is a sometimes-overlooked tool for diligence. Understanding inventors, assignees, and assignors on patents and trademarks can reveal a great deal about an enterprise structure and the nature of a firm's operations. A careful review of this material may reveal offshore entities in tax haven and privacy jurisdictions which are not otherwise identifiable.

Check for Professional Associations, Registration, and Licenses. This kind of data is inherently non-derogatory but can serve to quickly develop a picture of a company's global operational and administrative footprint. The presence of business records in under-regulated markets and tax haven or privacy jurisdictions can reveal much about a firm's activities and intentions.

Check for Nonprofit Affiliations. While most often these organizations do indeed perform charitable and altruistic services, these firms can also serve as vehicles for political influence, corruption, and tax avoidance.

Check for Tangible Assets. The discovery of offshore real estate holdings, private aircraft, or yachts may dramatically change the picture of the research subject. Every entity and every person identified above should be checked for correlation to this kind of information.

Check for Adverse Media/Negative News. While much of what constitutes modern media (especially social media) is wholly unreliable in today's information environment, adverse media checks remain an essential part of the diligence process. Several companies market serviceable adverse media aggregators, but ultimately, researchers must keep in mind that journalists have editors, editors are subject to ownership directives, and owners are reliant on advertising revenue and sometimes directives from their governments. Understanding the track records of individual reporters (many of whom are freelancers) can be invaluable.

Identify and Perform Diligence on Suppliers, Vendors, and Subcontractors. In every instance in which a supplier or vendor is identified, the entire process above should be repeated. The concept of adjacency factors prominently in adversary targeting in the financial space, and while exceptionally arduous, this methodological step is where adjacent targeting can be discovered.¹³

CASE STUDY DESIGN

This research employs a single case study design, using a structured, focused questions approach and process tracing to examine the use of PAI and commercially available information (CAI) resident in tools and databases designed for AML compliance, transparency, and corporate intelligence. The case study focuses on the use of these tools to reveal the funding and corporate network behind the autopilot software of the Russian Orlan-10 UAV, as identified by a Ukrainian engineer in possession of the platform.

Figure 3. Research Questions

To support and frame the research, the above questions guided data collection and analysis.

Question 1	How can CTF and CTN disciplines (both designed for mapping networks of non-state actors) be applied against state-level actors in Great Power Competition using commercial methods and software applications?
Question 2	How can networks of persons, entities, jurisdictions, and timelines associated with the global supply chain of the autopilot software for a Russian Orlan-10 UAV be analyzed, identified, and documented?
Question 3	Why might such networks be constructed this way?
Question 4	How do these networks facilitate circumvention of sanctions or export control laws?
Question 5	How can US. export-controlled technologies discovered in adversary nations' military weapons systems be traced to their ultimate beneficial owners (UBOs)?
Question 6	How do commercial tools and techniques complement CTF/CTN expertise in pursuit of state-level actors in Great Power Competition?
Question 7	How might these tools and databases be employed or modified to augment and adapt existing CTF/CTN methodologies to move past a non-state actors focus and to identifying state-backed financial threats?

Source: authors.

RESEARCH QUESTIONS

Limitations of the Single Case Study

While the single case study design offers important advantages for exploratory and theory-building research, it also introduces well-known methodological limitations. Most notably, findings derived from a single case face constraints on generalizability. As Yin notes, case studies rely on analytic rather than statistical generalization, limiting external validity. However, as Flyvbjerg argues, it is incorrect to assume that meaningful generalization cannot emerge from a single, well-chosen case.

Single case studies also raise concerns about researcher bias and subjectivity. Deep immersion in the case can shape interpretation, and case selection itself may reflect implicit bias, as highlighted by George and Bennett.¹⁴ In addition, the absence of comparative cases restricts the ability to identify broader patterns or test causal relationships across contexts, even though such cases may still yield valuable insights. Finally, single case studies often

face challenges of replication. Their context-specific nature can make reproduction difficult or impractical, limiting reliability and confirmability.¹⁵

Taken together, these limitations suggest that this case study should be understood as a proof of concept rather than a definitive explanatory model. Its purpose is to demonstrate the approach's feasibility and analytic value and to invite follow-on research across additional cases and contexts, potentially contributing to a more generalizable conceptual framework.

ANALYSIS OF THE CASE STUDY, USING ECM

As previously discussed, traditional search engines are a poor choice of tool to perform the kind of work required for effective investigations, necessitating the need for third-party commercial software capable of indexing the deep web and extracting the records derived from these searches. However, most commercial tools were designed for the compliance market, which is arguably an exercise designed to

Figure 4. Five analytical steps of the “Key Elements of Threat Finance”

Doctrinal analytical objectives of CTF.

- | |
|--|
| (1) Identify facilitators and gatekeepers |
| (2) Estimate threat networks’ scope of funding |
| (3) Identify modus operandi |
| (4) Understand the links between financial networks |
| (5) Determine geographic movement and location of financial networks |

Source: authors.

minimize fines and penalties from regulators, and a drain on the bottom line. The compliance process is specifically *not* designed to develop intelligence products. Therefore, the critique and selection of commercial tools for CTF purposes provided in Appendix A should not be construed as criticism of these platforms for their intended use.

Caveats and limitations aside, the following presents the research results from applying the ECM investigative methodology using the select commercial tools discussed in Appendix A. It should be noted that not all tools were employed in every step.

Specific names of companies and people were redacted here to prevent the undue proliferation of PII, and to protect the identities of subjects of this research in an open forum.

At the end of these methodological steps, the majority of the five analytical steps of the “*Key Elements of Threat Finance*” were satisfied, thereby lending support to the promise of ECM as an effective CTF tool.¹⁶ Those steps are:

The initial task in the ECM process involves identifying a starting point by performing wide and sweeping global searches for the subject company:

Step One – Perform Entity Resolution

Active COMPANY-1 branded entities were identified in Belarus, Spain, the United States, Hong Kong, Cyprus, and Canada. Dissolved or inactive entities were identified in the United Kingdom and Switzerland.¹⁷ The corporate structure (or lack thereof) employed in the establishment of these

firms precluded any discernment as to parent-sub-sidiary relationships, as all entities appear to be formed as stand-alone firms.

PERSON-1, a Russian national, appeared in corporate documents in the UK, Spanish, Swiss variants of the firm, thus providing positive correlation between and amongst these entities. Further the UK filings revealed PERSON-1’s location as Hong Kong, providing substantial evidence of correlation to the Hong Kong entity.

The Swiss filings revealed four other partners of PERSON-1, including three who provided addresses in Belarus: PERSON-2, PERSON-3, and PERSON-4. This provided compelling evidence of correlation to the Belarus-registered entity.

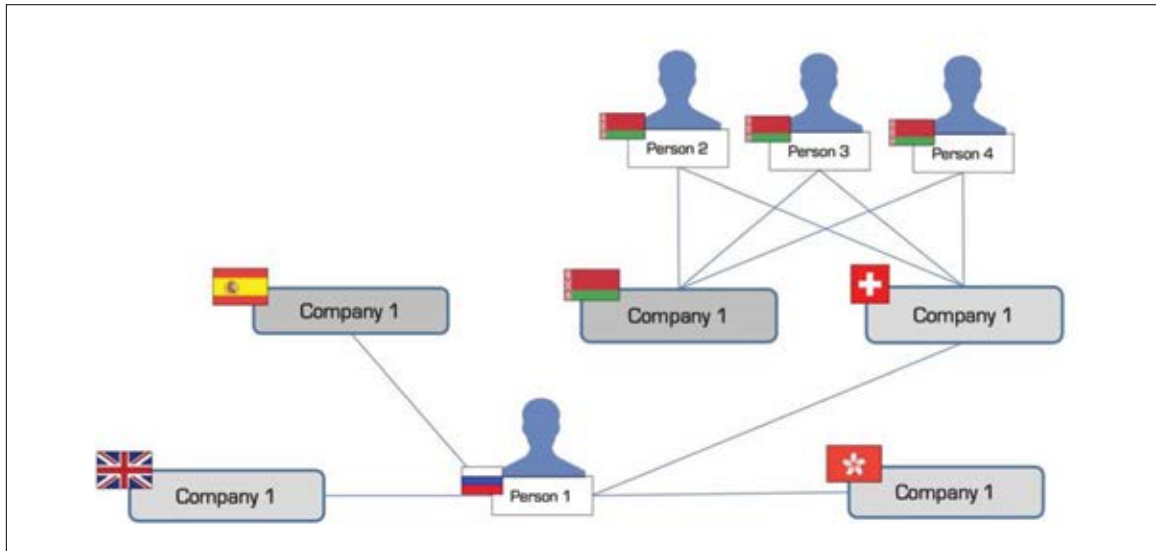
The American, Canadian, and Cypriot firms’ corporate filings did not provide anything which could be used to tie them together with the above apart from the branding.¹⁸ Thus far, this network appears as follows:

A search for COMPANY-1 on a professional networking site returned 22 hits. Of those, only two people – PERSON-2 and a yet unidentified person provided their locations as in the United States. The other personnel represented their locations in Belarus, Spain, Switzerland or the UAE.

An analysis of the firm’s website and associated public relations collateral reveals that this firm represents itself as an American company. The corporate identity logo was used consistently throughout these releases and material. These

Figure 5. Step 2 Findings as Equity Chain Map.

Corporate relationship network map based on knowledge gained at this point in the analysis.



Source: authors.

findings tie the U.S. (Delaware) entity together with the above network. Location data throughout the open-source material is invariably provided as Silicon Valley, but no business filings were identified in the State of California. A search on Google Maps provided an address and location for the entity, but associated imagery of the facility listed a different UAV related company on the front door signage. This entity was designated COMPANY-2 pending further analysis.

Press releases on COMPANY-1’s website revealed the presence of a UAE domiciled Joint Venture (COMPANY-1 JV) under a different brand. This correlates to location data of the affiliated persons on the professional networking site, and the JV was discovered in official UAE filings.¹⁹ PERSON-2 was also listed in corporate filings of the UAE-domiciled Joint Venture as Key Management Personnel along with PERSON-11 (whose nationality could not be discerned).

The Canadian and Cypriot entities still could not be positively resolved to this network.

Step Two – Ownership and Control

Corporate registration data was revisited to assess ownership and control. PERSON-5, a French national, was identified as part of the ownership and control structure of the now defunct Swiss entity. PERSON-6 and PERSON-7 were identified as part of the now defunct UK entity’s control and shareholder structure. Further, the Hong Kong entity was identified as the entity with significant control of the UK entity.

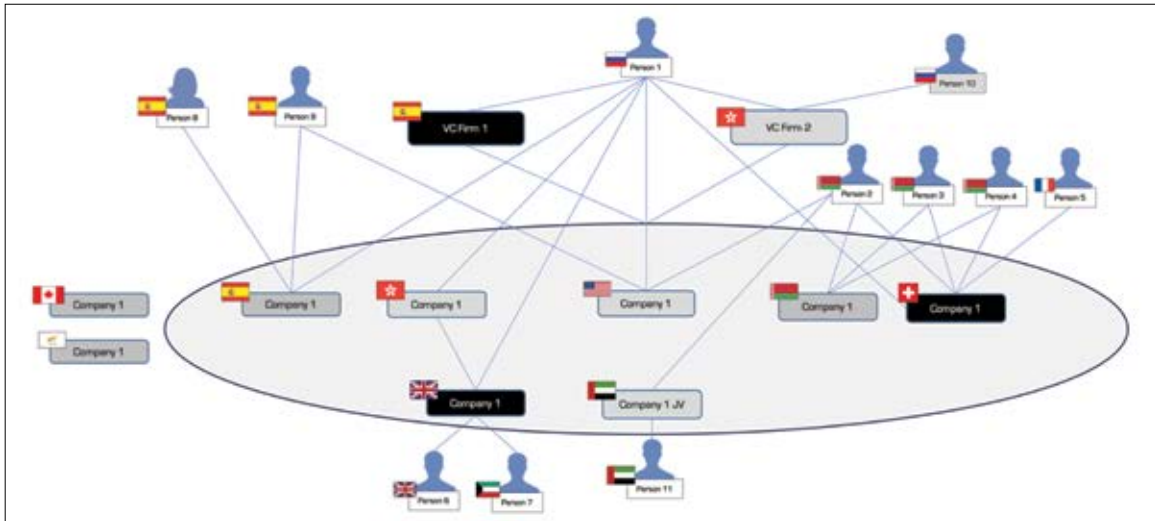
In Spain, PERSON-8 and PERSON-9 were identified as part of the control structure, but shareholders could not be ascertained from public records or commercial data.

Investor data not only greatly aided the picture of beneficial ownership, but also further correlated elements of this network.²⁰ Specifically, these databases revealed that:

- COMPANY-1’s initial investor came from now defunct VC FIRM-1 (domiciled in Spain) and was led by PERSON-1.

Figure 6. Initial Step 3 Findings as Equity Chain Map.

Corporate relationship network map based on knowledge gained at this point in the analysis.



Source: authors.

- COMPANY-1's second round of investment came from VC FIRM-2 (domiciled in Hong Kong) and was also led by PERSON-1.
- PERSON-10 (another Russian national) was identified as a partner in VC FIRM-2.
- Both PERSON-9 and PERSON-2 were correlated to the U.S.-based entity through analysis of this material.
- None of this material was specific as to which COMPANY-1 branded entity was the recipient of these investment rounds.

While the entirety of data thus far does not provide a clean, hierarchical picture of the COMPANY-1 family of companies, it does allow analysts to structure the picture of this network in a manner that both portrays an image of the network and moves the key sources of funding to the top of the graph. The following captures what was learned to this point in the study:

Note that in the above image, defunct entities are shaded black, and connective lines represent

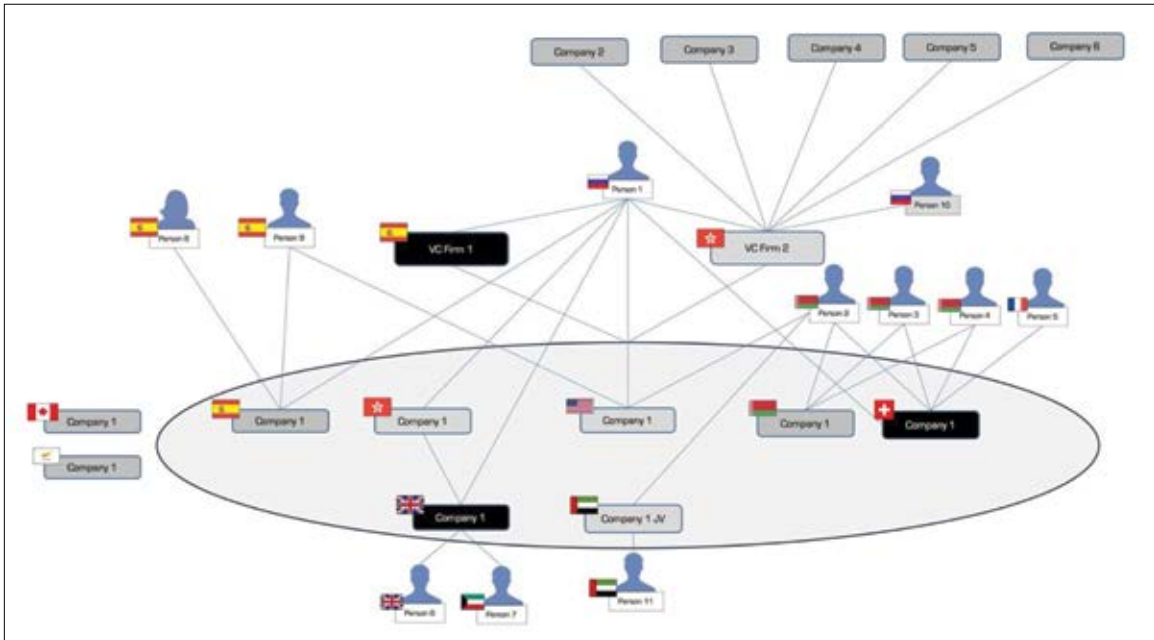
either ownership or control, or both. Ownership equity structures are only available in the (defunct) Swiss entity, and as such it is not possible to distinguish ownership from control at this point in other jurisdictions. However, using the Swiss entity's structure as a guide, PERSON-1 likely holds the majority equity across these investments, with other company officers in minority partner positions. In the case of the UK-based entity, PERSON-1 maintains control through the Hong Kong variant but appears to hold equity himself.

The lines from VC FIRM-1 and VC FIRM-2 to the oval surrounding the COMPANY-1 family of companies is because data sources are unclear as to which specific entity was the recipient of funding. These sources characterize this family of companies as a single entity – the U.S. firm.

Step 3–Perform Out-Degree Searches
 (3A) **VC FIRM-1 and VC FIRM-2:** Commercial data on VC FIRM-1 reveals that COMPANY-1 was its sole investment. However, the same source's data on VC FIRM-2 reveals investment into five other companies (one of which occurred in two separate

Figure 7. Initial Step 3 Findings as Equity Chain Map.

Corporate relationship network map based on knowledge gained at this point in the analysis.



Source: authors.

investment rounds).²¹ Two of these investments were exited with the reason cited as “out of business.”

This data reveals that COMPANY-2 (Note that this is the same company identified in California earlier using Google Maps imagery), COMPANY-3, COMPANY-4, COMPANY-5, and COMPANY-6 may be part of this network as they were beneficiaries of funding from VC FIRM-2. COMPANIES 2, 4, and 5 are also UAV technology companies.

The following graphic depicts what was learned up to this point.

COMPANY-2 was identified in Poland. Executives and board members include PERSON-1, PERSON-3, PERSON-9 and two other individuals with Slavic surnames.²² These individuals were assessed to warrant inclusion in this analysis and were designated PERSON-12 and PERSON-13.

COMPANY-3 could not be effectively resolved to the correct entity given the lack of specific details in the data. However, companies branded the same

way were identified in Russia, Spain, and Delaware. One source stated this company is out of business.²³

COMPANY-4 was identified in Delaware using corporate registration data, and Securities Exchange Commission (SEC) filings were identified which revealed the firm’s address in Washington State and their key executives. Analysis of the surnames revealed three Slavic names, one Anglo name, and a fifth individual with surname that appears to be a hybrid of Slavic and South Asian subcontinent in origin. While no common personnel were identified with other elements of the network, these individuals were added to the network as PERSON-14, PERSON-15, PERSON-16, PERSON-17, and PERSON-18.²⁴

Note that this is the second – and possibly the third – instance of the establishment of a Delaware corporation for companies in this network followed by operational presence on the west coast U.S.

Figure 8. Initial personnel to company correlation matrix.

Illustration of common presence of people across corporate entities based on knowledge gained at this point in the analysis.

	Person-1	Person-2	Person-3	Person-4	Person-5	Person-6	Person-7	Person-8	Person-9	Person-10	Person-11	Person-12	Person-13	Person-14	Person-15	Person-16	Person-17	Person-18
Company-1 (US)	X	X							X									
Company-1 (UK)	X					X	X											
Company-1 (Belarus)		X	X	X														
Company-1 (Switzerland)	X	X	X	X	X													
Company-1 (Spain)	X							X	X									
Company-1 (Hong Kong)	X																	
Company-1 (Joint Venture)		X									X							
VC Firm-1	X																	
VC Firm-2	X									X								
Company-2	X		X						X			X	X					
Company-3																		
Company-4														X	X	X	X	X

Source: authors.

Figure 9. Interim personnel to company correlation matrix.

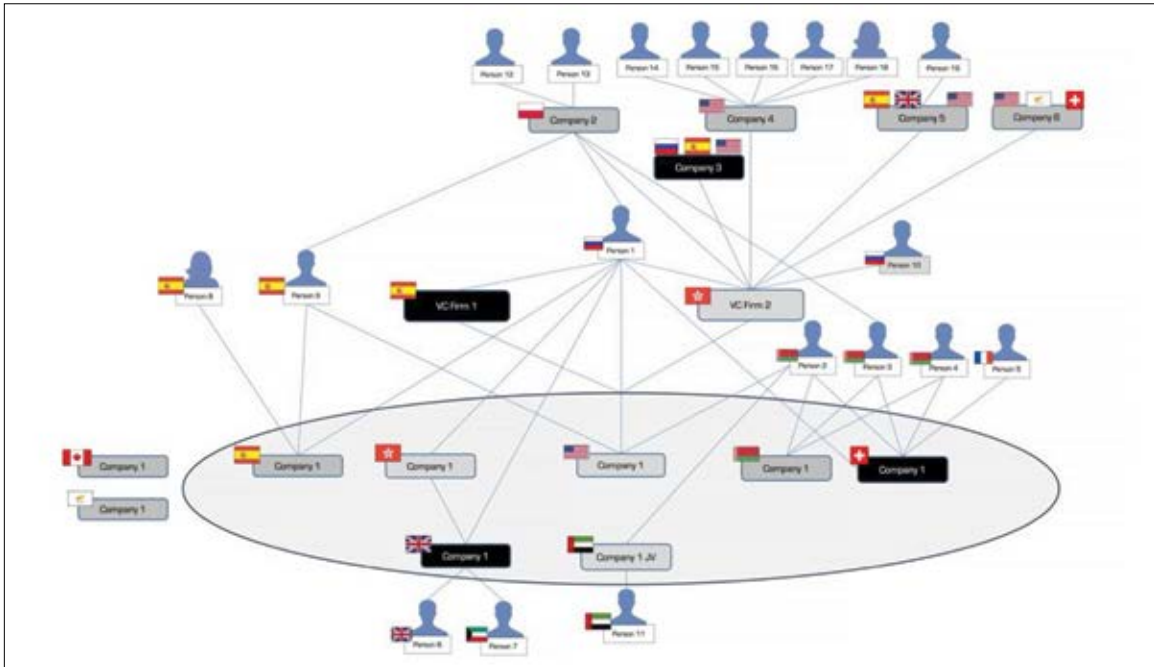
Illustration of common presence of people across corporate entities based on knowledge gained at this point in the analysis.

	Person-1	Person-2	Person-3	Person-4	Person-5	Person-6	Person-7	Person-8	Person-9	Person-10	Person-11	Person-12	Person-13	Person-14	Person-15	Person-16	Person-17	Person-18	Person-19	Person-20
Company-1 (US)	X	X							X											
Company-1 (UK)	X					X	X													
Company-1 (Belarus)		X	X	X																
Company-1 (Switzerland)	X	X	X	X	X															
Company-1 (Spain)	X							X	X											
Company-1 (Hong Kong)	X																			
Company-1 (Joint Venture)		X									X									
VC Firm-1	X																			
VC Firm-2	X																			
Company-2	X		X						X			X	X							
Company-3																				
Company-4														X	X	X	X	X		
Company-5																			X	
Company-6																				

Source: authors.

Figure 10. Interim Step 3 Findings as Equity Chain Map.

Corporate relationship network map based on knowledge gained at this point in the analysis.



Source: authors.

without requisite branch paperwork being filed with the appropriate State Corporation Commission.

COMPANY-5 was identified in Spain, the UK, and Delaware. The sole identifiable individual associated with this company (PERSON-19–Spain and UK) possesses a Slavic surname but could not be correlated to the rest of this network. Commercial data states this company is out of business, but all three companies appeared active.²⁵

A Belarussian company with some (but not all) common branding was identified.²⁶ PERSON-19 was not correlated to the Belarussian firm.

COMPANY-6 was identified in Delaware, Cyprus, and Switzerland, but associated management personnel and executives were not present in the data and thus little else could be learned.

The following graphics depict what was learned up to this point.

And below presented in network graph format.

(3B) VC FIRM-1 and VC FIRM-2’s PERSON-1 and PERSON-10:

PERSON-1 has a common Russian name, and databases were fairly saturated with the same-named individuals. Entity resolution was performed using PII (when publicly available) and related industry-sector activities, which were more readily available. A Cypriot hedge fund and a previously unidentified California-based aerospace company (COMPANY 7, with one other manager, PERSON-20) were identified. PERSON-20 possesses a Middle Eastern surname. Another UK company was also identified, but analysis of primary source material revealed this entity was likely unrelated to the UAV space.

PERSON-10’s activities appeared to be (a) limited to Russia, and (b) business platforms appear mostly defunct in commercial databases.

(3C) COMPANY-1 (UK)’s PERSON-6 and PERSON-7: Primary source material and subsequent

Figure 11. Final personnel to company correlation matrix.

Illustration of common presence of people across corporate entities based on knowledge gained at this point in the analysis.

	Person-1	Person-2	Person-3	Person-4	Person-5	Person-6	Person-7	Person-8	Person-9	Person-10	Person-11	Person-12	Person-13	Person-14	Person-15	Person-16	Person-17	Person-18	Person-19	Person-20
Company-1 (US)	X	X							X											
Company-1 (UK)	X																			
Company-1 (Belarus)		X	X	X																
Company-1 (Switzerland)	X	X	X	X	X															
Company-1 (Spain)	X							X	X											
Company-1 (Hong Kong)	X																			
Company-1 (Joint Venture)		X									X									
VC Firm-1	X																			
VC Firm-2	X									X										
Company-2	X		X						X			X	X							
Company-3																				
Company-4													X	X	X	X	X	X		
Company-5																				X
Company-6																				
Company-7	X																			X
Company-8	X							X	X											
SWF-1						X	X													

Source: authors.

Internet searches reveal that both PERSON-6 (a British national) and PERSON-7 (a Kuwaiti national) were also affiliated with a Saudi Arabian sovereign wealth fund (SWF-1) in executive positions. No correlation or activity between COMPANY-1 and SWF-1 could be drawn outside of shared personnel.

(3D) COMPANY-1 JV's PERSON-11:

Commercial data revealed that this person was also affiliated with a State-Owned Enterprise (SOE) seemingly unaffiliated with this network and is thus adjacent to political exposure.²⁷

(3E) COMPANY-1 (Spain)'s PERSON-8 and PERSON-9:

PERSON-8 was also found to be affiliated with eight other active companies and three inactive

companies.²⁸ Five of the eight active companies have other directors with Slavic surnames. One of the eight companies contains both PERSON-1 and PERSON-9 as principals, and by virtue of these relationships, this company was added to the network as COMPANY-8.

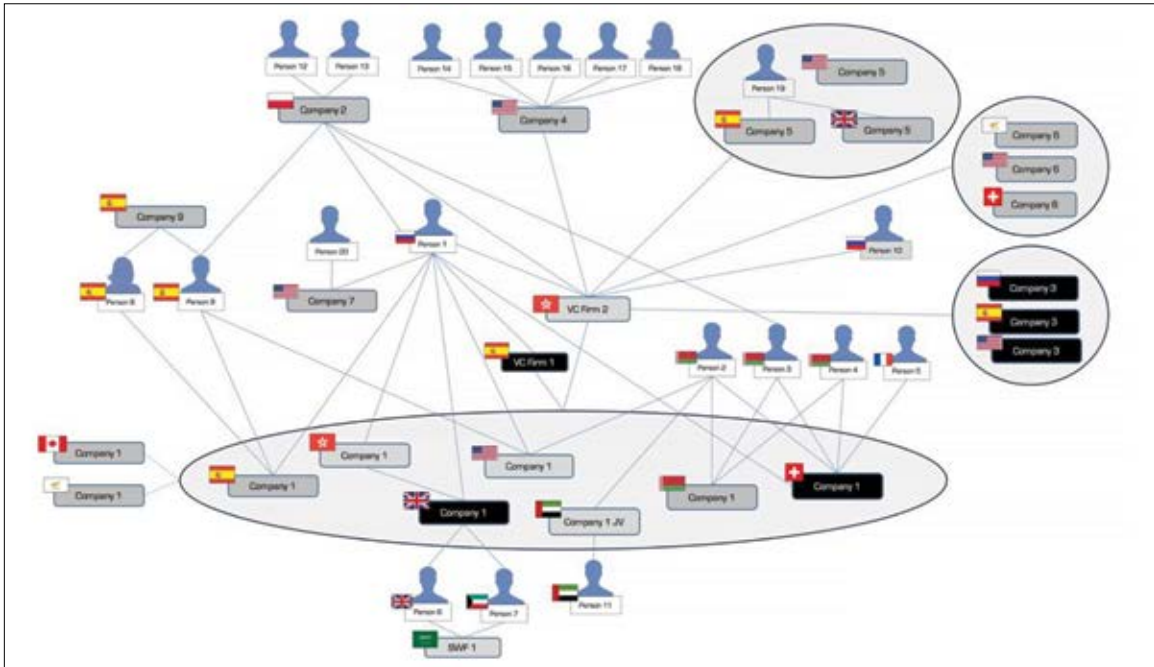
PERSON-9 was difficult to resolve as this is seemingly not an uncommon name. Other highly likely correlations based on industry sector include companies in Russia and Czechia, and possibly the United States – but these could not be validated with certainty given the lack of PII available publicly.

(3F) COMPANY-1 (Belarus)'s PERSON-2, PERSON-3 and PERSON-4:

No other corporate affiliations were discovered regarding PERSON-2 or PERSON-3.

Figure 12. Final Step 3 Findings as Equity Chain Map.

Corporate relationship network map at conclusion of methodological steps 1-3.



Source: authors.

PERSON-4 was discovered to be associated as CEO and owner with a different Belarusian UAV company, which – on the surface – appeared unrelated to this network.

(3G) COMPANY-1 (Switzerland)’s PERSON-5:

PERSON-5 appeared to be currently affiliated with an Irish firm in a similar sector, but other key management personnel had Anglo names, and this entity appeared unaffiliated with the network at hand.

The following network graph depicts all relevant entities and people discovered thus far, along with their relationships to each other, or the lack thereof.

At this point, all twenty persons and thirteen entities were searched individually in the commercial platforms, in the following steps.

Step 4–Check for Political Exposure.

No results were found.

Step 5–Check for Sanctions, Embargos, and Exclusions.

PERSON-4 was identified on OFAC’s Specially Designated Nationals List and on the U.S. Government Contract Exclusion list.²⁹

Step 6–Check for Wanted Fugitives and Persons of Interest.

No results were found.

Step 7–Check for Financial Regulatory Authority Enforcement Actions.

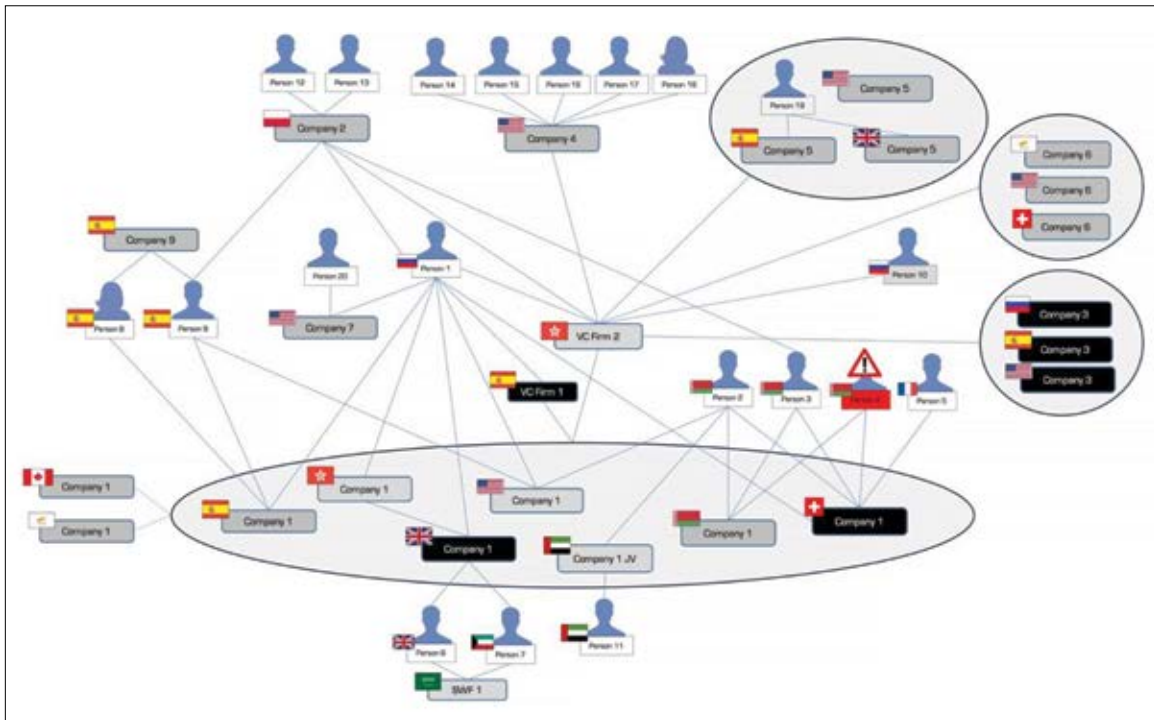
No results were found.

Step 8–Check for Criminal Litigation, Civil Litigation, and Arbitration.

PERSON-1 was identified as possibly associated with civil litigation in the Republic of Moldova, appearing as the defendant being sued by a Moldovan financial institution.³⁰

Step 9–Check for Tax Delinquency, Bankruptcies, Liens, and Judgements.

Figure 13. Final Findings using Equity Chain Mapping Methodology.
Corporate relationship network map at conclusion ECM methodological steps.



Source: authors.

No results were found.

*Step 10–Check for Patents, Trademarks, and Intellectual Property.*³¹

COMPANY-1 holds a registered aerospace-related patent in Hong Kong.

COMPANY-2 holds a registered aerospace control software patent in the Netherlands. This filing identifies PERSON-3's address in Minsk, Belarus.

COMPANY-2 holds the same registered aerospace control software patent as above in Sweden. This filing also identifies PERSON-3's address in Minsk, Belarus and lists a German law firm as the firm's representative.

*Step 11–Check for Professional Associations, Registration, and Licenses.*³²

PERSON-1 was validated as a Person with Significant Control in COMPANY-1 (UK).

PERSON-6 was noted as a Director of a seemingly unrelated company.

PERSON-6 was validated as a Director of COMPANY-1 (UK).

PERSON-15 was noted as a Director and a Person with Significant Control in an uncorrelated company, along with an unrelated Russian person and two Belize-registered financial/investment companies.

COMPANY-1 (HK) was validated as a Person with Significant Control in COMPANY-1 (UK).

COMPANY-5 (UK) was validated as a registered private limited company in the United Kingdom.

COMPANY-6 (CH) possessed a legal entity identifier (LEI) number from the Global Legal Entity Identifier Foundation (GLEIF).³³

Likely uncorrelated companies bearing the same name as VC Firm 2 were registered corporate entities in Australia and the United Kingdom.

VC Firm 2 possesses a possibly correlated GLEIF LEI.

Step 12–Check for Nonprofit Affiliations.

No results were found.

Step 13–Check for Tangible Assets.

No results were found.

Step 14–Check for Adverse Media/Negative News.

No results were found.

Step 15–Identify and Perform Diligence on Suppliers, Vendors, and Subcontractors.

No records of any identified companies importing to the United States were identified.

Findings

While this single case study does not provide definitive findings about Russian procurement networks generally, the application of the ECM process using commercial tools serves as a demonstration case for adapting CTF/CTN tradecraft to address GPC problem sets.

In total, the ECM graphing process in steps 1-3 has moved the analyst's knowledge of the research target from a single corporate identity to a relational network comprised of ten companies, three funding vehicles, and twenty key management personnel in fourteen jurisdictions spanning four combatant commands' areas of responsibility (AORs).

Steps 4 and 5 have revealed that one individual is a Specially Designated National by the U.S. Treasury Office of Foreign Assets Control (OFAC) but provided no evidence of political exposure – meaning that no person in this network appears to be an elected, appointed, or senior member of a foreign government.

Steps six to fifteen revealed one instance of litigation in a jurisdiction outside any corporate presence identified above, and the network's possession of intellectual property rights in three jurisdictions, at least one of which is managed by a German attorney. Further, there are indicators that this network includes funding vehicles and commercial platforms

at more than three outdegrees of remove from the original research target. Many associated details in these findings also validated and corroborated what was learned in steps one to three.

What was *not* identified may be equally important: a lack of bankruptcies, tax delinquency, regulatory enforcement, administrative dissolutions, or adverse media coverage. These are indicators of organizational professionalism and competence.

The use of jurisdictions renowned for their privacy legislation and tax advantages throughout this network has created conditions in which analysts are unable to construct a corporate hierarchy or organizational chart using the available data. Nor are analysts able to untangle funding from ownership, or ownership from control. It is important to distinguish here between using such jurisdictions for their tax advantages and leveraging the same for ownership obfuscation. The former is good legal and accounting practice for commercial entities and wealthy individuals to minimize corporate and personal tax liabilities. The latter is a tactic used by foreign adversaries to mask their equity chains, creating roadblocks to uncovering adversarial capital networks. The geography covered in this case study also includes the presence of corporate entities and nationals from heavily sanctioned nations (Russia and Belarus).

Most critically, the ECM process's findings are suggestive but do not prove state sponsorship of this network's enterprises and funding vehicles. This is *the* central question left unanswered in this case study. Conducting an analysis of more distant outdegrees of association might yield an answer, but more likely, enriching the information with classified intelligence could lead to a clearer determination.

Alignment with Existing Doctrine

At the conclusion of the ECM methodological steps and findings above, critical elements of the five analytical steps of the “*Key Elements of Threat Finance*” were satisfied using exclusively commercial software and open-source information available over the Internet.³⁴ Thus, the research substantiated a single instance of the utility of adapting CTF tactics to the GPC environment.

The following narrative findings are grouped to relate to current CTF/CTN desired outcomes, to assist the reader in relating the ECM findings to doctrine. This is not to suggest that ECM can simply be plugged into or supplant existing CTF doctrine. However, the outcomes do suggest that this case invites further study and could inform broader doctrinal adaptation, particularly in collaboration with financial sector partners.

OUTCOME 1: Facilitators and Gatekeepers

PERSON-1 is overwhelmingly central to this network. He holds key management positions in ten of seventeen identified entities and the venture capital firms he controlled/s and operated/s provided the funding behind another five entities. PERSON-1 is the key facilitator and gatekeeper of this network.

PERSON-2 and PERSON-9 are also key individuals. PERSON-2 has three critical network affiliations and appears to be PERSON-1’s designated lead in the UAE Joint Venture. PERSON-9 also has three key network affiliations and a possibly related fourth connection.

OUTCOME 2: Scope of Funding

While the data is incomplete in commercial databases, venture funding to this network was estimated at roughly \$2.5M in one database. Understanding the values of the network entities’ contracts and revenue, and details of balance sheets as well as profit and loss statements would be necessary

to accurately assess the scope of funding. This network’s entities no longer domicile in jurisdictions where this kind of data is freely available. However, these would make excellent (and specific) collection priorities for an intelligence agency.

OUTCOME 3: Modus Operandi

The corporate structure of COMPANY-1 is interesting in that there is little if any discernable hierarchy. Additionally, the wide range of domiciles among the active companies (the U.S., Spain, Belarus, Hong Kong, and the UAE) creates a variety of opportunities to game export control laws, geopolitical neutrality, talent pools, and treaty alliances.

OUTCOME 4: Links Between Financial Networks

These links are made explicit in the accompanying network graphs, and they encompass finance, ownership, and control – key metrics for regulatory authorities. However, one glaring question appears to be that if COMPANY-1 is actually formed as a single entity, does PERSON-4 possess minority ownership of a U.S. domiciled company, in spite of the fact he is on the U.S. Treasury’s OFAC SDN list?

OUTCOME 5: Geographic Movement and Location of Financial Networks

The expansive range of geography is one of the most noteworthy elements of this analysis. Critically, it spans U.S. Northern Command (USNORTHCOM), U.S. European Command (USEUCOM), U.S. Central Command (USCENTCOM), and U.S. Indo-Pacific Command (USINDOPACOM) areas of responsibility (AORs). However, as U.S. firms are threaded throughout the network, U.S. Persons limitations stemming from EO 12333 must be factored in, as well as Title 10 and Title 50 restrictions.

Possible informational, regulatory, and/or doctrinal gaps

It should be noted that related international transactions could currently be discoverable through subpoena of the U.S.-based SWIFT intermediary/correspondent banks, but this could change rapidly if the BRICS+ nations establish an effective trading mechanism external to the current U.S. dollar-based system.³⁵ This would complicate intelligence collection efforts immeasurably.

Could it be that the company is taking advantage of talented coders in Silicon Valley, then conducting an intra-company transfer to NATO-allied Spain, then to neutral Switzerland, and then to Russian-allied Belarus where contracts with Russia's Ministry of Defense are in place?³⁶ Would this intra-company transfer elude U.S. export control laws, given that nothing was technically sold to a third-party from the U.S.?³⁷

Conversely, was the software code written in Belarus and the western (especially Silicon Valley) entities merely established to create the illusion that COMPANY-1 is a U.S.-tech company for marketing purposes? Again, these questions could constitute focused collection priorities for an intelligence agency.

How would the U.S. Treasury treat the U.S. element of COMPANY-1 if this network was subject to broader sanctions? How would the entity in allied Spain be treated?

Where does Federal law enforcement need to act because DoW is restricted (either by statute or authority, or both) from doing so? What organization would be the Lead Federal Agency for such a task? Is a Joint Interagency Task Force required?

CONCLUSION

While single case studies are inherently constrained in their ability to offer generalizable conclusions, and this study does not provide definitive findings about Russian procurement networks generally, the application of the ECM process using commercial tools serves as a proof of concept for a possible

adaptation of CTF/CTN tradecraft to address GPC problem sets.

The ECM process – using exclusively publicly available information (PAI) and CAI – elicited financial proxies, opaque ownership structures, dual-use platforms, jurisdictional arbitrage, and other findings suggestive of state agency. All of which complicate attribution and sanctions enforcement in state contexts. In this instance, the ECM process moved the analyst's knowledge of the research target from a single corporate identity to a relational network comprised of ten companies, three funding vehicles, and twenty key management personnel in fourteen jurisdictions spanning four combatant commands' areas of responsibility (AORs).

Further, the “*Key Elements of Threat Finance*” were satisfied, thus demonstrating applicability of the ECM process in a Great Power Competition environment after further research.³⁸ In several instances where the capabilities fell short of precision or evidencing tradecraft, the investigative process did result in the development of specific, focused, collection priorities which could potentially be satisfied by Intelligence Community partners.

Irrespective of doctrinal adaptation, larger questions as to limitations of AORs, missions, authorities, restrictions (e.g., EO12333 and PII) and collection priorities loom large. In any case, commercially developed methodologies such as ECM, supported by commercial software and databases to mine CAI and PAI, may be a critical part of any GPC-focused CTF capability, and public-private partnerships may be crucial to the establishment of an effective solution. **PRISM**

Notes

¹ Joint Chiefs of Staff, “Joint Publication 3-25 Countering Threat Networks” (Department of Defense, December 21, 2016), <https://apps.dtic.mil/sti/pdfs/AD1025082.pdf>; Stringer, Kevin D.; Urban, Madison; and Mackay, Andrew, “Counter Threat Finance for Strategic Competition” (*The RUSI Journal*, Volume 168, 2023 Issue 7, Taylor and Francis Online. Published online March 14, 2024), <https://www.tandfonline.com/doi/full/10.1080/03071847.2024.2323740>.

² Financial Action Task Force (FATF), “International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations” (FATF, Paris, France, Updated February 2025), https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF_Recommendations_2012.pdf.coredownload.inline.pdf; “The KYC Process Explained,” (The Society for Worldwide Interbank Financial Telecommunication (SWIFT), July 7, 2025), <https://www.swift.com/risk-and-compliance/know-your-customer-kyc/kyc-process>; “Information on Complying with the Customer Due Diligence (CDD) Final Rule,” (Financial Crimes Enforcement Network (FinCEN), U.S. Treasury, accessed July 7, 2025), <https://www.fincen.gov/resources/statutes-and-regulations/cdd-final-rule>.

³ George, Alexander L., and Bennett, Andrew, *Case Studies and Theory Development in the Social Sciences* (MIT Press, 2005), https://www.academia.edu/19264308/Case_Studies_and_Theory_Development_in_the_Social_Sciences; Willis, Ben, *The Advantages and Limitations of Single Case Study Analysis* (E-International Relations, ISSN 2053-8626, July 5, 2014), <https://www.e-ir.info/2014/07/05/the-advantages-and-limitations-of-single-case-study-analysis/>; Yin, Robert K, *Case Study Research and Applications: Design and Methods* (Sage Publications, Sixth edition, 2018), <https://ebooks.umu.ac.ug/librarian/books-file/Case%20Study%20Research%20and%20Applications.pdf>.

⁴ *United States District Court Eastern District of New York v. Goltsev, Nasriddinov, and Puzyreva*, (United States District Court Eastern District of New York, Case 1:23-mj-00956-LB, filed October 30, 2023), <https://www.justice.gov/archives/opa/media/1322456/dl?inline=>.

⁵ Image provided to the researchers by private individuals with direct access to the component.

⁶ Byrne, James; Watling, Jack; Bronk, Justin; Somerville, Gary; Byrne, Joe; Crawford, Jack; and Baker, Jane, “The Orlan Complex: Tracking the Supply Chains of Russia’s Most Successful UAV.” (Royal United Services Institute for Defence and Security Studies (RUSI). December 2022), <https://static.rusi.org/SR-Orlan-complex-web-final.pdf>; International Volunteer Community, “Russian drone Orlan-10 consists of parts produced in the USA and other countries – photo evidence” (InformNapalm, February 6, 2018), <https://informnapalm.org/en/russian-drone-orlan-10-consists-of-parts-produced-in-the-usa-and-other-countries-photo-evidence/>.

⁷ “Orlan-10 Russian Unmanned Aerial Vehicle (UAV),” (OE Data Integration Network (ODIN), U.S. Army Training and Doctrine Command (TRADOC), accessed July 7, 2025), <https://odin.tradoc.army.mil/WEG/Asset/379eaac7d219f22f944c3b04bd4228cf>.

⁸ Zbrog, Matt, *What is Threat Financing? A Conversation with a Professor* (Forensics Colleges. Publication updated online January 23, 2019), <https://www.forensicscolleges.com/blog/follow-the-money/threat-financing>.

⁹ The Encyclopedia Britannica describes the deep web as “a part of the Internet that extends beyond the reach of search engines ... The deep web ... is likely some 500 times larger than the surface web and may contain as much as 96 percent of online content. Much of this content is in the form of databases that are accessible only by password or subscription or for a fee.” Samuel Greengard. “Deep Web,” *The Encyclopedia Britannica* (Last Updated July 5, 2025), (<https://www.britannica.com/technology/deep-web>).

¹⁰ See for example: <https://sanctionssearch.ofac.treas.gov/> and <https://data.europa.eu/apps/eusanctionstracker/>.

¹¹ National Counterintelligence and Security Center, “Venture Capital and Supply Chain Vulnerabilities” (Office of the Director of National Intelligence, 2024) https://www.odni.gov/files/NCSC/documents/supplychain/Final_VC.pdf; Cassidy, Kathleen and Conway, Ian, “Are Your Business Counter-parties PEPs? Rethinking Politically Exposed Persons Designations” (Information Professionals Association blog, April 18, 2024), <https://information-professionals.org/are-your-business-counter-parties-peps/>.

¹² See, for example: <https://www.sec.gov/enforcement-litigation/litigation-releases> and <https://www.nyse.com/regulation/disciplinary-actions>.

¹³ Conway, Ian; Cassedy, Kathleen, Ryan, Sean; and Danish, Clement, “Reconsidering Great Power Competition Below Armed Conflict” (*The Cipher Brief*, December 13, 2019), <https://www.thecipherbrief.com/reconsidering-great-power-competition-below-armed-conflict>; See for example the Chinese cyber intrusions monikered “Cloud Hopper” in which the objective was information on cloud storage services customers, not the service provider itself. Targeting adjacency is essentially a variant of the “weakest link” concept.

¹⁴ George, Alexander L., and Bennett, Andrew, *Case Studies and Theory Development in the Social Sciences* (MIT Press, 2005), <https://www.academia.edu/19264308/Case-Studies-and-Theory-Development-in-the-Social-Sciences>.

¹⁵ George, Alexander L., and Bennett, Andrew, *Case Studies and Theory Development in the Social Sciences* (MIT Press, 2005), <https://www.academia.edu/19264308/Case-Studies-and-Theory-Development-in-the-Social-Sciences>.

¹⁶ Joint Chiefs of Staff, “Joint Publication 3-25 Countering Threat Networks” (Department of Defense, December 21, 2016), <https://apps.dtic.mil/sti/pdfs/AD1025082.pdf>.

¹⁷ Platform-1 provided Cyprus, Switzerland, Hong Kong, Canada, U.S., and UK entities. Platform-2 provided all of these and added the Belarus and Spain domiciled entities, as well as one false positive.

¹⁸ The U.S. firm is domiciled in the State of Delaware, a notorious privacy jurisdiction. It is a relatively simple matter to establish a holdings company in Delaware using an attorney and a registration agent and successfully incorporate a Delaware LLC without ever providing beneficial ownership details to the state; the Canadian entity is domiciled in Ontario, and while the provincial government does sell more detailed corporate documents than they provide openly, the researchers assessed the acquisition of these documents constituted unnecessary risk of attribution to this project, as these organizations may be subject to insider threats; and the Cyprus entity filings reveal other stakeholders, but none which correlated to anything discovered at this point.

¹⁹ Data identified in Platform-2.

²⁰ Accessed through Platform-3 and Platform-4; Pursuant to JP 3-25 Appendix A *Key Elements of Threat Finance—Estimate threat networks’ scope of funding*, it should be noted that both Platform-2 and Platform-3 provide dollar values and dates of these investments.

²¹ Data accessed through Platform-3.

²² Surnames may offer preliminary indicators of regional or ethnic origin, but they are not definitive evidence of an individual’s nationality, political affiliation, or intent. Analysts should treat such information as circumstantial and corroborate it with additional data before drawing conclusions.

²³ Data accessed through Platform-3.

²⁴ In two further out-degrees of searches, PERSON-16 was found to be affiliated as an executive with a separate California-based company which included a family relation of a sanctioned Russian oligarch. However, this analysis is limited to two degrees of remove from COMPANY-1 and therefore this matter is excluded from this document.

²⁵ Data accessed via Platform-3; “Active” in this context means other corporate signs of life: a functioning website, recent blog posts or press releases, recruitment activities, professional networking site profiles indicating current/more recent employment dates, etc.

²⁶ Common branding is a good lead generation metric but requires additional correlating information to bring into the analysis. In this case, it was determined that similarly named companies had nothing else in common and were most probably unrelated.

²⁷ Data accessed using Platform-2.

²⁸ Data accessed using Platform-2.

²⁹ Data accessed via Platform-5 and Platform-2.

³⁰ Data accessed via Platform-5.

³¹ All data in this methodological step was accessed via Platform-5.

³² All data in this methodological step was accessed via Platform-5.

³³ Many international financial institutions either require or request GLEIF numbers, and thus the presence of a GLEIF number is highly suggestive of international trading.

³⁴ Joint Chiefs of Staff, “Joint Publication 3-25 Countering Threat Networks” (Department of Defense, December 21, 2016), <https://apps.dtic.mil/sti/pdfs/AD1025082.pdf>.

³⁵ “Who We Are” (The Society for Worldwide Interbank Financial Telecommunication (SWIFT), accessed July 7, 2025), <https://www.swift.com/>.

³⁶ An older version of COMPANY-1’s source code was located on Git Hub during this analysis.

³⁷ Code of Federal Regulations (CFR), “Title 15, Subtitle B, Chapter VII, Subchapter C, Export Control Regulations” (The National Archives, last amended March 24, 2025), <https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C>.

³⁸ Joint Chiefs of Staff, “Joint Publication 3-25 Countering Threat Networks” (Department of Defense, December 21, 2016), <https://apps.dtic.mil/sti/pdfs/AD1025082.pdf>.

Shadow Strategy

Air and Space Power in the Gray War

By Dr. J. William (Bill) DeMarco

FROM DOMINANCE TO DISRUPTION IN THE GRAY WAR

The strategic environment is no longer defined by the binary conditions of war and peace. Instead, modern conflict increasingly unfolds in the ambiguous terrain between them, where state and non-state actors wage campaigns of influence, coercion, and disruption without triggering open warfare.¹ This contested space—often referred to as the “gray zone”—demands new ways of thinking about national power, especially in the air and space domains, as the United States confronts an era of renewed great power competition.²

Air and space forces have historically been oriented toward conventional deterrence and high-end conflict, but their roles in this “gray war” require reexamination. To effectively compete, deter, and respond, U.S. air and space power must be reimagined, not merely as instruments of conventional superiority, but as agile tools of influence, disruption, and persistent strategic shaping in the gray zone.³ This shift entails not only technological innovation but also the doctrinal, organizational, and cultural transformation within the services that wield them. As great power competition intensifies, the ability to detect, disrupt, and deter adversary actions short of war may prove more strategically decisive than traditional battlefield dominance. To master this environment, U.S. air and space power must transition from a force optimized for kinetic dominance to a more nuanced instrument of persistent shaping, strategic signaling, and cognitive influence.

REDEFINING THE CONTESTED SPACE: GRAY WAR, POLITICAL WARFARE, AND HYBRID CONFLICT CONCEPTUAL CLARITY IN AN AMBIGUOUS DOMAIN

Contemporary strategic competition increasingly unfolds in a contested space below the threshold of conventional war. This space has been described variously as the “gray zone,” “hybrid warfare,” “political warfare,” and “irregular competition.”⁴ Yet, these overlapping terms risk conceptual ambiguity unless carefully delineat-

Dr. J. William DeMarco is Chief Academic Officer at the LeMay Center for Doctrine Development and Education, Air University. He is a senior U.S. Air Force civilian academic whose work focuses on professional military education, strategy, doctrine, and futures-oriented research. His scholarship and writing address leadership, cognitive warfare, and strategic judgment in complex security environments.

ed. The evolution of this lexicon often reflects the shifting threat perceptions of the Western security community; for instance, the term “hybrid warfare” was first popularized to describe the tactics of non-state actors like Hezbollah before being adapted to characterize Russia’s actions in Ukraine, broadening its meaning and causing it to bleed into the “gray zone” concept.⁵ Such conceptual drift can hinder the development of effective strategy. Establishing definitional precision is therefore a critical first step.

Differentiating the Concepts

“Gray war” refers to sustained campaigns of coercion, disruption, and influence conducted by state or state-backed actors that deliberately remain below the threshold of conventional armed conflict but are executed with strategic intent.⁶ These campaigns are characterized by ambiguity, gradualism, and the integrated use of non-military and quasi-military tools to achieve political objectives.⁷ This stands in contrast to “political warfare,” a term rooted in Cold War strategy and exemplified by George Kennan’s 1948 policy memorandum.⁸ Political warfare refers broadly to the use of all national instruments of power short of war—including diplomacy, propaganda, and economic statecraft—to achieve strategic aims.⁹ In this sense, political warfare is a broader strategic concept, while gray war refers more narrowly to the specific operational campaigns of coercion and influence often associated with near-peer competition and the manipulation of escalation thresholds.¹⁰

Gray war also differs from “hybrid warfare,” a term that gained prominence after the 2006 Israel–Hezbollah conflict and Russia’s 2014 actions in Ukraine. Hybrid warfare typically describes the blending of conventional and irregular tactics within active combat operations.¹¹ By contrast, gray war operates before open hostilities erupt, in what some have called the “pre-conflict phase.” This label is itself problematic, given that many modern

conflicts, such as the U.S. interventions in Iraq and Afghanistan, occurred without formal declarations of war.¹² The distinction, therefore, is not about legal declarations but about the absence of active, large-scale combat. Cold War contests such as the Berlin crisis exemplify gray war’s strategic shape.

Some scholars challenge the utility of gray zone concepts, arguing that they blur traditional distinctions between war and peace.¹³ However, when defined with precision, gray war provides an essential framework for understanding contemporary strategies that weaponize information, economic leverage, proxies, and technological disruption while avoiding overt conflict. This definitional clarity becomes crucial when evaluating the role of air and space power in this new arena.

AIR AND SPACE POWER AS INSTRUMENTS OF INFLUENCE AND DISRUPTION

Air and space power have traditionally been associated with high-intensity conflict and deterrence through overwhelming kinetic superiority. The demands of gray war, however, require a fundamental reimagining of these domains as agile tools of influence and disruption.¹⁴

Persistent ISR and Attribution

Gray zone campaigns thrive on ambiguity and deniability, allowing adversaries to make incremental gains while avoiding accountability.¹⁵ The primary counter to this ambiguity is persistent intelligence, surveillance, and reconnaissance (ISR). Space-based assets, including both national security and commercial satellite constellations, provide the persistent stare needed to uncover covert activities, from the construction of military facilities on artificial islands to the massing of “unmarked” troops.¹⁶ Similarly, airborne ISR platforms can monitor maritime militia movements or track the flow of illicit

Table: Defining the Shadows: Political Warfare, Hybrid Threats, and Gray War Compared

Concept	Primary Locus of Activity	Key Methods	Relationship to Armed Conflict	Primary Actors	Strategic Example
Political Warfare	The strategic level; shaping the political environment.	Diplomacy, propaganda, economic aid/sanctions, support to political movements.	Activities conducted “short of war.”	Primarily state intelligence and diplomatic agencies.	U.S./Soviet Cold War influence campaigns.
Irregular Competition/Warfare	The tactical/operational level; population-centric.	A violent struggle for legitimacy and influence; insurgency, terrorism, propaganda, subversion.	Can occur during peace, competition, and war; often avoids direct military confrontation.	State and non-state actors.	Taliban insurgency in Afghanistan.
Hybrid Warfare	The operational/tactical level; conduct of hostilities.	Blending conventional military forces, irregular tactics, terrorism, and criminal behavior.	Occurs <i>within</i> active combat operations.	State militaries and/or non-state proxies (e.g., Hezbollah).	Russia’s 2014 invasion of Crimea (fusing special forces, conventional military, and local proxies).
Gray War/Gray Zone	The strategic/operational level; the space <i>between</i> peace and war.	Information operations, economic coercion, cyber operations, proxy support, legal warfare (“lawfare”), gradualist military pressure.	Deliberately stays <i>below</i> the threshold of conventional armed conflict.	State and state-backed actors (e.g., China, Russia).	China’s island-building and maritime militia activities in the South China Sea.

Source: author.

arms to proxy forces. By “rendering the invisible visible,” ISR from air and space exposes adversary actions to global scrutiny, enables attribution, and creates a strategic dilemma for the aggressor: actions, once exposed, can lose their political utility and generate international condemnation, thereby imposing costs without firing a shot.¹⁷

Signaling and Strategic Messaging

The visible presence of air and space power is a potent form of strategic communication. Bomber task force missions over the South China Sea, aerial patrols in the Baltic region, and freedom of overflight operations serve as tangible, non-escalatory demonstrations of U.S. commitment and capability.¹⁸ These missions influence adversary calculations and reassure allies precisely because they are reversible and occupy the ambiguous space

between routine presence and overt hostility.¹⁹ They signal resolve and shape the strategic environment without crossing the kinetic threshold, making them an ideal instrument for managing escalation in a gray zone crisis.

Non-Kinetic Effects and Electromagnetic Spectrum Dominance

Modern air and space platforms are increasingly equipped to generate non-kinetic effects, directly targeting an adversary's ability to command and control its own gray zone operations.

The EC-37B *Compass Call* represents a significant leap in airborne electronic attack capability. Replacing the legacy EC-130H, this platform, based on a Gulfstream G550 airframe, is faster, flies higher, and has a longer range, making it more survivable and responsive in contested environments.²⁰ Its core mission is to deny, degrade, and disrupt adversary communications, tactical networks, and information ecosystems.²¹ In a gray zone scenario, the EC-37B could jam the communications between a maritime militia vessel and its shore-based command or disrupt the navigation systems of drones used for harassment, imposing operational costs without resorting to force.²² Its open-architecture design allows for rapid software updates, providing the agility needed to counter new threats in a protracted gray zone competition.²³

Orbital jamming satellites are another key tool for gray zone competition in space. Non-kinetic actions like jamming and spoofing satellite signals are becoming increasingly common because they can disrupt an adversary's command and control, ISR, and navigation with a degree of plausible deniability.²⁴ An orbital jammer can create widespread effects, sowing confusion and degrading an opponent's operational capability without generating debris or crossing the threshold of a direct attack on a sovereign asset.²⁵

Cyber-ISR drones blur the lines between physical presence and cyber operations. The proliferation of low-cost, adaptable unmanned aerial systems makes them ideal platforms for cyber and signals intelligence collection in contested areas.²⁶ A "perch and stare" operational concept, in which a drone covertly lands on a rooftop to passively collect data on wireless networks, is a quintessential gray zone tactic that creates significant attribution challenges.²⁷

THE COGNITIVE DOMAIN: STRATEGIC COMMUNICATION AND NARRATIVE WARFARE

Gray war is not fought solely with missiles and jamming pods; it is waged in the minds of populations and the perceptions of decision-makers.²⁸ Strategic communication has thus emerged as a battlespace in its own right, where adversaries such as China and Russia actively pursue narrative dominance as a form of coercive shaping.

Adversary Doctrine: China's "Cognitive Warfare"

China's approach to this domain extends far beyond traditional propaganda. People's Liberation Army (PLA) strategists conceptualize the "cognitive domain" as a distinct battlespace, on par with the physical domains of land, sea, air, space, and cyber.²⁹ Their objective is not merely to influence but to disrupt, change, or even usurp an adversary's entire decision-making process.³⁰ As articulated in PLA-affiliated writings and analyzed by experts like Elsa B. Kania, this doctrine of "cognitive warfare" involves the systematic leveraging of artificial intelligence (AI), big data, and a national strategy of military-civil fusion to target the cognitive processes of foreign populations and leaders.³¹ The ultimate goal is to achieve "mental/cognitive dominance" by manipulating perceptions, severing historical narra-

tives, and deconstructing national symbols to create and exploit cognitive vulnerabilities.³² Specialized units, such as PLA Base 311, are dedicated to executing the so-called “Three Warfares” of “Public Opinion Warfare, Psychological Warfare, and Legal Warfare” against specific targets like Taiwan.³³

THE ROLE OF AIR AND SPACE POWER IN THE COGNITIVE BATTLE

Air and space power must evolve to engage directly in this contested narrative space.

Truth-Telling and Counter-Disinformation: The high-fidelity, rapidly disseminated ISR data collected by air and space assets is a powerful tool for “truth-telling.” Releasing commercial satellite imagery that exposes the military nature of a supposedly civilian outpost or tracking data that refutes a false narrative about a maritime incident can directly counter adversary disinformation campaigns.³⁴

Enabling Information Access: Space-based assets can also play an offensive role in the cognitive domain. The proliferation of commercial satellite internet constellations, such as Starlink, presents an opportunity to bypass state-controlled firewalls and deliver uncensored information directly to populations within closed information ecosystems.³⁵ This capability represents a direct use of space assets for cognitive operations, challenging the narrative monopoly of authoritarian regimes.

This dynamic reveals an emergent operational cycle in modern conflict: space-based ISR collects vast amounts of data on an adversary society; AI processes this data to identify cognitive vulnerabilities and societal fissures; and information operations platforms deliver tailored messages to exploit those weaknesses. An effective U.S. gray zone strategy must therefore seek to disrupt this entire chain, not just the final narrative. This could involve using U.S. space capabilities to deny, degrade, or deceive an adversary’s own ISR collection, thereby

“starving” their cognitive warfare algorithms of the data they need to be effective.

INSTITUTIONAL ADAPTATION: A CASE FOR A JOINT GRAY ZONE OPERATIONS CELL

The complex, cross-domain nature of gray war demands more than mission-specific commands or domain-centric capabilities. While organizations like U.S. Cyber Command, Space Force deltas, and Air Force Special Operations Command play critical roles, their compartmentalized structures can hinder the timely and integrated responses required to counter adversaries who move fluidly across physical, cognitive, and virtual spaces.³⁶ Analysis from multiple strategic research institutions confirms that “organizational seams,” “fragmented governance,” and “divided statutory authority” are significant U.S. vulnerabilities in the gray zone.³⁷ Adversaries are aware of these gaps and deliberately exploit them.³⁸

To address these challenges, the creation of a Joint Gray Zone Operations Cell (JGZOC) is proposed: a small, cross-domain task force composed of representatives from air, space, cyber, intelligence, and information operations. This cell would not replace existing structures but would serve as an integrating node—much like Cold War fusion centers or the early Office of Strategic Services (OSS)—to synthesize signals, narratives, and operations in real time.³⁹ These earlier centers, such as the Defense Intelligence Agency’s Central America Joint Intelligence Team (CAJIT), brought together analysts from across the government to fuse strategic, operational, and tactical intelligence against persistent threats like the communist insurgency in El Salvador.⁴⁰ Trained for ambiguity and postured for forward influence, this team would provide agile, whole-of-government response options during the “long twilight” of strategic competition.

The call for such an integrated body is not a radical departure but a proven American response to shifts in the character of conflict. The OSS was created during World War II precisely because existing departments were incapable of integrating the unconventional intelligence, subversion, and psychological operations required for total war.⁴¹ Similarly, the formation of Joint Special Operations Command (JSOC) was a direct response to the inability of the separate services to effectively integrate for complex missions.⁴² The gray zone today presents a similar inflection point, demanding a similar institutional innovation. Barriers to such integration remain formidable—including inter-agency authorities, fiscal constraints, and cultural inertia—but the cost of inaction is a fragmented and ineffective response to a fused form of conflict.⁴³

STRATEGIC FORESIGHT: WARGAMING GRAY ZONE FUTURES

Effective preparation for gray war requires more than doctrinal clarity; it demands immersive experimentation. Wargaming, futures modeling, and scenario construction can reveal latent vulnerabilities, doctrinal blind spots, and the often counter-intuitive dynamics of gray zone crises.⁴⁴ The goal is not to predict the future but to make officers and planners more fluent in its grammar.⁴⁵

Recent wargames conducted by leading think tanks provide crucial lessons. A series of 20 crisis simulations run by the Center for Strategic and International Studies (CSIS), centered on a notional Chinese gray zone campaign against Taiwan’s Kinmen Islands, revealed a critical pathology in U.S. decision-making. In nearly every iteration, teams playing the United States opted to defer risk, choosing long-term, less confrontational responses like altering force posture or increasing military sales rather than responding directly to the immediate crisis. However, when the adversary’s pressure

continued in subsequent rounds, these same teams were statistically more likely to escalate dramatically. This phenomenon, termed “shadow risk,” highlights a dangerous dynamic where the desire to avoid short-term escalation inadvertently increases the appetite for risk and the potential for miscalculation in future disputes.⁴⁶

These simulations do more than test tactics; they expose the cognitive biases and institutional habits that can undermine effective U.S. responses. The consistent preference for de-escalation and risk deferral is not a failure of capability but a reflection of an institutional culture optimized for managing conventional crises, a culture that may be ill-suited to the persistent, attritional nature of gray zone competition. Other simulations, such as a structured game by the RAND Corporation examining Russian gray zone tactics in the Balkans and exercises by the Massachusetts Institute of Technology (MIT) and the Center for a New American Security (CNAS) on economic coercion, reinforce the need for integrated, whole-of-government planning that account for allied interests and the protracted timeline of these campaigns.⁴⁷

Future-facing scenarios must continue to push these boundaries, incorporating the convergence of intelligence, AI, and narrative. A plausible scenario could involve a coordinated influence and ISR disruption campaign against a U.S. base in the Pacific: Chinese satellites “shadow” allied military assets while state-aligned firms throttle local digital networks, and a viral disinformation campaign simultaneously stirs local protests.⁴⁸ Such a scenario forces planners to confront questions not of tactics alone, but of judgment under ambiguity. When does a cyber response become escalation? How long can forces remain on high alert before cognitive and logistical attrition sets in? These are the questions that wargames must explore to cultivate the mindset needed to adapt and win.

MASTERING THE GRAY ZONE

The contested space below the threshold of conventional war is no longer peripheral—it is now the principal arena of strategic competition. Gray war, when clearly defined, reveals a persistent operational environment where ambiguity is weaponized, narratives are contested, and influence can be more decisive than destruction. In this domain, traditional concepts of deterrence and escalation give way to more fluid metrics: shaping perceptions, disrupting adversary decision cycles, and sustaining positional advantage without triggering open conflict.

Air and space power, long optimized for decisive kinetic engagements, must evolve to meet the demands of this altered landscape. Platforms, posture, and doctrine must be reoriented toward persistent sensing, narrative agility, and non-kinetic effects. This requires not only new tools but new mindsets—ones that embrace tempo over mass, ambiguity over closure, and integration over domain parochialism.

Institutional adaptation will be slow unless catalyzed by operational demand and intellectual clarity. A dedicated cross-domain gray war cell—interlacing ISR, cyber, information operations, and space capabilities—offers a crucial starting point for bridging the bureaucratic seams that currently hinder a unified response. So too do wargames and future scenarios that test the edges of our assumptions, reveal doctrinal blind spots, and train leaders to navigate uncertainty with imagination and resolve. The gray zone is not a problem to be solved; it is a condition to be mastered. Those who shape its contours—technologically, cognitively, and strategically—will hold the initiative in the decades to come. **PRISM**

Notes

¹ Michael J. Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict* (Carlisle, PA: U.S. Army War College, Strategic Studies Institute, December 2015), <https://press.armywarcollege.edu/monographs/428/>.

² U.S. Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: U.S. Department of Defense, 2018), <https://media.defense.gov/2020/May/18/2002302061/-1/-1/1/2018-NATIONAL-DEFENSE-STRATEGY-SUMMARY.PDF>.

³ Richard D. Newton, “Air and Space Power in the Gray Zone,” *Irregular Warfare Initiative*, 2024, <https://irregularwarfare.org/articles/air-and-space-power-in-the-gray-zone/>.

⁴ See, for example, Joint Chiefs of Staff, *Irregular Warfare*, Joint Doctrine Note 1-22 (Washington, DC, March 22, 2022); and Frank G. Hoffman, *The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War* (Washington, DC: The Heritage Foundation, 2016), <https://www.heritage.org/sites/default/files/2019-10/2016-IndexOfUSMilitaryStrength-The%20Contemporary%20Spectrum%20of%20Conflict-Protracted%20Gray%20Zone%20Ambiguous%20and%20Hybrid%20Modes%20of%20War.pdf>.

⁵ Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, VA: Potomac Institute for Policy Studies, December 2007), https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.

⁶ Bastian Giegerich, “Hybrid Warfare and the Changing Character of Conflict,” *Connections: The Quarterly Journal* 15, no. 2 (2016): 77–83, https://connections-qj.org/system/files/download-count/15.2.05_giegerich_hybrid_warfare.pdf.

⁷ James Wither, “Making Sense of Hybrid Warfare,” *Connections* 15, no. 2 (2016): 64–72, <https://www.jstor.org/stable/26326441>.

⁸ Antulio J. Echevarria II, “Operating in the Gray Zone: An Alternative Paradigm for U.S. Military Strategy” (Carlisle, PA: U.S. Army War College, Strategic Studies Institute, April 2016), <https://apps.dtic.mil/sti/tr/pdf/AD1013691.pdf>.

⁹ Mazarr, *Mastering the Gray Zone*.

¹⁰ Hal Brands, “Paradoxes of the Gray Zone,” Foreign Policy Research Institute, February 5, 2016, <https://www.fpri.org/article/2016/02/paradoxes-gray-zone/>.

¹¹ Molly K. McKew, “Putin’s Real Long Game,” *Politico Magazine*, January 1, 2017, <https://www.politico.com/magazine/story/2017/01/putins-real-long-game-214589/>.

¹² George F. Kennan, “The Inauguration of Organized Political Warfare,” Policy Planning Staff memorandum, May 4, 1948, in *Foreign Relations of the United States, 1945–1950: Emergence of the Intelligence Establishment* (Washington, DC: U.S. Government Printing Office, 1996), document 269.

¹³ Gregory Mitrovich, *Undermining the Kremlin: America’s Strategy to Subvert the Soviet Bloc, 1947–1956* (Ithaca, NY: Cornell University Press, 2000), 16.

¹⁴ Todd J. Allison, “Deterrence in the Gray Zone: Old Theory to Counter New Strategies,” CIDP Policy Brief 4, no. 2 (Kingston, ON: Centre for International and Defence Policy, 2018), https://www.queensu.ca/cidp/sites/cidpwww/files/uploaded_files/4-2%20Spring18_PB_Allison_web.pdf.

¹⁵ Mazarr, *Mastering the Gray Zone*, 57.

¹⁶ Mazarr, *Mastering the Gray Zone*; Brands, “Paradoxes of the Gray Zone.”

¹⁷ Benjamin Jensen, “Shadow Risk: What Crisis Simulations Reveal about Deferring U.S. Responses to China’s Gray Zone Campaign against Taiwan,” CSIS Futures Lab, February 16, 2022, <https://www.csis.org/analysis/shadow-risk-what-crisis-simulations-reveal-about-dangers-deferring-us-responses-chinas>.

¹⁸ Julia Siegel, “Commercial Satellites Are on the Front Lines of War Today,” Atlantic Council, August 30, 2022, <https://www.atlanticcouncil.org/content-series/airpower-after-ukraine/commercial-satellites-are-on-the-front-lines-of-war-today-heres-what-this-means-for-the-future-of-warfare/>; Newton, “Air and Space Power in the Gray Zone.”

¹⁹ “B-1s Conduct Bomber Task Force Mission in South China Sea,” Pacific Air Forces, July 22, 2020, <https://www.pacaf.af.mil/News/Article-Display/Article/2284767/b-1s-conduct-bomber-task-force-mission-in-south-china-sea/>; “U.S., Allied aircraft fly together over Riga, Latvia – demonstrate readiness and unity,” U.S. Air Forces in Europe & Air Forces Africa, August 19, 2025, <https://www.afgsc.af.mil/News/Article-Display/Article/4278732/us-allied-aircraft-fly-together-over-riga-latvia-demonstrate-readiness-and-unity/>.

²⁰ “B-52 Conduct Missions Over the South China Sea, Indian Ocean,” U.S. Indo-Pacific Command, September 26, 2018, <https://www.pacom.mil/Media/News/News-Article-View/Article/1647101/b-52-conduct-missions-over-the-south-china-sea-indian-ocean/>.

²¹ “EA-37B Compass Call,” U.S. Air Force Fact Sheet, March 8, 2023, <https://www.af.mil/About-Us/Fact-Sheets/Display/Article/3320324/ea-37b-compass-call/>.

²² LHarris, “The EA-37B Compass Call: Delivering the Future of Electronic Warfare Today,” September 2024, <https://www.l3harris.com/newsroom/editorial/2024/09/ea-37b-compass-call-delivering-future-electronic-warfare-today>.

²³ BAE Systems, “Compass Call: Defense Against Electronic Attacks,” accessed October 15, 2025, <https://www.baesystems.com/en/product/compass-call>.

²⁴ “EA-37B Compass Call”; Jared Huerter and Dave Belinsky, quoted in “EC-37B Compass Call: US Air Force Prepares New Compass Call Platform and System,” *Journal of Electromagnetic Dominance*, February 21, 2023, <https://www.jedonline.com/2023/02/21/ec-37b-compass-call-us-air-force-prepares-new-compass-call-platform-and-system/>.

²⁵ Rachel S. Cohen, “‘Gray Zone’ Conflict Drives Space Weapons Development,” *Air & Space Forces Magazine*, March 30, 2020, <https://www.airandspaceforces.com/gray-zone-conflict-drives-space-weapons-development/>; “Satellite Jamming,” CSIS Aerospace Security Project, August 2019, <https://aerospace.csis.org/data/gps-jamming-in-the-arctic-circle/>.

²⁶ Paul Szymanski, “Techniques for Great Power Space War,” *Strategic Studies Quarterly* 13, no. 4 (Winter 2019): 79–90, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-13_Issue-4/SSQWinter2019.pdf; DeLaine Mayer, “Red Lines in Orbit: Deterrence, Sovereignty, and the Risk of Escalation in Space Conflict,” Modern War Institute at West Point, October 2025, <https://mwi.westpoint.edu/red-lines-in-orbit-deterrence-sovereignty-and-the-risk-of-escalation-in-space-conflict/>.

²⁷ “The Drone Renaissance: DIY Cyber ISR Drones,” LSEC, October 2025, <https://www.lsechub.com/blog/the-drone-renaissance-diy-cyber-isr-drones/>; “Heating up the Gray Zone: Drones over Germany,” *National Review*, October 5, 2025, <https://www.nationalreview.com/corner/heating-up-the-gray-zone-drones-over-germany/>.

²⁸ Todd W. Danko, Andreas Kellas, and Paul Yu Oh, “Robotic Rotorcraft and Perch-and-Stare: Sensing Landing Zones and Handling Obscurants” (paper, Drexel University, 2007), <https://ieeexplore.ieee.org/document/1507427>.

²⁹ Newton, “Air and Space Power in the Gray Zone.”

³⁰ Charles Davis, “Cognitive Warfare: China’s Effort to Ensure Information Advantage,” *Military Intelligence Professional Bulletin*, October–December 2022, <https://mipb.ikn.army.mil/media/dwzdignr/cognitive-warfare.pdf>.

¹¹ Kerry K. Gershaneck and Eric Chan, “Political Warfare against Intervention Forces,” *Journal of Indo-Pacific Affairs*, April 21, 2025, <https://www.airuniversity.af.edu/JIPA/Display/Article/4167178/political-warfare-against-intervention-forces/>.

¹² Elsa B. Kania, “The PLA’s Pursuit of Cognitive Warfare,” *China Brief* 20, no. 18 (Jamestown Foundation, October 8, 2020), https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-3/prism_8-3_Kania_82-101.pdf; “The Chinese Communist Party’s Military-Civil Fusion Policy,” U.S. Department of State, May 29, 2020, <https://2017-2021.state.gov/military-civil-fusion/>.

¹³ Elsa B. Kania, “Minds at War: China’s Pursuit of Military Advantage through Cognitive Science and Biotechnology,” *PRISM* 8, no. 3 (2020), https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-3/prism_8-3_Kania_82-101.pdf; Davis “Cognitive Warfare.”

¹⁴ Mark R. Cozad, “The Role of PLA Base 311 in Political Warfare against Taiwan (Part 3),” *Global Taiwan Brief*, February 15, 2017, <https://globaltaiwan.org/2017/02/the-role-of-pla-base-311-in-political-warfare-against-taiwan-part-3/>.

¹⁵ Jose M. Marcias III and Benjamin Jensen, “Signals in the Swarm: The Data Behind China’s Maritime Gray Zone Campaign Near Taiwan,” CSIS, October 8, 2025, <https://www.csis.org/analysis/signals-swarm-data-behind-chinas-maritime-gray-zone-campaign-near-taiwan>; Newton, “Air and Space Power in the Gray Zone.”

¹⁶ Siegel, “Commercial Satellites Are on the Front Lines of War Today.”

¹⁷ Newton, “Air and Space Power in the Gray Zone.”

¹⁸ Elizabeth G. Troeder, *A Whole-of-Government Approach to Gray Zone Warfare* (Carlisle, PA: U.S. Army War College Press, May 2019), <https://www.govinfo.gov/content/pkg/GOVPUB-D101-PURL-gpo130209/pdf/GOVPUB-D101-PURL-gpo130209.pdf>; John R. Schaus et al., “What Works in Countering Gray Zone Coercion,” CSIS, July 16, 2018; Jacob Andra, “Gray zone warfare part 2: Gray zone vulnerabilities and solutions,” Talbot West, November 8, 2024, <https://talbotwest.com/industries/defense/gray-zone-warfare/vulnerabilities-and-solutions>.

¹⁹ Michael C. McCarthy, Matthew A. Moyer, and Brett H. Venable, “Deterring Russia in the Gray Zone,” Joint Special Operations University Press, March 2019, <https://www.govinfo.gov/content/pkg/GOVPUB-D101-PURL-gpo125296/pdf/GOVPUB-D101-PURL-gpo125296.pdf>.

²⁰ Newton, “Air and Space Power in the Gray Zone.”

²¹ “DIA in the 1980s: The Agency Hits its Stride,”

Defense Intelligence Agency, May 26, 2022, <https://www.dia.mil/News-Features/Articles/Article-View/Article/3046720/dia-in-the-1980s-the-agency-hits-its-stride/>; E. A. Burkhalter, Jr., “Central America Joint Intelligence Team (CAJIT),” Memorandum for Director of Central Intelligence, July 18, 1983, CIA-RDP86B00269R000300020002-1, Central Intelligence Agency, https://www.cia.gov/readingroom/docs/DOC_0001361069.pdf.

²² “The Office of Strategic Services: America’s First Intelligence Agency,” Central Intelligence Agency, accessed January 5, 2026, <https://www.cia.gov/resources/csi/static/Office-of-Strategic-Services.pdf>; “Office of Strategic Services Established,” U.S. Army Intelligence Center of Excellence, June 13, 2022, <https://www.dvidshub.net/news/422791/office-strategic-services-established>.

²³ “JSOC: America’s Joint Special Operations Command,” Grey Dynamics, May 2025, <https://greydynamics.com/jsoc-americas-joint-special-operations-command/>.

²⁴ Newton, “Air and Space Power in the Gray Zone”; Lindsey R. Sheppard et al., “By Other Means Part II: Adapting to Compete in the Gray Zone,” CSIS, August 13, 2019, <https://www.csis.org/analysis/other-means-part-ii-adapting-compete-gray-zone>.

²⁵ Newton, “Air and Space Power in the Gray Zone.”

²⁶ Jensen, “Shadow Risk.”

²⁷ Jenny Oberholtzer et al., “Gaming Gray Zone Tactics, Design Considerations for a Structured Strategic Game” (Santa Monica, CA: RAND Corporation, 2019), https://www.rand.org/pubs/research_reports/RR2915.html; Eric Heginbotham and Jung Jae Kwon, “Deterring Chinese Economic Coercion of Taiwan: Lessons from an Economic Statecraft Simulation,” MIT Security Studies Program Wargaming Lab, 2024, <https://ssp.mit.edu/publications/2024/deterring-chinese-economic-coercion-of-taiwan>; Emily Jin, Emily Kilcrease, and Rachel Ziemba, “A Strategic Response to China’s Economic Coercion,” *The Diplomat*, referenced in “Sharper: Wargames,” CNAS, accessed October 2025, <https://www.cnas.org/publications/commentary/a-strategic-response-to-chinas-economic-coercion>; “Countering Coercion: Managing Chinese Gray Zone Activity in the South China Sea and Indian Ocean Region,” CNAS, March 29, 2024, <https://www.cnas.org/publications/reports/countering-coercion>.

²⁸ Newton, “Air and Space Power in the Gray Zone.”

Controlling Command

Is AI Capturing the Ethics of War?

Dr. James Giordano and Dr. Elise G. Annett

Capture [v]: (1) to take into one's possession or control by force; (2) to record, understand and/or express accurately; (3) to cause (data) to be stored in a computer or in a digital format.¹
(Oxford English Dictionary, 2025)

The integration of artificial intelligence (AI) with military operations is accelerating across global powers, including the United States, its allies, and competitor states such as China and Russia. AI's operational use in the military exists on a spectrum of autonomy, with varying degrees of human involvement across positional (in, on, or out of the loop), dimensional (which tasks are controlled), and temporal (when humans intervene) domains. This complexity disrupts traditional understandings of command and accountability. Current U.S. policy, such as Department of War (DOW) Directive 3000.09, mandates that autonomous systems operate under human authority and within defined legal and ethical bounds.² However, the rapid pace of AI development—and adversaries' less restrained deployment—call into question the adequacy of current frameworks.

This essay emphasizes that AI should complement, not replace, human judgment in military contexts. Ethical oversight must be embedded throughout AI design and deployment, ensuring that all decision-making remains accountable to human actors. AI is currently employed in roles that support human decision-making, autonomously control weapon systems, and conduct both kinetic and non-kinetic operations. While these capabilities offer significant advantages in speed, precision, and operational scale, they also introduce unprecedented ethical, legal, and strategic challenges—particularly as AI systems become increasingly autonomous. Systems that provide clear, explainable reasoning for their actions should be authorized for combat use. The

Dr. James Giordano is Head of the Center for Strategic Deterrence and Studies of Weapons of Mass Destruction; leads the Program in Disruptive Technology and Future Warfare of the Institute for National Strategic Studies (INSS) at the National Defense University (NDU), Washington, DC; and is Professor Emeritus of Neurology and Distinguished Scholar Emeritus of the CyberSMART Center at Georgetown University Medical Center, Washington, DC.

Dr. Elise G. Annett is a Research Fellow in the Program for Disruptive Technology and Future Warfare in INSS at NDU, Washington, DC. Her ongoing work addresses emerging operational issues arising from the use of iteratively autonomous generative, and agentic artificial intelligence and quantum systems in military applications.

Table 1. Roles and Functions of AI in Military Applications

AI Role	Function	Examples of Application	Operational Impact
Decision-Facilitating Element	Enhances human decision-making by providing real-time data analysis and recommendations	Target identification in drones, weapon system guidance	Improves accuracy, reduces decision latency, enhances situational awareness
Autonomous Command-and-Control	Directly controls systems or coordinates multiple assets without human intervention	AI-operated drone swarms, cyber operations, electronic warfare	Enables rapid, multi-domain effects; reduces human cognitive load; introduces new risk paradigms
Non-Kinetic Engagements	Executes cyber-attacks, electronic warfare, psychological operations	Disruption of enemy communication networks, misinformation campaigns	Expands battlefield to information domain; creates strategic asymmetry
Kinetic Engagements	Controls or assists in firing weapons, unmanned vehicles, or other physical systems	Autonomous missile targeting, robotic combat platforms	Accelerates kill chains; increases operational tempo; raises ethical and accountability challenges

Source: authors.

illusion of precision and neutrality in AI can mask moral disengagement and accelerate impunity as detached from human judgment. To mitigate these risks, we advocate for a framework that recognizes global diversity in values while establishing shared norms to guide responsible AI use.

THE USE OF AI IN MILITARY OPERATIONAL CONTEXTS

There is growing consideration and adoption of AI in the military operations of the United States (U.S.), its allies [e.g., United Kingdom, and several European Union (EU)], and competitor states such as China, Russia, North Korea and Iran.³ As illustrated in table 1, AI can be employed as decision-facilitating elements in control chains of other weapon systems (e.g., conventional weapons; drones/unmanned vehicles; non-conventional weaponry, etc.); and/or as a command-and-control (C2) system itself that can be deployed for disruptive or destructive effects in non-kinetic and/or kinetic engagements.

In both contexts, AI confers considerable speed, capability and power. To restate a perdurable proverb, with great power comes great responsibility. Accountability for such responsibility can become questionable if and as AI systems become iteratively autonomous.⁴ Indeed, current and proposed AI systems exist along a spectrum of autonomous functionality, which entails differential human involvement within various positional (i.e.- humans being “in”, “on”, or “out” of the proverbial “loop” of AI functions), dimensional (i.e.- differential engagement of humans in various aspects of particular functions) and temporal domains (i.e.- distinct periods of human involvement with certain aspects of AI function[s] – see table 2).

Thus, a simple definition of autonomy (viz. “independence;” “self-determinative capacity,” as applied to AI systems does little to disambiguate the type, extent, or domains of human engagement with AI actions; nor does it clarify whether, and to what degree, human involvement is necessary or appropriate).⁵ Autonomy denotes the experience of volition

Table 2. Domains of Human Involvement in Iteratively Autonomous AI Systems

Domain	Definition	Operational Impact & Accountability Challenges
Positional Control	The locus of human authority in AI decision loops, e.g., <i>In the Loop, On the Loop, Out of the Loop</i>	Variations in positional control directly affect command responsibility—from active oversight to full delegation. Autonomous systems operating <i>Out of the Loop</i> significantly increase risks of accountability gaps and unintended outcomes.
Dimensional Control	The depth and scope of human engagement across AI system functions (planning, targeting, execution, assessment)	Partial human involvement results in complex control environments that require clearly defined responsibility assignments and robust governance frameworks to manage operational and ethical risks.
Temporal Control	The timing and duration of human intervention throughout the AI lifecycle—from initialization to post-mission review	Periods without human oversight allow AI systems to act independently, creating accountability gaps that challenge existing command authority and ethical standards.

Source: authors.

and self-direction in cognition and action, anchored in the perception of being self-governed rather than externally driven.⁶ Within human-AI interactions, acknowledging this broader conception of autonomy sharpens an understanding of how humans relate to and are affected by autonomous systems.

Human autonomy is a multifaceted construct rooted in philosophical and ethical traditions. It entails self-rule, rational self-governance, and the authentic endorsement of one's values and desires, alongside the competencies required to critically reflect, make informed choices, and act freely without coercive influence.⁷ It also requires access to meaningful options and agency over how choices are made and enacted.

This distinction becomes particularly exigent when AI systems are deployed in kinetic or non-kinetic military operations. In contexts where autonomous systems may execute disruptive or destructive actions affecting both combatants and civilians, it is necessary to clearly define autonomy – and its limits – in operational, ethical, and legal terms. Conflating machine autonomy with human

autonomy risks assigning moral judgment to machine systems, thereby threatening regnant principles of human responsibility, and just war conduct. Ethically informed oversight remains imperative; human autonomy drives strategic decision-making, authorizes action, and ensures accountability in the deployment of autonomous systems.

CURRENT ETHICAL CONSIDERATIONS AND THEIR LIMITS

For U.S. military forces, DOW Directive 3000.09 provides a codified framework for the integration of autonomous systems across operational domains.⁸ It strengthens command authority, anchors systems to legal and ethical imperatives, and defines autonomy as an extension of human judgment that is rigorously accountable. Autonomy, in this context, functions through deliberate assignment, bounded by mission parameters, and validated through legal oversight. It operates within a structure where accountability is inherent, not optional. Despite several misconceptions, this directive yokes

operational law and strategic design, ensuring that autonomous capabilities serve as force multipliers under human-defined constraints. The clarity of its principles, however, reaches full effect only through disciplined implementation. Strategic impact emerges through alignment—policy, posture, and platform operating as a unified construct under real-world conditions. Drafting sets the direction; execution drives dominion.

Yet, in this regard, “appropriate human judgment” can remain somewhat ambiguous in practical, operational terms. We argue that in this context, human judgment cannot be abstract; it must be situated. But this prompts questions of: Who exercises it? When? Under what conditions? With what awareness of the system’s behavior, constraints, and failure modes? As adversaries design decision-dominant systems, U.S. debate remains somewhat bounded by rhetorical cycles that delay the deployment of readiness. China presents a case study in contrast.⁹ Its behavior in global AI diplomacy illustrates a deliberate departure from collective restraint. Notably, in 2024 November, China refrained from signing a non-binding declaration advocating for human control over nuclear weapons decisions.¹⁰ This action suggests a preference for maintaining autonomy in military AI development, particularly in areas not directly addressed by international agreements. So, while the U.S. deliberates over ethical baselines, China codes for operational asymmetry.¹¹ It leverages state-aligned AI development to optimize deniability, resilience, and tempo.

We believe that this divergence requires a recalibration of U.S. strategic posture. Advanced platforms must be met with doctrinal authority. The idea of keeping a human somewhere proximal to affect “the loop” essential to engaging human judgment in system architecture, ethical reasoning at execution parameters, and ethical-legal accountability embedded in system design. In this context,

a synthesized command and control, which we term as *SYNTHComm* emerges as a conceptual framework that emphasizes augmented, distributed human-machine communication loops capable of sustaining responsible command authority in accelerated operational environments.¹² As Michael Horowitz has recently argued, insisting on real-time human intervention during algorithmic engagement compresses capability into irrelevance. Decision latency becomes strategic liability.¹³ Indeed, such developments incite inquiry to what extent AI is controlling command. Does this represent a mere convenience of using AI for more detailed data-based informing of human decisions; a reliance upon AI to comprehend the rules of engagement and their execution in real-world settings; or a surrender to the decisional capacity of the AI? Thus, we must also ask—and address—what AI’s “capture” of command entails and obtains?

THE IMPLICATIONS OF MORE DETACHED VIOLENCE

AI is no longer just a tool for gaining tactical advantage; rather, it represents a paradigm shift that establishes impunity in warfare. A possible impact of AI command and control systems lies in their capability for faster, more detached, and less accountable forms of violence.¹⁴ This evolution demands a fortified architecture of responsibility and unambiguous attributability. We opine that a structure that binds human decision-makers to the operational consequences of the AI systems they empower is necessary in this domain, as accountability cannot diffuse across code, complexity, or computational speed. By embedding AI into military decision-making, an illusion of precision is created that can undermine deliberation, moral judgment, and human restraint—the essential elements of ethical command.

The term “autonomous assistance” is a misnomer, masking what may well be a disturbing

truth: Decision-making is now being ceded to code. Allowing AI to recommend — or even execute — lethal force without meaningful human oversight, represents an abdication of moral responsibility.¹⁵ AI calculates probabilities, executes patterns, and makes decisions at machine speed — without human ethical pause. It is important to ask whether, and/or to what extent autonomous AI systems will “handicap” (i.e.- slow) the speed of their decisional processing to enable moderation by human users situated somewhere in the command-and-control chain. Velocity of decision-making alone cannot justify authority.

Therefore, AI is becoming an actor in systems of control, influence, and execution.¹⁶ In light of this, we argue that accountability must reside in the human domain, for without insistence upon clear, enforceable human command and accountability, this represents a surrender of human authority. We concur with William Casebeer’s proposition for the possibility and value of “moral AI.”¹⁷ Yet here too, the responsibility for action, and burden of consequence must remain firmly within the human dimension. Anything less is impunity under the guise of innovation. As Casebeer notes, it will be important to instill moral precepts within military AI systems; and extant iterations of ethics for military AI, as detailed in DOW Directive 3000.09, may certainly provide a basis for these parameters. Such encoding confers a “builders’ bias” to the system that grounds the relative discrimination of “right” and “wrong” action to some definable construct of “good” established by those (humans) who develop and program the AI.¹⁸ Thus, attribution of any “wrongs” exercised by the AI could be levied upon the human entity of its creation. And should an AI system deviate from these established parameters, such variance with its programmed human intent must be demonstrated, and even then, question could — and we believe should — arise as to why the system was not constructed to “fail safe.”

TOWARD A MORE COMPREHENSIVE-AND COSMOPOLITAN-ETHICAL CODEX

But perhaps the larger issue rests upon the relativist nature of morality and ethics, writ large. Paraphrasing moral philosopher Alasdair MacIntyre, it becomes critical to ask, “what good; which rationality?”¹⁹ Fundamentally, this harkens Cicero’s prudential query, *cui bono; cui malo?* (who benefits; who is harmed?).²⁰ If the goal of military AI ethics is to deter uses in practice that violate some defined norms of bellicose conduct, then any realistic view of deterrence must appreciate that the priority of states’ interest is preservation of their established set of “goods” and values. Given this reality, it’s reasonable to question whether a common morality for military AI, akin to that proposed by ethicist Bernard Gert might be viable to instantiate Casebeer’s conception of moral AI.²¹ Gert’s common moral constructs, which in the main directly and/or indirectly proscribe infliction of basic harms, if modified to prohibit machine systems from causing such harms to humans (absent direct human command and control) might be likened to the fictional “robot rules” espoused by Isaac Asimov.²² We feel that there is appreciable value to science-fictional accounts serving as morality plays for real-world scenarios, but if, and only if monitored and bounded by recurrent reality checks.²³ In this case, realistic deterrence demands recognition of, and response to the fact that different nations maintain differing values, which must be appropriated within any calculus of capabilities and constraints that can be determined and governed for emergent technology such as AI.

Further, we recognize that machine system versus machine system engagements represent a possible artifact of the proscription of machine vs human engagement(s). However, even in these

scenarios, regard must be rendered for human cost and toll. Machine-based and -enacted conflicts may be more readily tolerable, easier to start, harder to stop, and rapidly escalatory.²⁴ As well, it may be that in some cases, technology may be more valued than human capital. Irrespective of the relative valuation of technology or humanity that may spur intensification of engagement, any such escalation can—and likely will—incur human burden, if not harms as the effects of machine system destructions incur increasingly destabilizing manifestations within human ecologies (e.g., network disablement, infrastructure damage, resource and services’ degradation/loss, etc.). Indubitably, these manifestations will impact the quality of human life and may cause human mortality “downrange” consequential to disruption of public health. Thus, any genuinely pragmatic posturing toward an ethics of military AI must regard and incorporate a valuation of deterring, mitigating, or preventing these human costs.

Therefore, rather than espousing a common morality, we have advocated an approach to ethical oversight, guidance, and exercise of military AI that (1) situates and maintains human values and agency at various positions within and upon the loop of AI capabilities and actions; (2) appreciates and engages variance(s) in those values; and (3) employs a process of reflective equilibrium that remains fixed upon primacy of purpose – as determined by consensus through multinational convention; and flexible to adapt to changes in technology, socio-politics, and domains and dimensions of power balance.²⁵

Operationally, this framework translates into enforceable mechanisms. Human agency remains concrete, embedded in defined nodes of decision and control, with AI actions of consequence routed through traceable human authorization. Layers of human review accompany critical system actions, ensuring accountability is distributed across the chain of command. Continuous test, evaluation,

verification, and validation (TEVV) incorporates human judgment at each stage, with real-time monitoring that identifies drift, bias, or misalignment. Decisions, authorizations, and system triggers are logged in forensic telemetry to make accountability granular, transparent, and unambiguous. Multinational oversight structures operate to audit, enforce, and adjudicate adherence to shared norms, ensuring that the reflective equilibrium of human values extends beyond theory into AI deployment. In this environment, speed, complexity, or autonomy does not diffuse responsibility; it reinforces the need for precision, clarity, and enforceable ethical and operational standards.²⁶ The core issue is the sacrifice of humanity in warfare to the golem of machine-based military efficiency, war loses its last ethical scaffolding when machine systems dictate the calculus of life and death, and humans merely rubber-stamp these decisions. We concur with Wehrey and Bonney that AI accelerates impunity, and we note that a greater risk is the erasure of accountability itself.²⁷

The key task is ensuring ethical oversight in an era increasingly defined by AI in warfare. While regional regulation is a crucial starting point, the issue extends to the core of modern conflict. Real-time targeting, surveillance, and rapid-response systems are driven by algorithms that operate faster than human decision-making. The challenge—and we believe opportunity—is embedding ethical reasoning and responsible command structures into these systems to maintain human agency, accountability, and restraint in the battlespace. To prevail, the United States must confront acceleration with decisiveness. It must match adversarial systems with coherent integration and lead through command that is both principled and prepared.

RECOMMENDATIONS

Navigating the ethical challenges posed by military AI requires urgent clarity. All AI systems that pro-

pose or execute lethal force ought to adhere to strict standards of explainability. This requires robust auditability: full logging of decision processes, traceable model provenance, and periodic review by independent human-auditors capable of dissecting system outputs. Explainable AI in the military domain has been explicitly identified as critical, since opacity undermines traceability and the ability to ascribe responsibility.²⁸ Explicability is non-negotiable: any system unable to clearly demonstrate how it reaches decisions must be excluded from operational command. Decisions involving lethal force demand transparent judgment accountable through human responsibility, not obscured behind algorithmic complexity.

Furthermore, AI should serve to complement, not replace, human judgment. Human oversight should remain essential to all final decisions involving lethal force. AI technologies can enhance recommendation and operational effectiveness, but ultimate authority, accountability, and moral responsibility must remain firmly in human hands.

Moreover, the creation and use of military AI systems should occur under an ethical framework that, fosters a comprehensive and globally enforceable regulations. Such regulations should uphold shared ethical standards, mandate legal adherence, and ensure human agency remains central to every decision-making process. These guidelines are essential to prevent technology from diminishing or obscuring human culpability. Lastly, given the rapid advancement and widespread deployment of AI technologies, these recommendations require immediate attention. Regional powers and multinational forums must act decisively and ethically to govern military AI, or risk becoming governed by it. Thus, the true question facing us is not whether we can control AI, but whether we will actively choose to do so. **PRISM**

Notes

¹ Oxford University Press, *Oxford English Dictionary*, s.v. “Capture,” 2025, <https://www.oed.com/>.

² U.S. Department of War (DOW). DOW Directive 3000.09 „Autonomy in Weapon Systems.” 25 January 2023.

³ Kelley M. Saylor, *Artificial Intelligence and National Security* (Washington, DC: Congressional Research Service, 2020); Vincent Boulanin et al., *Artificial Intelligence, Strategic Stability and Nuclear Risk*, SIPRI Policy Paper No. 53 (Stockholm: Stockholm International Peace Research Institute, 2020); Becca Wasser and Josh Wallin, “Build Allied AI, or Risk Fighting Alone,” *Foreign Policy*, 2025.

⁴ William J. Tyler, Anusha Advikottu, et al., “Neurotechnology for Enhancing Human Operation of Robotic and Semi-Autonomous Systems,” *Frontiers in Robotics and AI* 12 (2025), <https://doi.org/10.3389/frobot.2025.1491494>.

⁵ Oxford University Press, *Oxford English Dictionary*, s.v. “Autonomy,” 2025, <https://www.oed.com/>.

⁶ Paul Formosa, “Robot Autonomy vs. Human Autonomy: Social Robots, Artificial Intelligence (AI), and the Nature of Autonomy,” *Minds and Machines* 31, no. 4 (2021): 595–616; Ilse Verdiesen, Filippo Santoni de Sio, and Virginia Dignum, “Accountability and Control over Autonomous Weapon Systems: A Framework for Comprehensive Human Oversight,” *Minds and Machines* 31, no. 1 (2021): 137–63.

⁷ Formosa, “Robot Autonomy vs. Human Autonomy.”

⁸ Department of Defense, *DoD Directive 3000.09*, Department of Defense, *DoD Directive 3000.09: Autonomy in Weapon Systems* (Washington, DC: Department of Defense, 2023).

⁹ Elsa Kania and Ian B. McCaslin, *Learning Warfare from the Laboratory: China’s Progression in Wargaming and Opposing Force Training* (Washington, DC: Institute for the Study of War, 2021), <https://www.understandingwar.org/report/learning-warfare-laboratory-china%E2%80%99s-progression-wargaming-and-opposing-force-training>.

¹⁰ Jarrett Renshaw and Trevor Hunnicutt, “Biden, Xi Agree That Humans, Not AI, Should Control Nuclear Arms,” *Reuters*, November 16, 2024, <https://www.reuters.com/world/biden-xi-agreed-that-humans-not-ai-should-control-nuclear-weapons-white-house-2024-11-16/>.

¹¹ Roy D. Kamphausen, ed., *China’s Military Decision-Making in Times of Crisis and Conflict* (Seattle: The National Bureau of Asian Research, 2023), <https://www.nbr.org/publication/chinas-military-decision-making-in-times-of-crisis-and-conflict/>.

¹² Elise Annett and James Giordano, “AI versus AI: Human Engagement via Synthesized Command (SYNTHComm) in AI Warfare,” *HDIAC Journal* 10, no. 1 (2026): forthcoming Spring 2026.

¹³ Michael C. Horowitz, “Autonomous Weapon Systems: No Human-in-the-Loop Required, and Other Myths Dispelled,” *War on the Rocks*, May 2025, <https://warontherocks.com/2025/05/autonomous-weapon-systems-no-human-in-the-loop-required-and-other-myths-dispelled/>.

¹⁴ Yvonne R. Masakowski, “Ethical Constraints and Contexts of Artificial Intelligence in Biomedical Applications for Public Health and Safety, National Security, and Defense Operations,” in *Artificial Intelligence and Global Security: Future Trends, Threats and Considerations*, ed. Yvonne Masakowski (London: Emerald Press, 2020), 1–34; Pauline S. Kaurin and Casey T. Hart, “Ethical Constraints and Contexts of Artificial Intelligence in Biomedical Applications for Public Health and Safety, National Security, and Defense Operations,” in *Artificial Intelligence and Global Security: Future Trends, Threats and Considerations*, ed. Yvonne Masakowski (London: Emerald Press, 2020), 121–136.

¹⁵ Bartłomiej Chomanski, “A Moral Bind? — Autonomous Weapons, Moral Responsibility, and Institutional Reality,” *Philosophy & Technology* 36, no. 1 (2023): Article 41, <https://doi.org/10.1007/s13347-023-00647-2>.

¹⁶ John R. Shook, Tamas Solymosi, and James Giordano, “Ethical Constraints and Contexts of Artificial Intelligence in Biomedical Applications for Public Health and Safety, National Security, and Defense Operations,” in *Artificial Intelligence and Global Security: Future Trends, Threats and Considerations*, ed. Yvonne Masakowski (London: Emerald Press, 2020), 137–52.

¹⁷ William D. Casebeer, “Building an Artificial Conscience: Prospects for Morally Autonomous Artificial Intelligence,” in *Artificial Intelligence and Global Security: Future Trends, Threats and Considerations*, ed. Yvonne Masakowski (London: Emerald Press, 2020), 81–94

¹⁸ Department of Defense, *DoD Directive 3000.09* (2012); Department of Defense, *DoD Directive 3000.09* (2023).

¹⁹ Alasdair MacIntyre, *Whose Justice? Which Rationality?* (Notre Dame, IN: University of Notre Dame Press, 1988), <https://doi.org/10.2307/j.ctv1bvnf11>.

²⁰ Marcus Tullius Cicero, *The Basic Works of Cicero* (New York: Modern Library, 1951).

²¹ Bernard Gert, Charles M. Culver, and K. Danner Clouser, *Bioethics: A Systematic Approach*, 2nd ed. (Oxford: Oxford University Press, 2006)

²² Isaac Asimov, *I, Robot* (New York: Gnome Press, 1950).

²³ Rachel Wurzman, David Yaden, and James Giordano, “Neuroscience Fiction as Eidolá: Social Reflection and Neuroethical Obligations in Depictions of Neuroscience in Film,” *Cambridge Quarterly of Healthcare Ethics* 26, no. 2 (2017): 292–312.

²⁴ James Giordano, “Opening the Replicator Program’s Pandora’s Box,” *National Defense Magazine*, 2023; Daniel Howlader and James Giordano, “Advanced Robotics: Changing the Nature of War and Thresholds and Tolerance for Conflict—Implications for Research and Policy,” *The Journal of Philosophy, Science & Law* 13, no. 2 (2013): 1–19.

²⁵ Shook, Solymosi, and Giordano, “Ethical Constraints and Contexts of Artificial Intelligence.”

²⁶ I. Bode, A. Nadibaidze, T. Watts, et al., “Ensuring the Exercise of Human Agency in AI-Based Military Systems: Concerns across the Lifecycle,” *Ethics and Information Technology* 27 (2025): Article 50, <https://doi.org/10.1007/s10676-025-09861-2>.

²⁷ Frederic Wehrey and Andrew Bonney, “The Middle East’s AI Warfare Laboratory,” *War on the Rocks*, April 28, 2025, <https://warontherocks.com/2025/04/the-middle-east-ai-warfare-laboratory/>.

²⁸ I. Bode et al., “Ensuring the Exercise of Human Agency in AI-Based Military Systems: Concerns Across the Lifecycle,” *Ethics and Information Technology* 27 (2025): art. 50, <https://doi.org/10.1007/s10676-025-09861-2>.

Preparing for Future Wars

Incongruent Beliefs on Autonomous Weapons

By MAJ Nelson R. Godbolt, Dr. Craig Douglas Albert, Dr. Lance Y. Hunter, and Dr. Jeffrey Morris

Significant debate has been brewing within the literature on the Revolution in Military Affairs (RMA) regarding the potential of lethal autonomous weapons systems (LAWS) waging wars mostly independent from human input in future warfare. Some authors suggest there is a high probability of autonomous robots replacing the soldier, whereas others argue that LAWS will likely only serve as a force multiplier rather than replacing human soldiers.¹ As Pekarev notes, “armed forces worldwide are developing, using and integrating new technology to gain military superiority. It is believed that AI (artificial intelligence), robotics, and autonomous systems will impact future armed conflicts. Still, the precise consequences of the deployment of autonomous systems in the military decision-making are still unclear.”²

Russia and Ukraine are deploying Unmanned Ground Vehicles (UGVs) against each other in Ukraine, but they are ineffective, and we maintain will remain so until they transition from what we call Lethal semi-Autonomous Weapons Systems (LSAWS) into fully autonomous LAWS.³ Electromagnetic Warfare (EW) is one of the primary reasons why these efforts will remain ineffective. While public reports suggest that both Russia and Ukraine are utilizing strategies like frequency agility and fiber optic cables to enhance the effectiveness of airborne drones, these measures mitigate the impact of EW on communications through the electromagnetic spectrum (EMS). However, they do not restore the assured communications that the United States has become accustomed to in its wars in the Middle East. Consequently, a technical problem caused

Nelson R. Godbolt (Major) is an Army Soldier with 14 years in service and a student in Augusta University’s Master of Arts in Intelligence and Security Studies program.

Craig Douglas Albert, Ph.D., is a professor of Political Science at Augusta University. He is the graduate director of National Defense Studies programs, including the Master of Arts in Intelligence and Security Studies, and the PhD in Intelligence, Defense, and Cybersecurity Policy.

Lance Y. Hunter, Ph.D., is a professor of Political Science at Augusta University located in Augusta, Georgia. He received his PhD in 2011 from Texas Tech University.

Jeffrey Morris, Ph.D., is an assistant professor in the School of Computer and Cyber Sciences at Augusta University. He is a retired Army Soldier with over 35 years of experience in the combat arms, military intelligence, and cyber branches, with several combat tours.

by the loss of assured communications due to EW will force the U.S. and other nations to confront the moral issue of adopting LAWS.

Currently, the United States is committed to having “a human responsible for the use of force,” (i.e., LSAWS and not LAWS).⁴ True, fully autonomous LAWS have not been fielded, but when they are, will require minimal human input beyond initial programming and then a mission to conduct. With the aforementioned in mind, this paper asks the question, “are LAWS the future of armed conflict?” Although a large-scale war may not be fought with fully autonomous LAWS in the next one to two years, we argue that future wars being waged by LAWS, which are designed to operate without continuous or reliable human input, is a likely scenario in the long-term. Armed conflict is moving towards autonomous “robot wars.” If not robot wars, then certainly hybrid wars in which LAWS are used in an increasing manner. To demonstrate the infeasibility of human-controlled LSAWS, this article reviews some proposed constraints on LSAWS and LAWS in general, and the plethora of issues with these constraints. As explored later, we will investigate under what conditions it may be possible that a human is completely out of the loop in the use of force during the potential transition to fully autonomous LAWS.

A central issue is that many nations will be hesitant to adopt LAWS, but the technical requirements of LSAWS versus an EW-equipped adversary will force nations to make an uncomfortable decision to ensure the performance of their weapons. The considerations of fielding an inadequate LSAWS weapon system vulnerable to EW and thus risking service members’ lives, the threat of technologically falling behind an adversary, and an increased perception of threat, such as continued Russian aggression in Ukraine and against Europe, will be weighed against the moral concerns of relegating the use of force to a computer program. Nations have often prioritized effective weapons over collateral damage concerns,

and we believe that LAWS will be used in a conflict prior to any treaty banning them. Before delving too deeply into the subject, some definitional precision is needed regarding LAWS.

We define fully autonomous LAWS as those systems that “select and apply force to targets without human intervention.”⁵ This conceptualization is slightly modified by Bhattacharjee (2024), who writes that LAWS “are military platforms that use AI to autonomously locate and engage targets without human intervention.”⁶ In layman’s terms, the software decides when to strike a target, drop a munition, or kill a human being without human input or an assured ability to override the act. These systems are not science fiction, and there are concerns that the first use of a LAWS may have already occurred in 2021.⁷ Bhattacharjee notes, “LAWS are autonomous weapons systems that, once activated, are either entirely or almost entirely free of human control.”⁸ LAWS are not confined to ground or aerial vehicles and operate in all warfighting domains under various names: Unmanned Aircraft Systems; Unmanned Ground Systems (UGV); Unmanned Maritime Systems; Unmanned Aerospace Systems (UAV); and in the cyberspace domain, Self-acting Software.⁹

For clarity in this paper, the term LSAWS delineates systems where a human can stop a pending use of force or must make the decision to use force whereas LAWS does not entail either criterion.

This paper contributes to the security studies and military science literature by arguing that large-scale operations between militaries using LAWS with minimal human interference are highly probable for future warfare. The paper proceeds through six main sections. Firstly, we illustrate how unmanned vehicles, and autonomous and semi-autonomous LAWS operate, including the constraints under which they operate. Next, the paper describes how the proposed constraints on unmanned vehicles and LSAWS are vulnerable to EW. Third, the

paper discusses the U.S. Army’s EW gap. Fourth, we illustrate how LSAWS operate when humans are “in the loop.” Fifth, the paper explains how previous weapons conventions and arms control treaties limiting other military technologies might limit LAWS technology. Finally, we conclude with a discussion of policy implications for the United States.

CONSTRAINTS ON LETHAL AUTONOMOUS WEAPONS SYSTEMS

Within the context of LAWS, the Department of War (DOW) and academia propose three general categories to constrain these systems. The first is the human-in-the loop where LSAWS “only engage individual targets or specific target groups that have been selected by a human operator.”¹⁰ This means a human must select a target and “click” yes, every time before force is applied, and the command is then transmitted to the LSAWS where it then follows its programming to deliver force. The second category is human-on-the loop where LSAWS are “autonomous weapon systems, in which operators can monitor and halt a weapon’s target engagement.”¹¹ This means a human needs to be able to constantly monitor and send an abort command to the LSAWS at any time. The third category is human-out-of-the-loop operations, in which the machine has complete control, there is no communication between the human and the system, and thus, there is no human intervention.¹² This paper groups LSAWS with human-in/on-the-loop and LAWS with human-out-of-the-loop.

There are many other constraints, such as cyber security requirements, but none as foundational as the human on/in the loop.¹³ These constraints work under some scenarios but could also create vulnerabilities. Table 1 describes in more detail what is meant by the human loop, using the current U.S. “self-driving” car evolution as an example.

Levels 1 and 2 are comparable to humans-in-the loop. The system assists the operator with target selection, weaponeering, etc., but the human directs the car. Levels 3 and 4 are comparable to humans-on-the-loop. With Level 3, the system does the job but still requires human assistance in complex situations. Level 4 is the ideal situation for humans-on-the-loop control, but it has safety parameters disabling the “weapon system” if faced with a complex situation. Levels 1-4 are all comparable to LSAWS. Level 5 is comparable to LAWS, with the car simply being told where to go while the human rides inside as a passenger. Some Level 4 vehicles exist in limited capacities, such as taxis in pilot cities, but Level 5 vehicles are only being prototyped.¹⁴ Time remains to adjust policy before LAWS are developed and adopted, though a crisis or conflict could rapidly compress the timeline. Unfortunately, designing a car to navigate roads has far fewer considerations than the application of deadly force. The following section addresses why issues may arise using LSAWS.

VULNERABILITY TO ELECTROMAGNETIC WARFARE

A major issue with both humans-in or on-the-loop constraints that enable LSAWS is the requirement for reliable and continuous communication. Unreliable communications could be a driving issue forcing nations away from LSAWS and to LAWS. However, the LSAWS communication requirement is a vulnerability when the adversary is EW-capable. How useful is a weapon that renders itself inert when communications are cut versus one that can continue to operate in a communications-denied environment? The LSAWS requirement for assured communications may force nations to shift to LAWS, despite their moral desire to retain firm control over the use of force. One must understand what EW is and how it is being applied in current conflicts to grasp the issues facing direct human

Table 1. Taxonomy of road vehicle automation derived from SAE (2016a).

Level of Automation	Automated driving system operational function		Human Driver operational function	
	Control:	Capability	Operational function	Capability
Level 1 (most functions are controlled by driver)	Control: Lateral and longitudinal	In some driving modes	Localization Perception Planning Management	In all driving modes
Level 2 (at least one driver assistance system is automated)	Control: Lateral and longitudinal	In some driving modes	Localization Perception Planning Management	In all driving modes
Level 3 (driver is able to shift safety-critical functions to vehicle)	Control: Lateral and longitudinal Localization Perception Planning	In some driving modes	Management	In all driving modes
Level 4 (fully-autonomous, but not in every driving scenario)	Control: Lateral and longitudinal Localization Perception Planning Management	In some driving modes	n/a	n/a
Level 5 (fully-autonomous, vehicle's performance is equal that of human driver in every driving scenario)	Control: Lateral and longitudinal Localization Perception Planning Management	In some driving modes	n/a	n/a

(See reference from Source: Table from Faisal, Asif, Md Kamruzzaman, Tan Yigitcanlar, and Graham Currie. "Understanding Autonomous Vehicles: A Systematic Literature Review on Capability, Impact, Planning and Policy." *Journal of Transport and Land Use* 12, no. 1 (2019): 49. <https://www.jstor.org/stable/26911258>.)

control of distant weapon systems. The U.S. Army's *Field Manual 3-12: Cyberspace Operations and Electromagnetic Warfare* defines EW as "military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum [EMS] or to attack the enemy."¹⁵ Winning in the EMS ensures friendly forces can use the EMS for command-and-control activities and deny the enemy from using the EMS to its advantage.

Unfortunately, the U.S. weapons procurement seems to have ignored this facet of warfare. Russian

EW equipment has been able to target U.S. equipment provided to Ukraine. This has disrupted or made targets of U.S.-provided communications equipment, rendered U.S. precision munitions ineffective, and affected NATO-provided drones.¹⁶ Essentially, the effectiveness of EW in the Russia Ukraine war against U.S. or NATO equipment indicates that it will be able to impact future equipment such as LSAWS.

EW is comprised of three main subcomponents with multiple subdisciplines under each. First is

Electromagnetic Attack (EA), often referred to as jamming. It is defined as “the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires,” one of the warfighting functions.¹⁷ EA can be offensive, such as jamming enemy communications, or defensive, such as jamming Global Positioning Systems (GPS) to prevent precision-guided munitions (PGMs) from striking friendly forces. Satellite jammers are a form of offensive EA and provide non-lethal deterrence options.¹⁸ Israel’s jamming of GPS to degrade looming Iranian strikes in the spring of 2024 was an example of defensive EA.¹⁹ Ukraine and Russia conducting EA on UAVs, communications, and radar is both defensive and offensive.²⁰

Second, Electromagnetic Support (ES) is defined as “actions tasked by, or under the direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for immediate threat recognition, targeting, planning, and conduct of future operations.”²¹ ES simply identifies a likely enemy signal and provides a tactical understanding of the battlefield. An example is a U.S. Army retransmission site being geolocated by an adversary’s EW. The adversary knows that this site is constantly broadcasting and is either a command-and-control center or a retransmission site due to its continuous broadcasting. Either way, it is likely to receive lethal targeting in short order.²²

Finally, Electromagnetic Protection (EP) is defined as “actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability.”²³ Examples include designing equipment to be compatible, using terrain to hide signatures,

and altering communications plans to avoid enemy ES and EA. The application for the front-line user is best summed up as counter-enemy EW, since they are altering their communications or transmitting while masked by terrain to protect against enemy ES and EA. Military personnel and contractors design the equipment currently in use and organize how friendly forces are using the electromagnetic spectrum.²⁴

The 21st century’s first large ground war with Russia and Ukraine showed that simple communications can lead to being rapidly and lethally targeted.²⁵ As Col. Liam Collins writes, “An enemy unmanned aerial vehicle monitors the cellphone signals of troops below, identifies their location and sends the coordinates to a headquarters, which launches an artillery strike against the unsuspecting troops.”²⁶ Col. Collins continues, “This is the capability Russia brings to the ongoing conflict in eastern Ukraine’s Donbas region.”²⁷ Perhaps even more famously, Russia was able to target GPS application signals intercepted from Ukraine. Riehle (2024) writes that in 2014, Ukraine began using an application to calculate artillery targeting data.²⁸ He notes, “However, the [Russia’s Main Directorate] GU successfully infected the application with malware that allowed the GU to receive the targeting information that the Ukrainian forces were developing. The GU infiltration of the targeting application led both to the geolocation of Ukrainian artillery for counterbattery strikes and to the foreknowledge of Ukrainian strikes to allow Russian units to relocate.”²⁹ With the aforementioned examples, it is well-known that nation-state adversaries will contest U.S. communications with EW, and counter-adversary EW is a top priority for the Secretary of the Army.³⁰ Unfortunately, the U.S. is coming out of 20 years of fighting in an environment where communications were minimally contested. As a result, the backend support for U.S. Army ground-based EW systems is not currently available or effective.³¹

The transition to a contested EMS is a difficult one to manage. In the Russia-Ukraine war, both sides are in a constant race to communicate safely and reliably while preventing the enemy's communication.³² Much of the prevention fight is to ensure modulation is correct, that is, the jamming matches the enemy's communication signal. This is one of the key aspects of effective jamming, and the resources of nation-states are competing against each other with constant wins and losses on either side in the EMS. Ukraine's shifting to Starlink from traditional communications is an outsized adaptation that the Russians were not prepared for and are still trying to field EW equipment that can affect it.³³ The U.S. should not assume that it will always be able to outsmart an adversary and design a signal like Starlink that is un-jammable, and AI-enabled EW will probably be key to denying advanced communication.³⁴ Adversaries will react to U.S. capabilities in the EMS, which is highlighted by the ability of Russians to effectively target Ukrainians equipped with well-known U.S. communications systems and their profile in the EMS.

The current Russia-Ukraine war highlights the required agility in the EMS. One side will develop a new way to control a drone and within two weeks the other side's EW will adapt and begin to degrade it. Within three months, EW can completely degrade the once-reliable means of communication.³⁵ This also indicates that a robust, nation-state level of support may be required to enable basic communication and to ensure that EW can be effective against adversaries. The innovation trend continues, with scholars noting that Israel had robust counter-drone technology on October 7th, 2023, but that it was not designed to operate against the drones Hamas used.³⁶

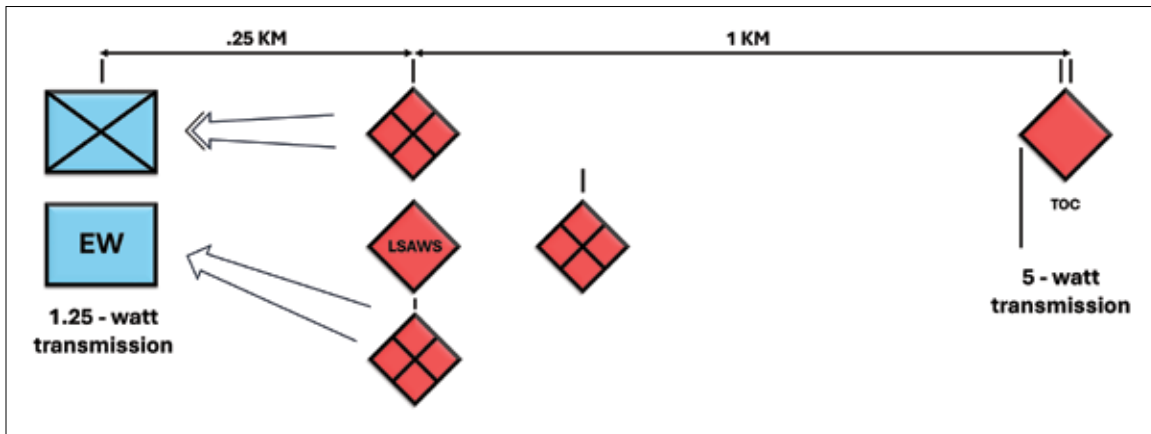
Jamming is simple considering communications from a control station to a LSAWS. It considers the distance from the transmitter to receiver versus the distance from the jammer to the receiver, the

power being broadcasted, and being able to match the frequency. If the LSAWS and the control station are extremely close and the jammer is far away, the jammer must overcome the tyranny of distance and free space loss to drown out the control signal at the receiver. The inverse is true if the control station is far away, and the transmitter is close. LSAWS jamming possibilities are explained in detail by Bhamidipati and Gao (2019) who write, "However, due to low signal power, the GPS signals are vulnerable to jamming attacks. A jammer broadcasts high power signals in the GPS frequency band and causes the receiver to lose track of satellites, due to which the navigation solution can no longer be computed by the receivers."³⁷

To dive deeper into why assured communications to/from LSAWS are infeasible, the math behind jamming must be explored. The formula that calculates the minimum power needed to effectively jam a signal is " $P_j = P_t \times K \times (H_t/H_j)^2 \times (D_j/D_t)^n$."³⁸ P_j is the minimum jammer power required, and P_t is the power output of the enemy transmission in watts. H_t/H_j are the height in meters above sea level of the enemy transmitter and the jammer. K is FM tuning accuracy, and n is the terrain conductivity factor. D_j is the distance from the jammer location to the target receiver, and D_t is the enemy transmitter to the enemy receiver distance.³⁹

Figure 1 provides an example of an adversary battalion attacking a U.S. company which highlights UGV's weaknesses to EW. The adversary has LSAWS that are being controlled from their Battalion Tactical Operations Center (TOC), and the U.S. company has EW support embedded. K , n , and (H_t/H_j) equal 1, making the formula: $P_j = P_t \times (D_j/D_t)$. The maximum transmission power of 5 watts of the common Harris 152 tactical radio is used for P_t since matching the power of a common transmission would help obscure the control station.⁴⁰ The D_t is assumed to be at 1km, just outside of most dismantled direct fire. The location of the jammer

Figure 1. This figure demonstrates the watt power needed for jamming enemy LSAWS.



Source: authors.

is assumed to be with the formation being attacked by LSAWS, so D_j is .25km at the initial engagement in a forested environment so $P_j = 5w \times (.25km/1km)$. The power required to prevent constant communication with the LSAWS is 1.25w. This means that an antenna powered by AA batteries could prevent assured communication to the LSAWS if it matched the modularity (which would likely require processing capacity and its associated power requirements).

This has significant tactical ramifications. To ensure reliable and continuous communication a U.S. control station must a) be very close to the LSAWS or b) transmit at a very high power.⁴¹ The war in Ukraine demonstrates the ability to target formations based on their EMS use, so a control station near a front line constantly receiving and broadcasting becomes a high-priority target and is prosecuted by jamming or lethal means.⁴² A similar situation occurs if the control station is at a distance and broadcasting with a higher power. The requirement for assured communications places LSAWS at a disadvantage because they must be in constant communication to enable “human-in-the-loop,” revealing the LSAWS of control station to EW.

The closer the LSAWS are to the front line, the greater the chance that EW is an effective counter

because they are further from their human-in-the-loop and closer to enemy EW assets. If a U.S. control station is placed outside the range of a Russian rocket artillery BM-30, it has 130 kilometers to transmit across. This means that .01w is required to jam the signal under ideal circumstances for LSAWS control. Heavily congested terrain (e.g., forested, urban, etc.) only helps the enemy jammer and degrades the ability to control LSAWS due to signal attenuation. The requirements to communicate and the opposing EW ensure that LSAWS are not feasible in future warfare when nation-states collide, regardless of distance.

LSAWS will have varying success when considering proxies or irregular warfare, but EW use by irregular forces faces two issues. First, the innovation cycle mentioned above, with the technical support required for EW to be effective. Second, the density of required EW equipment for successful coverage. In the Russian Ukrainian war, the Russian forces’ EW equipment is now spread throughout their entire formation. Arguably, hundreds of systems in a brigade with man-portable systems blanket the front lines, with more sophisticated systems positioned farther back.⁴³ Fielding, maintaining, and updating these EW systems would be

difficult for a proxy or irregular force to do routinely. However, as Hamas demonstrated on October 7th, 2023, an irregular force can achieve surprise for brief periods.

THE U.S. ARMY'S EW GAP

The U.S. Army is not well-positioned to understand these constraints. Its EW branch was established less than a decade ago, and there is no common EA or ES equipment fielded to U.S. formations.⁴⁴ 2nd Brigade Combat Team, 10th Mountain recently returned from the Middle East where they were targeted by over one hundred one-way attack drones.⁴⁵ Most of their EW systems were not effective, and in an open-source interview, the commanding officer of the unit detailed how EW simply did not work against the drone attacks.⁴⁶ There may have been some mitigating issues, such as the inability to jam GPS due to civil concerns, but the overall performance of U.S. EW against drones was poor.⁴⁷ The fact that the Army highlighted the counter-drone failings on its West Point-affiliated publication and Podcast is an indicator that it understands there is a serious problem.⁴⁸ Essentially, the Army is simply not prepared to fight with EW or against an enemy with EW. This is understandably so, with the Army rebuilding its EW capability after decommissioning it in the 1990s.⁴⁹ The Army still has not fielded “Program of Record” equipment to its EW soldiers as of 2024, for conducting jamming or geolocation, with the force relying instead on quick reaction force equipment.⁵⁰

This means that the Army cannot effectively train the whole organization on EW with its lack of equipment and nascent understanding of the problem set as a bureaucratic organization. The commandant of the Maneuver Center of Excellence detailed efforts to introduce EW training to infantry and armor basic training in 2024, and at the same conference, current Russian EW use was discussed.⁵¹ Simply put, the U.S. Army is behind. As Frost,

McClung, and Walls write, “The current mode of Army EW operations will not achieve even a limited window of tactical advantage.”⁵² The authors continue, “Our Army’s continued heavy reliance on devices and digital systems operating within the EMS will be our downfall if we do not recognize and work to mitigate our vulnerabilities, and our techniques for operating in a contested environment.”⁵³

If the West fully analyzes adversary EW capabilities against friendly communications capabilities, it will have to admit that assured communications are unlikely in large-scale war. Without the leg of assured communications, LSAWS are infeasible. The West will need to weigh its moral concerns against military effectiveness and adversary LAWS development and may be forced to overlook the moral concerns and adopt LAWS. This would create multiple competing requirements and a precarious situation for developers and those who implement LAWS. The cybersecurity of LAWS would be world-class, as the DOW requires it already, and the political pressure for the system to be flawless would be a requirement in Western democracies.⁵⁴ Unfortunately, the opposing pressures such as program cost and human error, among others, could undermine the system and lead to a scenario where the flawless success of LAWS includes luck. If a similar mistake to the recent 2024 CrowdStrike software glitch, that disrupted travel and banking globally, occurred in a DOW software update during conflict and LAWS killed civilians or U.S. service members, would the U.S. populace allow LAWS to continue?⁵⁵ Simultaneously, would the U.S. populace allow the DOW to field unreliable weapons systems that risk service members’ lives? The public and political backlash over ineffective U.S. body armor and the U.S.’s refusal to ban anti-personal land mines indicate that civilian casualties may be more palatable.⁵⁶

Americans are already wary of driverless cars, so a public pivot to LAWS is unlikely. The U.S. will probably slowly lurch towards LAWS and a lack

of a ‘human on/in the loop’ in multiple ways.⁵⁷ Geofencing, time constraints, and periodic data dumps for review when communications are viable, are all plausible ways to still cling to “there is human oversight,” but the U.S. is more likely headed towards ‘humans-out-of-the-loop’ and LAWS. The LAWS of the future, operating against an adversary using EW will, despite these constraints, not operate under the current DOW policy. The first time a U.S. LAWS destroys an adversary unit; it will be morally different than striking an entire apartment block with a missile strike launched by humans. The LAWS cannot feel compassion or other emotions that may inhibit violence, which leads to the question of who is accountable if a LAWS commits a war crime.⁵⁸ The U.S., unless in an existential conflict, could face internal pressure to cease LAWS development; academic literature is already rife with articles calling for regulation or a ban.⁵⁹ As an example, a training accident occurring with a nascent LAWS in development, combined with foreign influence operations, could easily sway popular perceptions. Conversely, constraining LAWS to the point where they did not employ lethal force to protect U.S. service members could cause a political backlash like the public criticism of U.S. forces’ “Rules of Engagement” in Afghanistan.⁶⁰ Nevertheless, there are many future pressures driving militaries towards LAWS.

Casualty sensitivity is present in modern democracies with presidential candidates sparring over military casualties and the advent of the “Dover Test” (i.e., are Americans willing to accept casualties for a military action).⁶¹ Historians have highlighted Western democracies’ ability to overcome casualty sensitivity, where “‘The Supreme Sacrifice’ was to dominate literature, speeches, sermons... the casualty lists that a later generation was to find so horrifying was considered ... not an indication of military incompetence, but a measure of national resolve.”⁶² The horrors of World War One (WWI)

and the subsequent improvements in media, such as satellite TV (with decreased or hamstrung efforts to censor), created an environment where casualties can have an outsized political or social impact compared to that of historical wars. For example, scholars of the Vietnam-era have argued that “cumulative casualties is the best predictor of war-time opinion.”⁶³

Authoritarian regimes are also experiencing societal complexity. In 2022, the People’s Republic of China’s (PRC) population peaked but has since started a 50 to 100-year decline.⁶⁴ The demographic makeup of the decline has significant impacts. Currently, the PRC has ~49 dependents per 100 working-aged people. The best- and worst-case scenarios estimate an increase to 83.8 or 158.0, respectively, per 100 by the year 2100. Regardless of whether the state feeds and shelters the dependents or if it is left to working-age relatives, it is projected to consume 23-30% of China’s GDP and generate social pressure on the Chinese Communist Party to create an environment where care can be provided.⁶⁵ Conducting a two-to-three-week war over Taiwan risks a minimum of tens of thousands of PRC soldiers dead, potentially further driving up this ratio.⁶⁶ Imagine a family with eight grandparents in their 70s, four parents in their 50s, and one 20-year-old son who died on the beaches of Taiwan. The parents cannot conceive again after investing in their child’s upbringing, have a 2-to-1 dependent-to-working age ratio, lose a future caregiver, and the state loses a future revenue source. Holistically, in a skewed working-age to non-workers situation, younger generation casualties in a conflict scenario have lasting impacts on countries with poor demographics and weak immigration. An example of this is Japan’s “Lost Decades” when demographics shifted older, and the economy and population size shrank.⁶⁷ The countries in, or about to be in, population decline include Russia, Iran, North Korea, and others.⁶⁸ The impacts of demographics on warfare are noticeable

in Ukraine, a country in an existential conflict, with their front-line soldier's average age being 45 while younger men are not drafted in order to protect that generation.⁶⁹ As of 2024, the average volunteer for the Russian military is over the age of 50.⁷⁰ Whether an autocratic country seeking to maintain social order, or a Western democracy sensitive to casualties, most major world powers are facing pressures to reduce casualties. The demographic crisis of an aging population is an issue where a conflict could drastically worsen population replacement. LAWS provides a potential way to mitigate the issue.

LETHAL AUTONOMOUS SYSTEMS WITHOUT A HUMAN-IN-THE-LOOP

Since LSAWS humans-in/on-the-loop systems are not feasible for the next large-scale war with adequately EW-equipped belligerents, this paper proposes several ways states could progress toward LAWS. First, LAWS aimed at naval or airborne targets may pave the way from a target prosecution standpoint. Second, they could be developed as a deterrent after one power implements them. Third, the conflict would need to be existential for Western democracies to transition at a wide scale (autocracies are not under this constraint). Fourth, a heightened great power competition between China and the U.S. may push the world toward LAWS. We elaborate below.

First, warships, fighters, and bombers have distinct signatures. The future B-21 Raider or current B-2 Spirit bomber is unique. A B-2 Spirit is 52.12 meters across, 5.1 meters high, and can fly at high subsonic speeds for thousands of miles with four General Electric F118-GE-100 engines.⁷¹ This is significantly different from a Boeing 777 carrying passengers around the world with its two engines, 64.8-meter length, and 18.6-meter height.⁷² For another comparison, an F-35 Fighter has one engine with 10.7-meter width.⁷³ A simple function

to confirm the target matches a hostile aircraft's physical specification with an electro-optical sensor is required. If it does not match a target, then the LAWS can render itself inert and dive as an example. This is just an example of target identification, but there are many options to confirm aerial and maritime targets.⁷⁴

The development of loitering munitions or surface-to-air missile (SAM) complexes that choose which targets to engage and destroy could degrade an opposing nation's air power without risking U.S. lives or inflicting civilian casualties. The same set of characteristics apply to naval vessels. While countries could explore dual-use systems (i.e., use a civilian fishing vessel to carry anti-ship cruise missiles), countries have a lengthy history of then targeting these types of assets.⁷⁵ Additionally, major military powers have invested significantly in standard military hardware such as cruisers or fighter aircraft that are much more capable than dual-use systems. LAWS will likely be designed to degrade and destroy these high-end systems, possibly leaving the decision to apply force against dual-use systems to humans or human-in/on-the-loop systems.

The application of LAWS designed for ground combat is trickier and comes at a cost. Currently, Ukrainian and Russian first-person view drones (FPVs) are inexpensive compared to their targets, but their use and battlefield countermeasures are nascent.⁷⁶ A Javelin missile system costs ~\$250,000.⁷⁷ One can assume that an autonomous system that can differentiate targets and decide when and where to apply a quarter of a million-dollar munition would be expensive. This expense is compounded by a LAWS' ability to select targets. Differentiating a T-72 tank from an Abrams tank is a plausible task, but distinguishing between a dismounted friend, foe, and civilian is a significantly more complex problem. Lab-based programming would undoubtedly fail to accurately account for all the decisions made regarding when to apply force. Consider the

CrowdStrike catastrophe of 2024, where a worldwide leader in cybersecurity conducted multiple stress tests but still had a multi-billion-dollar software failure.⁷⁸ Expense would be an issue if true target discernment is a hard requirement. Comparing the U.S.'s efforts to avoid collateral damage in Afghanistan and Iraq over the last 30 years to the Russia Ukraine war, U.S. LAWS will face stringent requirements and costs to prevent civilian casualties, while Russia can focus on friend vs. foe and force application. The impact of monetary cost on the battlefield is uncertain, but the cost difference between U.S. LAWS and those of authoritarian regimes will exist. It is worth considering in this scenario where the comparative advantage lies.

Second, if an adversary invests in ground combat-focused LAWS, then a deterrent is required. LAWS deterrents could take many forms. The U.S. Space Force's Chief of Space Operations said, "Satellites don't have mothers," and this applies to LAWS as well.⁷⁹ Tactics and weapons systems that could be employed against LAWS are not constrained by the suffering they inflict or other moral considerations. There are several deterrence options available against LAWS such as nuclear weapons, Electromagnetic Pulses (EMPs), and offensive cyber weapons that the U.S. is currently hesitant to employ and/or develop. The 2017 National Security Strategy implies the right to respond kinetically to any cyberattack against the United States.⁸⁰ In the same vein, all tools necessary should be on the table as deterrents to LAWS. The 2022 Nuclear Posture Review states, "While the United States maintains a very high bar for the employment of nuclear weapons, our nuclear posture is intended to complicate an adversary's entire decision calculus, including whether to instigate a crisis, initiate armed conflict, conduct strategic attacks using non-nuclear capabilities."⁸¹ Adding verbiage that specifies LAWS-centric armies as a possible target is a feasible option. There is a plethora of other options across the whole of

government from degrading LAWS supply chain critical components or the software of LAWS. If armies become more robotic as Gen. (retired) Milley predicts, then investing in EMPs may bear fruit.⁸² Whatever the response, U.S. LAWS development and implementation as a response to adversary LAWS will be a policy consideration for leaders to manage in the 21st century.

Thirdly, a serious conflict, or threat of it, is required for LAWS to be utilized on a mass scale. Providing a tactical advantage in war or reducing casualties alone could inspire most countries to use them, but the moral arguments against LAWS may preclude their adoption by Western democracies. A legitimate threat of war is required for these countries to embrace their own LAWS. Toppling a second-rate power and receiving casualties as the U.S. did in Iraq in 2003 did not reach this threshold. The U.S. continued the Iraq War and then Afghanistan while reasonably adhering to the Law of Armed Conflict (LOAC) and while taking statistically low casualties (partially due to its belief that it would succeed.)⁸³ A direct conflict with a global power creating significant casualties or a threat to a nation's existence could drive any state towards more indiscriminate weapons, as shown by Russia, Germany, and the U.S.' pursuit of nuclear weapons in the 1940s or with the pending withdrawal from the Ottawa Treaty by several Western nations concerned with Russian aggression.⁸⁴

Finally, a great power competition could drive LAWS development. This is different from the deterrence perspective of the West versus the Soviet arms race in the 20th century. During the Cold War both sides developed thousands more nuclear weapons than required to render each other unable to win a war.⁸⁵ The U.S. had 31,255 nuclear warheads in 1967 at the height of the arms race, which was far more than required to destroy the USSR. The U.S. has since reduced its nuclear arsenal, and since 2010 has just maintained ~3,750 warheads (or an 88%

reduction).⁸⁶ While nuclear arms treaties and de-proliferation efforts are positive developments since the 1950s, applying existing treaties to LAWS regulation has not panned out.⁸⁷ What does this mean for great power competition? Currently, the West and various authoritarian regimes compete for dominance, with the U.S. and the PRC leading the way, especially in the realm of information warfare and artificial intelligence.⁸⁸ Both are investing heavily in research and development across multiple areas to the tune of hundreds of billions of dollars.⁸⁹ American views on China have deteriorated in the past two decades, with a significant majority of citizens now holding unfavorable opinions of the country.⁹⁰ The PRC's focus on EW endangers any human-on/in-the-loop proposals. The U.S. Secretary of the Navy Carlos Del Toros stated, "The People's Liberation Army is also pursuing a strategy to develop, test, field, and integrate... electronic, and information warfare capabilities, posing potential challenges to how we operate across the spectrum."⁹¹ The PRC already fielded EW equipment down to its Army's tactical echelons, causing the U.S. Army to scramble to catch up.⁹² If the U.S. enters an arms race as it did with the Soviet Union, human-in/on-the-loop systems are already hindered, and the human cost of a war with the PRC would be substantial. Thus, the U.S. is nudged towards LAWS development regardless of the cost or common sense.

Gen. (retired) Mark Milley, the 20th U.S. Chairman of the Joint Chiefs of Staff, made a prediction in 2024 that a significant portion of the U.S. Army, possibly a third, could be robotic within the next 10 to 15 years.⁹³ If robotics become commonplace and the pressures to minimize casualties intensify, converting Army robotics to LAWS becomes a software update and armament issue in a crisis. Without a crisis, a LAWS-capable adversary likely compels the U.S. to amend its policy to allow for a LAWS buildup. Regardless of the circumstances, the likelihood of a conflict involving

significant LAWS utilization is increasing. If LAWS can successfully discriminate and destroy maritime and airborne targets in a conflict, an adversary country implements LAWS, a large-scale war erupts between advanced nations, or if the ongoing great power competition between China and the U.S. continues, widespread development and implementation of LAWS will follow. This could lead to a conflict akin to WWI, where political and military leaders were cognizant of the horrors they were unleashing, but future generations condemned the conflict as abhorrent and took measures to prevent such a conflict from ever occurring again.⁹⁴

WEAPONS CONVENTIONS AND ARMS CONTROL TREATIES

The Geneva Conventions required hundreds of years, and millions of deaths, to be developed and implemented.⁹⁵ Biological, chemical, and nuclear weapons, as well as the indiscriminate killing of prisoners and civilians, were only prohibited after their use. Unfortunately, for humanity to fully embrace a ban on LAWS, it needs to experiment with its new weapons first. UN efforts to regulate LAWS have stalled.⁹⁶ Reducing a war's casualties is an admirable goal, but wars do not happen on ideal battlefields and inflicting casualties on the opposing side can contribute to the end of the conflict. A LAWS capable of selectively engaging targets in testing may be ill-prepared to differentiate targets in a metropolis under siege, where civilians are unable to flee. Current conflicts are characterized by a significant number of civilian casualties, some of which are deliberate war crimes, while others are accidental and a consequence of large-scale war in urban environments. LAWS could easily cause as much harm. If Russian one-way-attack drones were to become autonomous, avoiding civilian casualties would likely be a secondary priority in programming, and the systems would retain their explosive capabilities for targeting.

One only needs to observe the Russia-Ukraine war to find strategies that lead to indiscriminate uses of force. The Russian's claims of adhering to international law during the Ukraine war with "precision" munitions have repeatedly been proven false.⁹⁷ Russia predominantly utilizes massed artillery strikes or imprecise weapons in civilian areas.⁹⁸ Russian and PRC conventional militaries are designed primarily for mass warfare, although they are less mass-oriented than in the 1980s and 1990s.⁹⁹ Recently, scholars have noted Russia's reliance on massed infantry tactics even after taking 315,000 injuries or deaths, indicating Russia will continue to be more "mass" oriented than the U.S. in the foreseeable future.¹⁰⁰ Russia's historical conduct during previous wars likely informs their future approach to LAWS programming and should give any policymaker pause. The "mass" oriented forces from militaries with a pattern of excess collateral damage will lead to excess human suffering. If a child picks up a weapon, are they a combatant or does that equal hostile intent? This is difficult for a human to decide when present, let alone programming a LAWS for the same situation. Add on a political system that does not prioritize precision or target discrimination like Russia, and it is a human catastrophe in the making.

The approach of U.S. adversaries to land warfare also suggests that LAWS suits their way of war. The U.S. Army tries to instill disciplined initiative, mission command, and a trusted and competent Officer and NCO corps, meaning that the U.S. encourages junior leaders to take charge when faced with uncertainty and adapt to situations found on the battlefield. The U.S. relies on a volunteer military force, tries to retain experienced members, and designs its formation and weapons systems to preserve U.S. life. Russia and China do not follow this paradigm. The war in Ukraine has shown that Russia "focused on following orders, even if they were no longer appropriate."¹⁰¹ Russia conscripts

convicts and ethnic minorities, barely trains them, and sends them into combat, with horrific casualties, the predictable result.¹⁰² Analysis of the PLA highlights a tendency to, "elevate all problems to the center and a corresponding reluctance to devolve decision-making authority to lower levels."¹⁰³ Russia, with its poorly programmed and cheaper LAWS, would likely find them advantageous. Losing a poorly trained and ill-equipped conscript due to friendly fire or civilian casualties would not be significant obstacles for them. In contrast, the U.S. would need a much more sophisticated system to replicate its human force's fighting capabilities and minimize collateral damage.

Aside from the possible civilian casualties, other broad security implications for U.S. and international security are grim. Does conventional deterrence work if a country plans to expend its entire LAWS inventory before risking a person? What if or when the Allied coalition invaded after an extensive air campaign, thousands of LAWS fought until being destroyed instead of surrendering en masse like the Iraqi Army in the first Gulf War? The U.S. Army lost 148 soldiers to enemy fire, but replacing the ~69,000 Iraqis who surrendered in the Gulf War with LAWS would have increased the number of U.S. casualties.¹⁰⁴ Considering both Russia and Ukraine's persistent expansions of conscription, having a substantial LAWS inventory and believing a country can win an initial conflict makes war more likely in the 21st century if LAWS are adopted wholesale.¹⁰⁵ Does LAWS adoption tip the scales in a conventional war if only one side has them? The answers are unknown, but imagining North Korea or Iran with LAWS leads to an unenviable problem-set for Western leaders. This is all worthy of future research, which the present authors are currently engaged in.

DISCUSSION AND U.S. POLICY RECOMMENDATIONS

LAWS presents a perplexing dilemma: adopt LAWS and eliminate human intervention in lethal force applications, resulting in adversaries facing lopsided casualties; or, as humanity failed to do with nuclear, chemical, and biological weapons, ban these systems before they can be deployed. While the U.S. specifies it will have a human-on or in-the-loop, the driving factors of degraded communications due to EW, causality sensitivity, LAWS capability to target military assets with specific target profiles, deterrence against adversaries developing LAWS, and great power competition and conflict are all pushing the U.S. towards LAWS development. We believe that this will result in an overall erosion of deterrence, based on one key assumption: the less likely the loss of a service member's life, the more likely the use of force is authorized. Even if both sides have LAWS and the situation escalates, one could then assume both powers would conduct reprisal attacks on unmanned facilities, opening avenues for accidental escalation.¹⁰⁶

Current treaties and international norms are not equipped to address LAWS, a situation that mirrors the challenges posed from using cyber weapons.¹⁰⁷ Therefore, there may be similarities between the two. Unfortunately, efforts to create LAWS treaties are stalled, and there is no foreseeable near-term breakthrough as countries speed toward actual LAWS development.¹⁰⁸ The *Tallinn Manual on the International Law Applicable to Cyber Operations* (Tallinn Manual) will be updated to version 3.0 in the near future.¹⁰⁹ It may provide some insight into spurring movement on creating applicable law and treaties even though international consensus supports the supposition that at least one cyber weapon, known as Stuxnet, has been successfully used to destroy a target.¹¹⁰ The stagnant efforts at regulation will likely lead to a conflict

where LAWS operate outside the current definition of human-controlled systems. This creates a conflict scenario that LOAC and other international norms are ill-equipped to manage.¹¹¹ **PRISM**

Notes

¹ Michael Zequeira, "Artificial Intelligence as a Combat Multiplier: Using AI to Unburden Army Staffs," *Military Review* (Online Exclusive, September 2024), <https://www.armyupress.army.mil/journals/military-review/online-exclusive/2024-ole/ai-combat-multiplier/>.

² Janar Pekarev, "Attitudes of Military Personnel Towards Unmanned Ground Vehicles (UGV): A Study of In-Depth Interview," *Discover Artificial Intelligence* 3, no. 24 (2023): <https://doi.org/10.1007/s44163-023-00058-4>.

³ Matt Burgess, "Robots Are Fighting Robots in Russia's War in Ukraine," *Wired*, January 30, 2024, <https://www.wired.com/story/robots-are-fighting-robots-in-russias-war-in-ukraine/>.

⁴ Kathleen H. Hicks, "Remarks by Deputy Secretary of Defense Kathleen H. Hicks on 'The State of AI in the Department of Defense,'" *Department of Defense*, November 2, 2023, <https://www.defense.gov/News/Speeches/Speech/Article/3578046/remarks-by-deputy-secretary-of-defense-kathleen-h-hicks-on-the-state-of-ai-in-t/>.

⁵ Davison, Neil, and Knut Sverre, "Towards A Movement Position on Autonomous Weapon Systems," *International Red Cross*, 2022, <https://rcrcconference.org/blog/towards-a-movement-position-on-autonomous-weapons/>.

⁶ Sandeep Bhattacharjee, "Lethal Autonomous Weapons Systems (LAWS)," *Journal of Defence Studies* 18, no. 2 (April–June 2024): 49, 58, <https://ssrn.com/abstract=4952206>.

⁷ Bode, Ingvild, Hendrik Huelss, Anna Nadibaidze, Guo Qiao-Franco, and Tom F. Watts, "Prospects for the Global Governance of Autonomous Weapons: Comparing Chinese, Russian, and US Practices," *Ethics and Information Technology* (2023): 1–15, <https://doi.org/10.1007/s10676-023-09678-x>.

⁸ Sandeep Bhattacharjee, "Lethal Autonomous Weapons Systems (LAWS)," *Journal of Defence Studies* 18, no. 2 (April–June 2024): 49, 58, https://idsa.in/wp-content/uploads/2024/08/18-2_Sandeep-Bhattacharjee-04.pdf.

- ⁹ Zahradníček, Pavel, Luděk Rak, Jan Nohel, and Bedřich Rýznar, “Combat Unmanned Ground Vehicles: Perspectives for Implementation into Operational Application,” *Security & Future* 5, no. 3 (2021): 108–111, <https://stumejournals.com/journals/confsec/2021/3/108.full.pdf>.
- ¹⁰ Kelley Saylor, “Congressional Research Service,” February 1, 2024, <https://crsreports.congress.gov/product/pdf/IF/IF11150>.
- ¹¹ Saylor, “Congressional Research Service.”
- ¹² Jacopo Scipione, “The Lethal Autonomous Weapons Systems: A Concrete Example of AI’s Presence in the Military Environment,” *CSI Review* (2021), https://www.researchgate.net/publication/351100004_The_Lethal_Autonomous_Weapons_Systems_A_concrete_example_of_AI%27s_presence_in_the_military_environment.
- ¹³ Office of the Under Secretary of Defense for Policy, “DOD Directive 3000.09 Autonomy in Weapon Systems,” January 25, 2023, <https://media.defense.gov/2023/Jan/25/2003149928/-1/-1/0/DOD-DIRECTIVE-3000.09-AUTONOMY-IN-WEAPON-SYSTEMS.PDF>.
- ¹⁴ John Bogna, “Is Your Car Autonomous? The 6 Levels of Self-Driving Explained,” *PCMag*, June 14, 2022, <https://www.pcmag.com/how-to/6-levels-of-autonomous-self-driving-explained>.
- ¹⁵ US Army, “FM 3-12 Cyberspace Operations and Electromagnetic Warfare,” Washington, DC: US Army, 2021.
- ¹⁶ Jack Watling, *The Arms of the Future*, (London: Royal United Services Institute, 2024), p. 178; Watling, Jack, and Nick Sylvia, *Competitive Electronic Warfare in Modern Land Operations*, London: Royal United Services Institute, 2025, 1–38.
- ¹⁷ U.S. Army, “FM 3-12 Cyberspace Operations and Electromagnetic Warfare,” 2021.
- ¹⁸ Benjamin S. Lambeth, “On Space Control and Space Force Application,” In *Mastering the Ultimate High Ground: Next Steps in the Military Uses of Space*, 111, (Santa Monica, CA: RAND Corporation, 2003), https://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/MR1649.pdf.
- ¹⁹ Christopher Swope, Kaitlyn A. Bingen, Mark Young, Michael Chang, Samuel Songer, and Joseph Tammelleo, “Space Threat Assessment 2024,” *Center for Strategic and International Studies*, 2024, 29, <https://www.csis.org/analysis/space-threat-assessment-2024>.
- ²⁰ B. Vile, (2024, 09 11), Brigadier General, Deputy Director of U.S. Cyber Command Future Operations, (N. Godbolt, Interviewer).
- ²¹ U.S. Army, “FM 3-12 Cyberspace Operations and Electromagnetic Warfare,” 2021, Glossary-5.
- ²² B. Vile, (2024, 09 11), Brigadier General, Deputy Director of US Cyber Command Future Operations, (N. Godbolt, Interviewer).
- ²³ U.S. Army, “FM 3-12 Cyberspace Operations and Electromagnetic Warfare,” 2021, Glossary-4.
- ²⁴ T. Boudreau, (2024, 9 11), Deputy Commandant, United States Army Cyber and Electromagnetic Warfare School, (N. Godbolt, Interviewer).
- ²⁵ B. Vile, (2024, 09 11), Brigadier General, Deputy Director of US Cyber Command Future Operations, (N. Godbolt, Interviewer).
- ²⁶ Liam Collins, “Russia Gives Lessons in Electronic Warfare,” *Association of the United States Army*, July 26, 2018, <https://www.ousa.org/articles/russia-gives-lessons-electronic-warfare>.
- ²⁷ Collins, “Russia Gives Lessons in Electronic Warfare.”
- ²⁸ Kevin Riehle, “The Ukraine War and the Shift in Russian Intelligence Priorities,” *Intelligence and National Security* 39, no. 3 (2024): 460, <https://doi.org/10.1080/02684527.2024.2322807>.
- ²⁹ Riehle, “The Ukraine War and the Shift in Russian Intelligence Priorities,” 460.
- ³⁰ John. R. Hoehn, “Defense Primer: Electronic Warfare,” *Congressional Research Service*, November 14, 2022, <https://crsreports.congress.gov/product/pdf/IF/IF11118>.
- ³¹ Ferguson, Max D., and Russell Lemler, “Understanding the Counterdrone Fight: Insights from Combat in Iraq and Syria,” *Modern War Institute*, May 14, 2024, <https://mwi.westpoint.edu/understanding-the-counterdrone-fight-insights-from-combat-in-iraq-and-syria/>.
- ³² T.X. Hammes, “Game-changers: Implications of the Russo-Ukraine War for the Future of Ground Warfare,” *Atlantic Council*, 2023, 4–5, <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/game-changers-implications-of-the-russo-ukraine-war-for-the-future-of-ground-warfare/>.
- ³³ Joscha Abels, “Private Infrastructure in Geopolitical Conflicts: The Case of Starlink and the War in Ukraine,” *European Journal of International Relations* 30, no. 4 (2024): 842-866, <https://doi.org/10.1177/13540661241260653>.
- ³⁴ Sharma, Purabi, Kandarpa K. Sarma, and Nikos E. Mastorakis, “Artificial Intelligence Aided Electronic Warfare Systems—Recent Trends and Evolving Applications,” *IEEE Access*, December 14, 2020, <https://ieeexplore.ieee.org/abstract/document/9292960>.
- ³⁵ Dan Patt, “Too Critical to Fail: Getting Software Right in an Age of Rapid Innovation,” *Congress.gov*, March 13, 2024, <https://www.congress.gov/118/meeting/house/116957/witnesses/HHRG-118-AS35-Wstate-PattD-20240313.pdf>.

- ³⁶ Antebi, Liran, and Or Adar, "FPV Drones: From the Ukrainian Battlefield to the Middle East," *Institute for National Security Studies*, February 8, 2024, <https://www.inss.org.il/publication/fpv/>.
- ³⁷ Bhamidipati, Sriramy, and Grace X. Gao, "Locating Multiple GPS Jammers Using Networked UAVs," *IEEE Internet of Things Journal* 6, no. 2 (2019): 1817, doi: 10.1109/JIOT.2019.2896262.
- ³⁸ U.S. Army, "US Army Training Publication 3-12.3, Electromagnetic Warfare Techniques," January 2023, Appendix B-1.
- ³⁹ Bhamidipati and Gao, "Locating Multiple GPS Jammers," 1817.
- ⁴⁰ L3Harris, "L3Harris Falcon III AN/PRC-152A," *L3Harris*, July 2019. <https://www.l3harris.com/sites/default/files/2021-01/cs-tcom-falcon-iii-an-prc-152a-wideband-networking-handheld-radio-datasheet.pdf>.
- ⁴¹ Department of Defense, "Electromagnetic Spectrum Superiority Strategy," 2020, https://media.defense.gov/2020/Oct/29/2002525927/-1/-1/0/electromagnetic_spectrum_superiority_strategy.pdf.
- ⁴² Jones, Grace, Armughan Syed, and Sydney Hansen, "From the Frontlines to the Future: Assessing Emerging Technology in Russia's Invasion Strategy and NATO's Next Moves," *Belfer Center*, 2023, <https://www.belfercenter.org/publication/frontlines-future-assessing-emerging-technology-russias-invasion-strategy-and-natos>.
- ⁴³ Michael Kofman, "Assessing Russian Military Adaptation in 2023," *Carnegie Endowment for International Peace*, 2024, <https://carnegieendowment.org/research/2024/10/assessing-russian-military-adaptation-in-2023?lang=en>.
- ⁴⁴ US Army Cyber School, "Cyber School History," *U.S. Army Cyber Center of Excellence (CCoE)*, 2024, <https://cybercoe.army.mil/Cyber-Center-of-Excellence/Schools/Cyber-School/About-Cyber-School/>; U.S. Army-PEO IEW&S, "Program Manager-Electronic Warfare and Cyber," *U.S. Army Program Executive Office: Intelligence, Electronic Warfare & Sensors*, 2024, <https://peoiews.army.mil/pm-ewc/>.
- ⁴⁵ John Amble, "MWI Podcast: Defending Against Drones," *Modern War Institute*, June 13, 2024, <https://mwi.westpoint.edu/mwi-podcast-defending-against-drones/>.
- ⁴⁶ Amble, "Defending Against Drones."
- ⁴⁷ Ferguson, D. Max, and Russell Lemler, "Understanding the Counterdrone Fight," *Modern War Institute*, May 14, 2024, <https://mwi.westpoint.edu/understanding-the-counterdrone-fight-insights-from-combat-in-iraq-and-syria/>.
- ⁴⁸ John Amble, "MWI Podcast: Defending Against Drones," 2024; Ferguson, D. Max, and Russell Lemler "Understanding the Counterdrone Fight," 2024.
- ⁴⁹ Morgan J. Spring-Glace, "Return of Ground-Based Electronic Warfare Platforms and Force Structure," *Military Review*, August 2019, <https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/July-August-2019/Spring-Glace-Electronic-Warfare/>.
- ⁵⁰ U.S. Army-PEO IEW&S, "Program Manager-Electronic Warfare and Cyber," 2024, <https://peoiews.army.mil/pm-ewc/>.
- ⁵¹ Todd South, "Electronic Warfare Training Is Headed to an Army School Near You," *Army Times*, October 6, 2023, <https://www.armytimes.com/news/your-army/2023/10/06/electronic-warfare-training-is-headed-to-an-army-school-near-you/>.
- ⁵² Frost, Patricia, Clifton McClung, and Christopher Walls, "Tactical Considerations for a Commander to Fight and Win in the Electromagnetic Spectrum," *Cyber Defense Review* 3, no. 1 (2018): 17, <https://www.jstor.org/stable/26427371>.
- ⁵³ Frost, McClung, and Walls, "Tactical Considerations for a Commander," 17.
- ⁵⁴ Department of Defense, "DOD DIRECTIVE 3000.09: Autonomy in Weapon Systems," *Department of Defense*, January 25, 2023, <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300009p.PDF?ver=e0YrG458bVDI3-oyAOJjOw%3d%3d>; Humans Rights Watch, "Making the Case: The Dangers of Killer Robots and the Need for a Preemptive Ban," *Humans Rights Watch*, December 9, 2016, <https://www.hrw.org/report/2016/12/09/making-case/dangers-killer-robots-and-need-preemptive-ban>.
- ⁵⁵ US Cybersecurity and Infrastructure Security Agency, "Widespread IT Outage Due to CrowdStrike Update," August 6, 2024, *CISA*, <https://www.cisa.gov/news-events/alerts/2024/07/19/widespread-it-outage-due-crowdstrike-update>.
- ⁵⁶ Will Schrepferman, "All Mine: The United States and the Ottawa Treaty," *Harvard International Review*, 2019, <https://hir.harvard.edu/all-mine-the-united-states-and-the-ottawa-treaty/>.
- ⁵⁷ Rainie, Lee, Cary Funk, Monica Anderson, and Alec Tyson, "AI and Human Enhancement: Americans' Openness Is Tempered by a Range of Concerns," *Pew Research Center*, March 17, 2022, <https://www.pewresearch.org/internet/2022/03/17/americans-cautious-about-the-deployment-of-driverless-cars/>.

⁵⁸ Humans Rights Watch, “Dangers of Killer Robots,” 2016; Christopher Grut, “The Challenge of Autonomous Lethal Robotics to International Humanitarian Law,” *Journal of Conflict & Security Law* 18, no.3 (2013): 5–23, <https://www.jstor.org/stable/26296246>; Vivek Sehrawat, “Autonomous Weapon System: Law of Armed Conflict (LOAC) and Other Legal Challenges,” *Computer Law & Security Review* 33, no. 1 (2017): 38–56, <https://ssrn.com/abstract=2962760>.

⁵⁹ Frank Sauer, “Stopping ‘Killer Robots’: Why Now Is the Time to Ban Autonomous Weapons Systems,” *Arms Control Today*, October 2016, 8–13; Yanitra Kumaraguru, “A Pre-emptive Ban on Lethal Autonomous Weapon Systems,” In *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk: Volume III South Asian Perspectives*, edited by Petr Topychkanov, 55–58, Stockholm International Peace Research Institute, April 1, 2020, <http://www.jstor.org/stable/resrep24515.14>; Grut, “Challenge of Autonomous Lethal Robotics,” 2013; Sehrawat, “Law of Armed Conflict (LOAC),” 2017.

⁶⁰ David French, “How Our Overly Restrictive Rules of Engagement Keep Us from Winning Wars,” *National Review*, December 21, 2015, <https://www.nationalreview.com/2015/12/rules-engagement-need-reform/>.

⁶¹ Kriner, Douglas L., and Francis X. Shen, “Reassessing American Casualty Sensitivity: The Mediating Influence of Inequality,” *The Journal of Conflict Resolution* 58, no. 7 (2014): 1174–1201.

⁶² Michael Howard, “Men Against Fire: The Doctrine of the Offensive in 1914,” In *Makers of Modern Strategy: from Machiavelli to the Nuclear Age*, edited by Peter Paret, 510–522, (Princeton: Princeton University Press, 1986).

⁶³ Gartner, Scott S., and Gary M. Segura, “War, Casualties, and Public Opinion,” *The Journal of Conflict Resolution* 42, no. 3 (1998): 281, <https://www.jstor.org/stable/174515>.

⁶⁴ Silver, Laura, and Christine Huang, “Key Facts About China’s Declining Population,” *Pew Research Center*, December 5, 2022, <https://www.pewresearch.org/short-reads/2022/12/05/key-facts-about-chinas-declining-population/>.

⁶⁵ Cai, Yong, and Wei Feng, “Fiscal Implications of Population Aging and Social Sector Expenditure in China,” *Population and Development Review* 44, no. 4 (2019): 811–831, <https://www.jstor.org/stable/45174458>.

⁶⁶ Cancian, Mark, Matthew Cancian, and Eric Heginbotham, “The First Battle of the Next War: Wargaming a Chinese Invasion of Taiwan,” *Center for Strategic and International Studies*, January 2023, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/230109_Cancian_FirstBattle_NextWar.pdf.

⁶⁷ Reiko Aoki, “A Demographic Perspective on Japan’s ‘Lost Decades,’” *Population and Development Review* 38 (2012): 103–112, <https://www.jstor.org/stable/23655289>.

⁶⁸ Russia invaded Ukraine with a demographic crisis, and the war (and its attritional tactics) worsened it. (Also see Feldman, Bat Chen Druyan, and Arkady Mil-Man, “The War in Ukraine: Exacerbating Russia’s Demographic Crisis,” *INSS: The Institute for National Security Studies*, August 22, 2023. <https://www.inss.org.il/publication/russia-demographic/>).

⁶⁹ Kofman, Michael, and Ryan Evans, “Fortifications, Manpower, and Munitions in Ukraine’s Daunting Year Ahead,” *War on the Rocks*, March 17, 2024, <https://warontherocks.com/2024/03/fortifications-manpower-and-munitions-in-ukraines-daunting-year-ahead/>.

⁷⁰ The Moscow Times, “Russia’s Army Recruits Are Increasingly Older, Less Capable Men—Vyorstka,” *The Moscow Times*, October 8, 2024, <https://www.msn.com/en-us/news/world/russias-army-recruits-are-increasingly-older-less-capable-men-vyorstka/ar-AA1rXbMJ>.

⁷¹ US Air Force, “B-2 Spirit,” *Air Force*, December 2015, <https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104482/b-2-spirit/>.

⁷² Boeing, “777 Technical Specs,” *Boeing*, accessed June 17, 2024, <https://www.boeing.com/commercial/777#Anchor6>.

⁷³ US Air Force, “F-35A Lightning II,” *Air Force*, April 2014, <https://www.af.mil/About-Us/Fact-Sheets/Display/Article/478441/f-35a-lightning-ii/>.

⁷⁴ Sumari, Arwin D. W., Aldi S. Pranata, Irsyad A. Mashudi, Ika N. Syamsiana, and Catherine O. Sereati, “Automatic Target Recognition and Identification for Military Ground-to-Air Observation Tasks Using Support Vector Machine and Information Fusion,” 2022 International Conference on ICT for Smart Society (ICISS), *IEEE*, 2022, <https://ieeexplore.ieee.org/document/9915256/>; Barnawi, Ahmed, Krishan Kumar, Neeraj Kumar, Nisha Thakur, Bander Alzahrani, and Amal Almansour, “Unmanned Aerial Vehicle (UAV) Path Planning for Area Segmentation in Intelligent Landmine Detection Systems,” *Sensors* 23, no. 16 (2023): 7264, <https://doi.org/10.3390/s23167264>.

⁷⁵ Alvina Hoffmann, “The Urbanization of Warfare: Historical Development and Contemporary Challenges for International Humanitarian Law,” *St Antony’s International Review* 12, no. 2 (2017): 180, <https://www.jstor.org/stable/26229179>.

⁷⁶ Dominika Kunertova, “Drones Have Boots: Learning from Russia’s War in Ukraine,” *Contemporary Security Policy* 44, no. 4 (2023): 576–591, <https://doi.org/10.1080/13523260.2023.2262792>.

⁷⁷ Department of the Army, *FY 21 President's Budget—Exhibit P-1, A-3*, January 15, 2020, accessed June 24, 2024, https://www.asafm.army.mil/Portals/72/Documents/BudgetMaterial/2021/Base%20Budget/Procurement/MSLS_FY_2021_PB_Missile_Procurement_Army.pdf.

⁷⁸ CROWDSTRIKE, “Executive Summary: Root Cause Analysis — Channel File 291,” August 6, 2024, CROWDSTRIKE, accessed September 18, 2024, from https://www.crowdstrike.com/wp-content/uploads/2024/08/Executive-Summary_Root-Cause-Analysis_Channel-File-291.pdf.

⁷⁹ Sandra Erwin, “Space Force Eyes Closer Ties with Civil Space: It’s Good for Taxpayers,” *Space News*, February 3, 2021, accessed June 17, 2024, <https://spacenews.com/space-force-eyes-closer-ties-with-civil-space-its-good-for-taxpayers/>.

⁸⁰ The White House, *National Security Strategy of the United States of America*, 2017, *The White House*, <https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.

⁸¹ US Department of Defense, “2022 National Defense Strategy of The United States of America: Including the 2022 Nuclear Posture Review and 2022 Missile Defense Review,” *Department of Defense*, October 27, 2022, accessed September 11, 2024, <https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF>.

⁸² Milley, Mark A., and Eric Schmidt, “America Isn’t Ready for the Wars of the Future and They’re Already Here,” *Foreign Affairs*, August 5, 2024, accessed August 10, 2024, <https://www.foreignaffairs.com/usa/america-isnt-ready-for-the-wars-of-the-future-and-theyre-already-here>.

⁸³ Gelpi, Christopher, Peter D. Feaver, and Jason Reifler, “Success Matters: Casualty Sensitivity and the War in Iraq,” *International Security* 30, no. 3 (2005/2006): 7–46, <https://www.jstor.org/stable/4137486>.

⁸⁴ United Nations, “World Population Prospects 2022,” *UN: United Nations*, accessed June 17, 2024, <https://population.un.org/wpp/Graphs/DemographicProfiles/408>.

⁸⁵ Daniel Ellsberg, *The Doomsday Machine: Confessions of a Nuclear War Planner*, (New York: Bloomsbury Publishing, 2017), p. 98.

⁸⁶ US State Department, “Fact Sheet: Transparency in the U.S. Nuclear Weapons Stockpile,” *US State Department*, October 5, 2021, accessed July 15, 2024, https://www.state.gov/wp-content/uploads/2021/10/Fact-Sheet_Unclass_2021_final-v2-002.pdf#:~:text=This%20number%20represents%20an%20approximate%2088%20percent%20reduction,when%20the%20Berlin%20Wall%20fell%20in%20late%201989.

⁸⁷ Bode, Ingvild, Hendrik Huelss, Anna Nadibaidze, Guo Qiao-Franco, and Tom F. Watts, “Global Governance of Autonomous Weapons,” 2023.

⁸⁸ Albert, Craig Douglas, Samantha Mullaney, Joseph Huitt, Lance Y. Hunter, and Lydia Snider, “Weaponizing Words: Using Technology to Proliferate Information Warfare,” *The Cyber Defense Review* 8, no. 3 (2023): 15–32, <https://www.jstor.org/stable/48755359>; Hunter, Lance Y., Craig D. Albert, Josh Rutland, Kristen Topping, and Christopher Hennigan, “Artificial Intelligence and Information Warfare in Major Power States: How the US, China, and Russia Are Using Artificial Intelligence in Their Information Warfare and Influence Operations,” *Defense & Security Analysis* 40, no. 2 (2024): 235–269, <https://doi.org/10.1080/14751798.2024.2321736>.

⁸⁹ Boroush, Mark, and Livia Guci, “Cross-National Comparisons of R&D Performance,” *NSB: Science and Engineering Indicators*, April 28, 2022, accessed June 24, 2024, <https://nces.nsf.gov/pubs/nsb20225/cross-national-comparisons-of-r-d-performance>.

⁹⁰ Christine Huang, Laura Silver, and Laura Clancy, “Americans Remain Critical of China,” *Pew Research Center*, May 1, 2024, accessed June 24, 2024, <https://www.pewresearch.org/global/2024/05/01/americans-remain-critical-of-china/>.

⁹¹ Katz, Jeremy, “Global Conflicts Spur a ‘Race’ to Develop, Field Electronic Warfare Systems: Navy Secretary,” *Breaking Defense*, December 12, 2023, accessed September 13, 2024, <https://breakingdefense.com/2023/12/global-conflicts-spur-a-race-to-develop-field-electronic-warfare-systems-navy-secretary/>.

⁹² Training and Doctrine Command, “China Landing Zone: Learn How China Fights,” *T2COM G2*, 2024, accessed June 24, 2024, <https://oe.tradoc.army.mil/china-landing-zone-how-china-fights/>.

⁹³ Colin Demarest, “One-third of U.S. Military Could Be Robotic, Milley Predicts,” *Axios*, July 11, 2024, accessed July 15, 2024, <https://www.axios.com/2024/07/11/military-robots-technology>. See also Riley Ceder, “One-third of US military could be robotic by 2039: Milley,” *MilitaryTimes*, July 14, 2024, <https://www.militarytimes.com/news/2024/07/14/one-third-of-us-military-could-be-robotic-by-2039-milley/>.

⁹⁴ Michael Howard, “Men Against Fire: The Doctrine of the Offensive in 1914,” In *Makers of Modern Strategy: from Machiavelli to the Nuclear Age*, edited by Peter Paret, 510. (Princeton: Princeton University Press, 1986); Walsh, James I., and Marcus Schulzke, *The Ethics of Drone Strikes: Does Reducing the Cost of Conflict Encourage War?* (Carlisle Barracks: Strategic Studies Institute and U.S. Army War College Press, 2015), <https://press.armywarcollege.edu/monographs/442/>.

⁹⁵ Christopher Bailey, “Assessing the Lieber Code as a Form of Strategic Lawfare,” in *The Laws of Yesterday’s Wars*, ed. Samuel White (Leiden, The Netherlands: Koninklijke Brill NV, 2022), 187–208, https://doi.org/10.1163/9789004464292_001; Samuel C. White, “The Late Middle Ages in Northern Europe,” In Samuel C. White, *The Laws of Yesterday’s Wars*, 2022, 101–126.

⁹⁶ Bode, Ingvild, Hendrik Huelss, Anna Nadibaidze, Guo Qiao-Franco, and Tom F. Watts, “Global Governance of Autonomous Weapons,” 2023.

⁹⁷ Bode et al., “Global Governance of Autonomous Weapons.”

⁹⁸ Armed Conflict Location & Event Data Project, “Still Under Fire: The Evolving Fate of Civilians in Ukraine,” *ACLEd*, 2024, <https://acleddata.com/report/still-under-fire-evolving-fate-civilians-ukraine>.

⁹⁹ Cordesman, Anthony H., and John Kendall, *Chinese Strategy and Military Modernization in 2016: A Comparative Analysis*. (Washington, DC: Center for Strategic and International Studies, 2016), <https://www.csis.org/analysis/chinese-strategy-and-military-modernization-2016>.

¹⁰⁰ Snegovaya, Maria, Max Bergmann, Tina Dolbaia, Nick Fenton, and Samuel Bendett, *Back in Stock? The State of Russia’s Defense Industry after Two Years of the War*, (Washington DC: Center for Strategic and International Studies, 2024), 36, <https://www.jstor.org/stable/resrep59343>.

¹⁰¹ Lojka, Jason R., and Jason Du, “11 Russia-Ukraine War Lessons on Maneuver,” *Strategic Studies Institute, US Army War College*, 2024, 185, <https://www.jstor.org/stable/resrep61511.17>.

¹⁰² Ivshina, Olesya, Ben Dale, and Kate Brewer, “Russia’s Meat Grinder Soldiers—50,000 Confirmed Dead,” *BBC*, April 17, 2024, accessed June 24, 2024, <https://www.bbc.com/news/world-68819853>.

¹⁰³ Chase, Michael S., Jeffrey Engstrom, Tai Ming Cheung, Kristen Gunness, Scott W. Harold, Susan Puska, and Samuel K. Berkowitz, *China’s Incomplete Military Transformation: Assessing the Weaknesses of the People’s Liberation Army (PLA)*, (Washington, DC, RAND, 2015), 55, 60, 66.

¹⁰⁴ Nese F. DeBruyne, “American War and Military Operations Casualties: Lists and Statistics,” *US Census Bureau*, April 26, 2017, accessed July 15, 2024, <https://www.census.gov/history/pdf/wwi-casualties112018.pdf>.

¹⁰⁵ Walsh, James I., and Marcus Schulzke, *The Ethics of Drone Strikes: Does Reducing the Cost of Conflict Encourage War?* (Carlisle Barracks: Strategic Studies Institute and U.S. Army War College Press, 2015); Nathan Wood, “Autonomous Weapons Systems and Force Short of War,” *Journal of Ethics and Emerging Technologies* 32, no. 2 (2022): 1–16, <https://doi.org/10.55613/jeeet.v32i2.115>.

¹⁰⁶ Walsh and Schulzke, *The Ethics of Drone Strikes*.

¹⁰⁷ Grut, “Challenge of Autonomous Lethal Robotics,” 2013; Sehwat, “Law of Armed Conflict (LOAC),” 2017.

¹⁰⁸ Bode, Ingvild, Hendrik Huelss, Anna Nadibaidze, Guo Qiao-Franco, and Tom F. Watts, “Global Governance of Autonomous Weapons,” 2023.

¹⁰⁹ Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. (Cambridge, UK: Cambridge University Press, 2017), <https://doi.org/10.1017/9781316822524>; For the Tallinn 3.0 project, see CCDCOE, “The Tallinn Manual,” *The NATO Cooperative Cyber Defence Centre of Excellence*, accessed October 30, 2025, <https://ccdcoe.org/research/tallinn-manual/>.

¹¹⁰ Stamatis Karnouskos, “Stuxnet Worm Impact on Industrial Cyber-Physical System Security,” *IECON 2011–37th Annual Conference of the IEEE Industrial Electronics Society, Melbourne, IEEE*, 2011, 4490–4494, <https://doi.org/10.1109/IECON.2011.6120048>.

¹¹¹ Grut, “Challenge of Autonomous Lethal Robotics,” 2013; Sehwat, “Law of Armed Conflict (LOAC),” 2017.

Warfare in the Technology Arena

Cost-Imposition and Maneuver in the Electromagnetic Battlespace

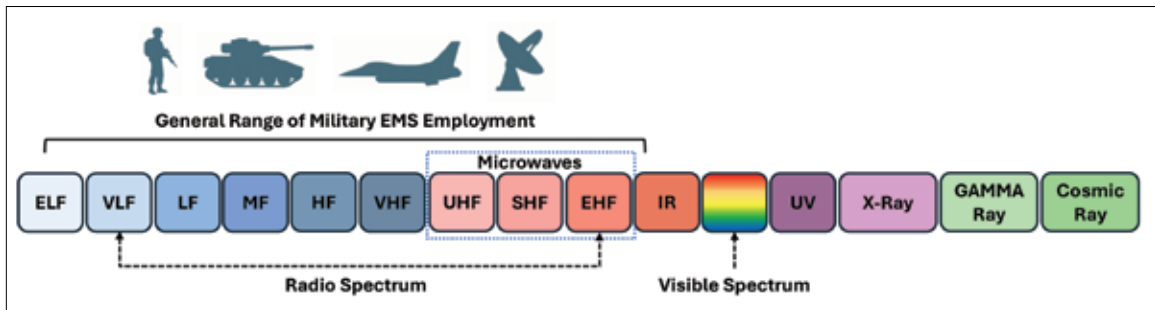
By Lt. Col. Sean "Nick" Blas

The electromagnetic spectrum (EMS) enables modern maneuver approaches, which demand a higher level of network connectivity to ensure joint operations are synchronized across all domains via a sensor-to-shooter link. Assumptions abound that sensors will provide accurate intelligence to users of precision-guided weapons (PGWs), improving the speed and accuracy of targeting.¹ However, the Russia-Ukraine war highlights the difficulties of operating in the EMS and demonstrates technology's disruptive tendencies, which can hinder maneuvering. The EMS is a highly contested environment where both friendly and adversary forces seek to enable the full capabilities of their weapon systems and endeavor to gain an advantage while also trying to disrupt the opposition's access to the spectrum.² Access to the EMS is not guaranteed, necessitating a shift in operational planning that emphasizes its placement as a critical aspect of joint all-domain maneuver. The remainder of this article will explore the concept of EMS maneuver, connect that concept with cost-imposition strategy, and then provide potential cost-efficient options to compete on the EMS battlefield.

The United States has spent considerable effort exploring and developing Electronic Warfare (EW) capabilities, but there has not been sufficient effort placed into understanding the EMS as a maneuver space. Conceptually, EMS maneuver involves the dynamic use of electromagnetic energy to achieve objectives by controlling or disrupting the flow of information and communications. In the traditional sense, maneuver refers to moving forces to gain positional advantage over an adversary.³ However, in the EMS, this concept translates to shifting, adapting, or controlling signals and energy across frequencies to provide a similar positional advantage. Maneuver in the EMS must be understood as fluid and not limited to the non-physical. Instead, agile EMS maneuver requires rapidly adapting to shifting conditions in both the physical (infrastructure) and non-physical (spectrum) spaces to achieve desired effects.

Lt. Col. Sean "Nick" Blas is an Air Force Intelligence officer and PhD in International Relations with several deployments supporting special operations and operational planning. He is currently an assistant professor at Air Command and Staff College where he is the Director of Staff for the Joint-All Domain Strategist (JADS) Concentration.

Figure 1: EMS Environment



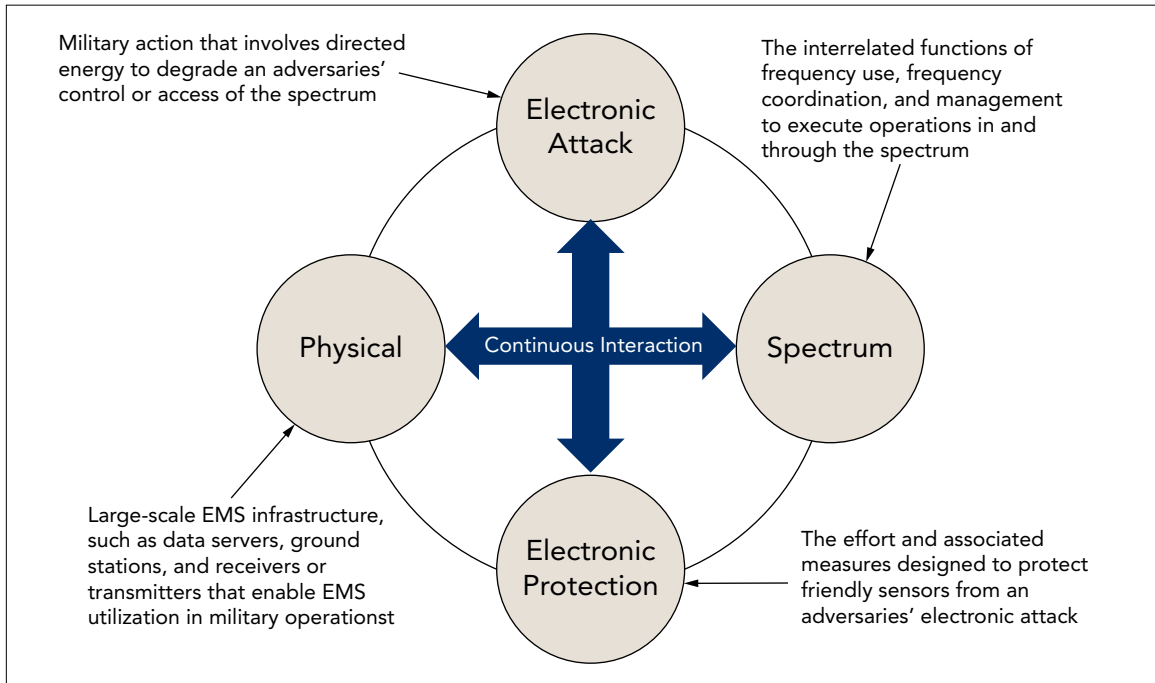
Source: author.

Maneuvering within the EMS requires a nuanced understanding of two key components: the distinction between physical and non-physical domains and the balance between offensive and defensive actions. The non-physical aspect of EMS maneuver encompasses the more traditional understanding of EW within the spectrum. This spectrum maneuvering entails the manipulation of the electromagnetic environment through altering frequencies or signal characteristics to gain an advantageous position. A basic example would be to employ Time-Division Multiplexing (TDM), which allows multiple signals to use a single frequency by dividing it into time slots. In contrast, the physical maneuver domain involves positioning tangible assets, such as jamming equipment or signal transmission devices, to achieve an advantage within the EMS. Additionally, maneuvering in the EMS can be framed in terms of offense and defense. The offensive side of EW, or electronic attack (EA), actively seeks to degrade or deny enemy access to the EMS. Electronic protection (EP), the defensive side of EW, focuses on protecting and securing one's own electromagnetic capabilities from hostile actions. Understanding and effectively balancing these components is essential for successful operational maneuver in the EMS.

In response to the challenges within the EMS, the U.S. must further recognize it as a critical

maneuver space and adopt cost-imposition strategies that leverage affordable, repurposed civilian technologies. Recent conflicts like the Russia–Ukraine war highlights the influence of maneuvering within the EMS and the use of a varied set of low-cost technologies to gain cost-imposition advantages over an adversary. *Google Loon* is an example that is not currently being fielded but could demonstrate the use of commercial technology to counter adversaries and reduce development costs. *Google Loon*, which will be discussed later in detail, is an example of an innovative use of commercial technology that can be repurposed to gain a positional advantage within the EMS by leveraging cost-imposition leverage using, for example, low-cost stratospheric balloons over more costly countermeasures. By relying on technologies widely available in the civilian sector, militaries can reduce the research, development, and production costs of creating new military platforms.

The spectrum component of the EMS encompasses the range of electromagnetic radiation that supports wireless network connectivity, and effective control of military frequency positioning is essential for achieving a decisive operational advantage. In military operations, controlling and positioning frequencies within this range is crucial for gaining a decisive advantage. The typical starting point for EMS consideration is the range of electromagnetic radiation, as the military employs

Figure 2: EMS Range⁶

equipment across the range of the spectrum and most military equipment require some connective through the spectrum to function (see Figure 2).⁴ Effective military operations depend on reliable Command and Control (C2) systems, which use various parts of the EMS for secure and rapid communication across all levels of command. The network-centric nature of military operations necessitates maintaining freedom of movement and positional advantage within the non-physical component of the EMS.⁵ This positioning encompasses both occupying space on the spectrum and countering jamming efforts through signal strength. High-fidelity data communication is needed for situational awareness across the battlespace and requires significant bandwidth. A salient example of bandwidth-intensive operations is sharing of full-motion video from sensors to analysts and operators. Furthermore, as EMS and cyber operations likely deepen, military operations will become more network centric. This sensor to shooter architecture is an important aspect of operations today, and

maintaining custody of a target until an appropriate munition can strike the desired target is essential. A noteworthy experience on both sides of the Russia-Ukraine war is the disruption EW causes within the EMS, making the ability to maintain target custody until munitions impact difficult at best. Securing a positional advantage within the spectrum will be critical to maintaining operational superiority and ensuring the success of joint military efforts.

While the spectrum receives the preponderance of attention, the spatially dispersed nature of military operations requires consideration of both the frequency and physical aspects of EMS. Understanding the physical layout of systems and equipment is essential because the data pathway must traverse EMS' spectral and physical components.⁷ The physical location of adversary EW attack capabilities directly impacts interference on friendly systems. A common misperception of EA is that by simply turning on a jammer an adversary or target systems will be rendered ineffective. Contrary to that notion, jamming strength is

affected by distance and terrain which forms gaps in the jamming coverage. This geographic separation provides avenues of approach that must be both defended and exploited.⁸ The physical placement of systems and terrain are components of EW that combatants use to achieve positional advantage in the EMS. Ultimately, radiated susceptibility, which is the potential level of interference on the equipment, is determined by the system type, the surrounding terrain, and proximity to a jammer.⁹ Each of these elements plays a role in equipment placement and access to the spectrum amidst the physical realities of military operations.

In modern combat, access to the EMS is an implied requirement for operations that opens offensive options to attack and disrupt an adversary's connectivity. EA involves using the EMS to disrupt, deceive, or deny the enemy's spectrum access, degrading its ability to employ connected systems and making them reliant on network connections. The Department of War (DOW) defines EW explicitly as "the use of electromagnetic energy and directed energy to control the [EMS] or attack the enemy."¹⁰ In current conflict paradigms, EW tends to focus on EA efforts to adversely affect an adversary's EMS-linked systems, such as radars, communication networks, and missile guidance. A primary EA technique in offensive EA is electromagnetic interference (EMI), which induces and degrades a system's access to the spectrum through electric or magnetic field interference.¹¹ Developing new EA systems forces adversaries to divert resources from other military or economic priorities to avoid vulnerabilities. By denying an adversary access to the EMS, a military can force that adversary into costly defensive or compensatory actions.¹² Challenging an adversary's access to the EMS through EA creates vulnerabilities thereby forcing that opponent to assume greater costs.

Reciprocally, modern operations dispersed and disaggregated nature necessitates a robust

defense to protect linked communication avenues of approach. EP defends these avenues, accounting for choke points that lead to single points of failure and ensuring overlapping capabilities to enhance security against EMI.¹³ When considering the physical and spectral aspect of the EMS, the priority is not to defend everywhere but instead to look at the critical data and communication pathways. For example, current information requirements can already overwhelm pure EMS transfer and storage without EMI. This shortfall necessitates a level of physical infrastructure to enable connectivity between data sources and the end users. The connection between sensor and storage, coupled with low bandwidth latency at the tactical edge of employment, creates an environment where poor planning could result in operational loss of access during crucial moments.¹⁴ The deliberate placement of physical infrastructure and spectrum positioning are vital components of EP, ensuring efficiently integrated data while maintaining low latency within current information infrastructures.

Maneuvering within the EMS to maintain critical nodes and access is made even more challenging by current force employment strategies that prioritize an expeditionary approach. Chinese and Russian EW capabilities, for instance, are focused on denying U.S. forces the ability to leverage the EMS within expeditionary formations, challenging command and control in joint operations.¹⁵ Extended lines of communication complicate safeguarding critical nodes and access points, making them more vulnerable to EW threats. The Finnish military has demonstrated strategies for safeguarding key nodes while navigating EW through spectrum agility and fortified access points. However, the Finnish model emphasizes a defensive posture with significant control over internal lines of communication. An expeditionary model would require extended lines of communication over difficult terrain and across national borders. Long fiber optic or copper lines

would be extremely costly and politically difficult to emplace before a conflict. Additionally, those lines would have greater exposure to adversary attacks, emphasizing spectrum connectivity. The variety of EMS effects impacts the vulnerability of delivery systems, requiring a balance between distance and risk reduction when deploying expeditionary forces.¹⁶ While maneuvering within the spectrum, such as frequency hopping to evade elements of EW, physical access points should also be considered as part of the maneuver.¹⁷ Effectively maintaining critical nodes and access in an expeditionary model requires a multifaceted approach that integrates spectrum agility and adaptable physical infrastructure addressing the increased vulnerability posed by extended lines of communication.

COST-IMPOSITION STRATEGY IN THE ELECTROMAGNETIC BATTLESPACE

An operational-level cost-imposition strategy uses military strategies and tactics to force an adversary to expend significant resources, time, and effort in ways that weaken its fight effectiveness in a specific theater or campaign. Military strategy entails countering strengths, exploiting weaknesses, and doing both in ways that make accomplishing ones' objectives achievable.¹⁸ A military cost-imposition strategy aims to force an adversary to expend significant financial, technological, or human resources while limiting expenditures.¹⁹ This strategy disrupts the enemy's ability to act effectively or efficiently, creating a situation where their cost of action outweighs potential operational benefits. As Schelling (1967) succinctly argued, "any costs that the enemy is obliged to incur have a positive value to our side, just as the costs we incur in carrying out the act, or in consequence of the decision, must be valued negatively."²⁰ Cost-imposition leverages an imbalance, compelling the adversary to invest more heavily in areas that provide diminishing re-

turns or require disproportionate effort to maintain parity with one's capabilities.

Competing in the EMS requires a comprehensive mixture of exquisite weapons systems and cost-efficient technology to enable targeting and integration while imposing costs on adversaries. Victory often hinges on a force's ability to coordinate various flexible technologies to gain advantage rather than exploiting a single niche technology.²¹ Gaining an advantage rests on military engagements that force the adversary to continue expending resources without achieving decisive victories. From a technological standpoint, there are instances where production and cost advantages provided a military force the decisive edge in war. Often these cost-imposition advantages are not readily apparent. However, one recognizable instance was the tank competition between Germany and United States during World War I. By the middle of 1944, the United States was able to field 1,555 tanks in comparison to 300 German Tanks.²² The American ability to mass produce tanks at a reasonable pace and cost enable the fielding of additional force on the battlefield. Relatively inexpensive but effective innovations can force an adversary to spend disproportionately large amounts of resources in response. This approach exploits technological and economic imbalances between opposing forces by using cost-efficient technologies that can still impose significant operational challenges on the adversary.²³ Like the industrial tank competition of World War I, today's competition in the EMS necessitates an ability to quickly out-produce and innovate beyond an adversary's capability to match. By leveraging economical technologies, a military can inflict significant costs on an adversary while minimizing its own expenses, gradually undermining the adversary's capacity to sustain the fight.

Google Loon, also known as *Project Loon*, was an innovative enterprise developed by Google X, a subsidiary of Alphabet Inc. in June 2013.²⁴ The

project's primary goal was to provide internet access to remote and difficult-to-access areas across the globe using high-altitude balloons and telecommunications equipment. Specifically, *Google Loon* sought to establish a network of stratospheric balloons (about 18-25 km above the Earth) to deliver 4G LTE internet service to areas without existing infrastructure or affected by natural disasters.²⁵ The polyethylene balloons could withstand the harsh conditions of the stratosphere. Despite the balloons' durability and estimated five-year life cycle, the telecommunication equipment and batteries required service every 100 days.²⁶ Essentially, the balloons acted as floating cell towers, enabling internet connectivity in regions where building traditional infrastructure was challenging or economically unfeasible.

The *Loon* project offered an innovative and expeditions solution to providing internet coverage. Each balloon was equipped with solar panels for power and stayed aloft for several months, traveling around the world with wind currents. After reaching the stratosphere, operators used prevailing winds to maneuver the balloons, while ground-based systems managed the network by coordinating their positions to maintain continuous coverage.²⁷ The balloons were also designed to operate autonomously, with software algorithms adjusting their altitude and position to maintain optimal network coverage and connectivity. Once positioned, the balloons provided a mesh network, for relaying signals from one balloon to another until they reached a ground station connected to an internet service provider.²⁸ *Google Loon* successfully provided internet access in several regions, including rural areas of Kenya, Brazil, and Puerto Rico after Hurricane Maria in 2017.²⁹ Using balloons to create a high-altitude mesh network demonstrated a promising approach to overcoming the challenges of providing reliable connectivity in inaccessible regions.

Despite its innovative approach, *Google Loon* faced several challenges, including the high cost of deployment, difficulties in maintaining a stable and consistent network, and different countries' regulatory hurdles. In January 2021, Alphabet announced that it was shutting down *Project Loon* due to the venture's unsustainable business model.³⁰ The income generation from subscribers did not favorably compare to the balloons operational costs. Although the project was discontinued, *Google Loon's* technology and lessons learned influenced alternative efforts to provide global internet coverage innovatively. *Loon* pioneered the potential of using unconventional methods to bridge the digital divide, leaving a lasting impact on international telecommunications.

Leveraging Commercial Programs on the Battlefield

Google Loon helps overcome the two major EMS employment obstacles of trying to operate in an expeditionary model and facing an enemy, recognizing that spectrum access is a critical vulnerability to operations. An expeditionary mindset requires friendly forces to operate on external lines of communication that are often vulnerable to attack or can be easily compromised. *Google Loon* can provide a critical operational advantage, enabling network access for remote or hard-to-reach locations where traditional infrastructure may be compromised or unavailable. *Google Loon* balloons could establish or restore essential communication links for military operations involving rugged terrain or compromised infrastructure. This ensures that troops remain connected and maintain access to data and intelligence over the EMS, even in highly contested environments.

Google Loon enabled the deployment of mobile, flexible communication networks absent relying on vulnerable static ground-based systems which provides a more resilient communication integrity.

Figure 3: Cost Comparison: Google Loon Versus Air-to-Air Missiles³⁴

Google Loon	Air-to-Air Missiles		
Electronics \$13,180	RS-AA-11 (R-73)	\$78,000	Russia
Solar Panels \$1,140	RS-AA-12 (R-77)	\$550,000	
Battery \$2,400	Ch-AA-9 (PL-1C)	\$80,000	China
Gas Cylinder \$650	CH-AA-7 (PL-12)	\$120,000	
Parachute \$500	CH-AA-10 (PL 15)	\$120,000	
Total \$17,870			

Loon could provide an operational maneuver advantage by maintaining real-time connectivity in areas where adversaries might attempt to jam or disrupt communications. Special operation forces already employ this approach to EMS maneuver, training with goTenna which provides a portable narrowband mesh radio for tactical operations.³¹ In a similar fashion to the special operations example, *Google Loon* could further improve EMS maneuver to mitigate risk of EMI at the operational level. *Loon* can offer a more resilient, high-altitude platform that is less susceptible to conventional jamming techniques. These stratospheric balloons are harder to target than traditional ground-based infrastructure, providing a reliable alternative for maintaining communications in the face of aggressive electronic warfare efforts. Moreover, *Loon's* distributed architecture (with multiple balloons providing coverage) could create redundancy, making it more difficult for adversaries to completely disrupt communications across a large area.

Cost-imposition strategies use low-cost technologies that force the adversary to spend significantly more. *Google Loon* offers an inexpensive method for establishing network coverage compared to launching satellites or building new ground-based infrastructure. The dispersed and mobile nature of *Google Loon* makes it an uneconomical target due to its adaptability as a networked system and its ability to adjust positions to disrupt the enemy's kill chain.³² Furthermore, the cost to target these balloons exceeds *Loon's* production and sustainment price.

The estimated cost of a single balloon in 2017 was approximately \$17,870 (reference Figure 2).³³

For military operations, this means they could quickly deploy a communications network at a fraction of the cost of conventional methods while forcing adversaries to invest heavily in EW capabilities to try and disrupt it. Even looking at conventional interdiction, an air-to-air missile costs more than a single *Google Loon* balloon. A *Google Loon* balloon costs \$64,820 less than the least expensive missile (See figure 2). The balloon's low radar signatures and operating altitude make it even more difficult for adversaries to interdict the constellation and will likely require more than one attempt. If one balloon is compromised, others continue to provide coverage, ensuring a resilient communication network. The balloons are mobile and can be deployed rapidly across various regions, allowing for quick operational adaptation. This flexibility is particularly valuable in fast-moving, dynamic military campaigns where communication needs change rapidly, making the cost-imposition placed on an adversary a significant advantage.

In a similar fashion, other technological adaptations can be employed within the EMS battlefield to enable maneuverability and could generate cost-imposition advantages against adversaries. A level of interference could be avoided, and EMS operations can gain an additional level of agility using an electromagnetic battle management (EMBM) system.³⁵ The ability to change frequency bands and waveforms provides a basic method of maneuvering within

the spectrum. The jammer's purpose is to occupy space on specific frequencies within the spectrum by emitting the more powerful signal. This jamming methodology is not as agile or reactive to an opponent's ability to frequency-hop and use physical distance to counter the jammer's signal strength. An example would be two aircraft communicating at a sufficient altitude to overcome the jammer's power, given their distance and proximity to each other. However, in a complex EMS environment where enemy jamming and friendly operations can cause spectrum congestion. An EMBM enables commanders and planners to visualize the EMS battlefield more effectively.³⁶ Thus, planners can determine optimal operating frequencies to avoid enemy and friendly interference. Compared to jammers, agile spectrum employment offers a forward-leaning offensive posture in the EMS.

The ability to switch frequencies effectively across the spectrum represents a cost advantage over expensive adversary jamming systems. As many foreign militaries have sought to compete in the EMS, the heaviest investments have been in expensive jamming systems to deny adversaries access.³⁷ The Russia-Ukraine war provides a modern example of an EMS-degraded battlespace as both sides seek to jam their opponent's weapon system. However, within this degraded EMS environment, there is still maneuver space. Specifically, there is an opportunity to employ off-the-shelf programs to improve EMS battlespace awareness and enable operational and strategic planning. The U.S. Army is already moving forward with options to conduct EMBM. In its 2024 budget, the Army requested \$21.3 million to develop an operational EMBM system.³⁸ In comparison, a Russian R-330Zh Zhitel unit is estimated to cost approximately \$10 million, which is also less expensive than more advanced systems like the Krasukha-4 or Murmansk-BN.³⁹ Ultimately, the growing gap between low-cost EMS maneuver tools and high-end jamming systems presents an

opportunity for the U.S. to compete more effectively in a congested, contested spectrum.

Similarly, low-cost drone systems are also reshaping the electromagnetic battlespace in ways that challenge traditional defensive approaches. These cheap drones can locally and temporarily overcome most adversary defenses' EMS through a variety of applications.⁴⁰ The rapid proliferation of drones is introducing new pathways to exploit gaps in adversary EMS defenses. A salient example is the current employment of drones within the Russia-Ukraine war. Russians are successfully using first-person-viewer (FPV) drones to interdict Ukrainian logistics up to two kilometers beyond the forward line of troops.⁴¹ One-way attack drones (OWAD) are being used with extended ranges and to interdict logistics further into Ukraine's second echelon area.⁴² However, Ukraine is also on the cutting edge of drone employment, and with units like the NEMESIS unit from the Unmanned Systems Forces of Ukraine, they have innovated the ability to hold territory, conduct fire support, and destroy high-cost EMS jammers.⁴³ These dynamics underscore that small drone systems now play a pivotal role in determining EMS advantage at both the tactical and operational levels.

The cost-imposition generated by these systems is becoming increasingly apparent as low-priced drone systems force adversaries to expend disproportionately expensive resources to defend against them. Drone costs can vary depending on size and sophistication. FPVs currently cost between \$500-\$3,000, and larger OWAD systems like the Geran-2 can cost between \$30,000-\$80,000.⁴⁴ These various types of drone platforms can impose costs as adversaries try to compete with high-end EW systems, air-defense missiles, and radar assets that are orders of magnitude more costly than these threats. This cost and operational asymmetry strains logistics, accelerates materiel depletion, and complicates operational planning for adversaries. Moreover,

because drones can rapidly adapt flight profiles, frequencies, and payloads, adversaries face recurring expenses to update jamming tactics, harden nodes, and protect vulnerable command-and-control links. As Ukraine and Russia continue to iterate at speed, it is becoming more apparent that the side capable of fielding inexpensive systems at scale will impose a cumulative financial and operational burden on its opponent, demonstrating how small drones create strategic leverage by forcing adversaries into a cycle of costly, reactive EMS defense.

CONCLUSION

The EMS is increasingly recognized as a critical maneuver space, integral to modern warfare and joint operations. Control and effective use of the EMS can provide a decisive advantage, while failure to manage and protect access to the spectrum can yield vulnerabilities and operational failure. In multi-domain modern warfare, cost-imposition remains central to nations' efforts to outmaneuver adversaries while maintaining strategic superiority. As the challenges demonstrated in Ukraine reveal, access to and control of the EMS is far from guaranteed, and the ability to navigate its complexities can make the difference between success and failure on the battlefield. By adopting cost-imposition strategies that repurpose existing civilian technologies like *Google Loon*, EMS battlefield management systems, and low-cost drone systems the military can effectively counter adversaries while keeping costs manageable. Using commercially available platforms offers practical solutions, enabling greater agility and adaptability in EMS operations.

The DOW should consider new maneuver theories that account for the EMS and employ practical technology. The DOW should also increase the testing of these innovative and cost-saving balloons in operational exercises to refine employment dynamics further. As the warfare landscape continues to evolve, incorporating affordable and

innovative technologies will be crucial to maintaining a competitive edge in a contested and dynamic environment. **PRISM**

Notes

- ¹ Jon R Lindsay, *Information Technology and Military Power* (Cornell University Press, 2020), 13; Herbert; Swift Carlisle, Scott; Wesley, Eric, "Regaining Decision Advantage Revising Jadc2 to Buttress Deterrence in Our Window of Greatest Need," *Hudson Institute* (2022): 1; Jeffrey M Reilly, "Creating Competitive Space through a Framework of Joint All Domain Maneuver" (2020), 1.
- ² Mykhaylor Zabrodskiy et al., *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine, February-July 2022* (Royal United Services Institute for Defence and Security Studies London, 2022), 3; Christopher Petty, "Protecting Army Aviation and Enabling Military Dominance through Disruptive Innovation," in *Disruptive and Game Changing Technologies in Modern Warfare*, ed. Margaret E Kosal (Springer, 2020), 183 and 86; Lindsay, *Information Technology and Military Power*, 22-23; Bryan Clark, Whitney Morgan McNamara, and Timothy A Walton, *Winning the Invisible War: Gaining an Enduring Us Advantage in the Electromagnetic Spectrum* (Center for Strategic and Budgetary Assessments, 2019), 1-2.
- ³ Joseph Caldwell Wylie Jr, *Military Strategy: A General Theory of Power Control* (Naval Institute Press, 2014), 77-78; Liddell B. H. Hart, *Strategy*, Second Revised Edition ed. (London, England: Meridian, 1991), 325-28.
- ⁴ US Department of the Air Force, "Annex 3-51 Electromagnetic Warfare and Electromagnetic Spectrum Operations," ed. Air Force (AF) (Washington, DC: Government Publishing Office, 2019), 5-6; Robert Smith, "Maneuver at Lightspeed: Electromagnetic Spectrum as a Domain," *Over The Horizon: Multi-Domain Operations & Strategy* (2018): 2-3.
- ⁵ Vasicek, Radovan and Alena Oulehlova, "Cyber and Electromagnetic Activities and Their Relevance in Modern Military Operations" (paper presented at the Proceedings of the 31st European Safety and Reliability Conference (ESREL 2021), 2021), 1-2; Patricia Frost, Clifton McClung, and Christopher Walls, "Tactical Considerations for a Commander to Fight and Win in the Electromagnetic Spectrum," *The Cyber Defense Review* 3, no. 1 (2018): 15-16; Smith, "Maneuver at Lightspeed: Electromagnetic Spectrum as a Domain," 2.

⁶Publication, Air Force Doctrine. 3-85 Electromagnetic Spectrum Operations. LeMay Center, Maxwell AFB: AFDP, 2023: 1-3; Florenzen, Matthew J., Kurt M. Shulkitas, and Kyle P. Bair. “Unmasking the Spectrum with Artificial Intelligence.” *Joint Force Quarterly: JFQ*, no. 95 (2019): 116–117.

⁷“Maneuver at Lightspeed: Electromagnetic Spectrum as a Domain,” 3; Reilly, “Creating Competitive Space through a Framework of Joint All Domain Maneuver,” 2-3; Jacob Cox et al., “The Friction Points, Operational Goals, and Research Opportunities of Electronic Warfare and Cyber Convergence,” *The Cyber Defense Review* 4, no. 2 (2019): 83-84; Isaac R Porche et al., “The Information Environment and Information Warfare,” *Redefining Information Warfare Boundaries for an Army in a Wireless World* (2013): 11-12.

⁸Akshat Upadhyay, “Integral Air Support to Land Operations,” *Journal of Defence Studies* 17, no. 4 (2023): 179.

⁹KA Hossain, “Study on Electromagnetic Interference (Emi) and Electromagnetic Compatibility (Emc): Sources and Design Concept for Mitigation of Emi/Emc,” *Journal of Liberal Arts and Humanities (JLAH)* 4, no. 8 (2023): 71-73.

¹⁰U.S. Department of Defense, “Joint Publication (Jp) 3-13.1, Electronic Warfare,” ed. Joint Staff (Washington, DC: Government Printing Office, 2012), I-4.

¹¹Hossain, “Study on Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC): Sources and Design Concept for Mitigation of EMI/EMC.”

¹²Clark, McNamara, and Walton, *Winning the Invisible War: Gaining an Enduring Us Advantage in the Electromagnetic Spectrum*, 17-19.

¹³Carlisle, “Regaining Decision Advantage Revising Jadc2 to Buttress Deterrence in Our Window of Greatest Need,” 3; Gary Waters, “Information Warfare—Attack and Defence,” *Australia and Cyber-warfare* (2008): 51-52.

¹⁴Cox et al., “The Friction Points, Operational Goals, and Research Opportunities of Electronic Warfare and Cyber Convergence,” 93.

¹⁵Clark, McNamara, and Walton, *Winning the Invisible War: Gaining an Enduring Us Advantage in the Electromagnetic Spectrum*, 27; Madison Creery, “The Russian Edge in Electronic Warfare,” *Georgetown Security Studies Review* (2019): 1.

¹⁶Smith, “Maneuver at Lightspeed: Electromagnetic Spectrum as a Domain,” 6; Zabrodskiy et al., *Preliminary Lessons in Conventional Warfighting from Russia’s Invasion of Ukraine, February-July 2022*, 2-3.

¹⁷Smith, “Maneuver at Lightspeed: Electromagnetic Spectrum as a Domain,” 5.

¹⁸Antulio J Echevarria II, *Military Strategy: A Very Short Introduction* (Oxford University Press, 2017), 1; Michael Howard and AJ Wilson, “Military Science in an Age of Peace,” *The RUSI Journal* 119, no. 1 (1974): 5-6; Wylie Jr, *Military Strategy: A General Theory of Power Control*, 14-15; Hart, *Strategy*, 320-21.

¹⁹Kenneth P Ekman, “Applying Cost-Imposition Strategies against China,” *Strategic Studies Quarterly* 9, no. 1 (2015): 26-28; Thomas C Schelling, “The Strategy of Inflicting Costs,” in *Issues in Defense Economics* (NBER, 1967), 107; Thomas G Mahnken, “Cost-Imposing Strategies: A Brief Primer,” *Center for a New American Security* (2014): 5; Joseph; Keith Schmitt, Andrew, “An Expanded View of Cost-Imposition Application to Personnel and Nondefense Policies,” *Wild Blue Yonder* (2020): 1-2.

²⁰Schelling, “The Strategy of Inflicting Costs,” 108-09.

²¹Martin Van Creveld, *Technology and War: From 2000 Bc to the Present* (New York: The Free Press, 1991), 17 and 318; Ekman, “Applying Cost-Imposition Strategies against China,” 32; Upadhyay, “Integral Air Support to Land Operations,” 185.

²²Zaloga, Steven J. Panzer Iv Vs Sherman: France 1944. Vol. 70: Bloomsbury Publishing, 2015: 7-8.

²³Ekman, “Applying Cost-Imposition Strategies against China,” 28-29; Andrew F Krepinevich, Simon Chin, and Todd Harrison, *Strategy in Austerity* (Center for Strategic and Budgetary Assessments, 2012), 7-8.

²⁴Pablo Serrano et al., “Balloons in the Sky: Unveiling the Characteristics and Trade-Offs of the Google Loon Service,” *IEEE Transactions on Mobile Computing* 22, no. 6 (2021): 3165.

²⁵Pablo Serrano et al., “Balloons in the Sky: Unveiling the Characteristics and Trade-Offs of the Google Loon Service,” *IEEE Transactions on Mobile Computing* 22, no. 6 (2021): 3165-66; Aishwarya Srinivasan, “Balloon-to-Balloon Adhoc Wireless Network Connectivity: Google Project Loon,” (2022): 1; Ashlee Vance, “The Afterlife of Google Loon,” *Bloomberg Businessweek*, no. 4755 (2022): 21; James Burr, “The Feasibility of Google’s Project Loon,” *Australian National University (ANU) College of Engineering, Tech. report U 5350804* (2017): 8.

²⁶“The Feasibility of Google’s Project Loon,” 6-7.

²⁷Serrano et al., “Balloons in the Sky: Unveiling the Characteristics and Trade-Offs of the Google Loon Service,” 3165; Burr, “The Feasibility of Google’s Project Loon,” 8.

²⁸Serrano et al., “Balloons in the Sky: Unveiling the Characteristics and Trade-Offs of the Google Loon Service,” 3166-67; Srinivasan, “Balloon-to-Balloon Adhoc Wireless Network Connectivity: Google Project Loon,” 2.

²⁹ Serrano et al., “Balloons in the Sky: Unveiling the Characteristics and Trade-Offs of the Google Loon Service,” 3167-69; Vance, “The Afterlife of Google Loon,” 21.

³⁰ Serrano et al., “Balloons in the Sky: Unveiling the Characteristics and Trade-Offs of the Google Loon Service,” 3165; Srinivasan, “Balloon-to-Balloon Adhoc Wireless Network Connectivity: Google Project Loon,” 2-3.

³¹ John M. McHale, “Shared Situational Data for Warfighters Enabled by Gotenna/Everywhere Communications Joint Solution,” *Military Embedded Systems* (2024), <https://militaryembedded.com/comms/encryption/shared-situational-data-for-warfighters-enabled-by-gotennaeverywhere-communications-joint-solution>; John Keller, “Air Force to Help Gotenna Improve Military Mesh Network Radio Communications with Encryption Security,” *Military+Aerospace Electronics* (2024), <https://www.militaryaerospace.com/communications/article/55133123/communications-mesh-network-radio-encryption>.

³² Zabrodskiy et al., *Preliminary Lessons in Conventional Warfighting from Russia’s Invasion of Ukraine, February-July 2022*, 3; Clark, McNamara, and Walton, *Winning the Invisible War: Gaining an Enduring Us Advantage in the Electromagnetic Spectrum*, 29; Waters, “Information Warfare—Attack and Defence,” 33-34; Brett Van Niekerk and Christo Cloete, “Management Information Systems for Electronic Warfare Command and Decision Support,” *Journal of Information Warfare* 14, no. 1 (2015): 68-69.

³³ Burr, “The Feasibility of Google’s Project Loon,” 11.

³⁴ *Ibid.*; Forecast International, “Missile Forecast,” in *Forecast International* (Sandy Hock, Connecticut, 2021). Note: Chinese missile cost are estimates based on released production data.

³⁵ Ricciardi, Stéphane and Cédric Souque, “Modern Electromagnetic Spectrum Battlefield,” *PRISM* 9, no. 3 (2021): 127.

³⁶ Yang Huang et al., “Space-Based Electromagnetic Spectrum Sensing and Situation Awareness,” *Space: Science & Technology* 4 (2024): 4.

³⁷ Ricciardi and Souque, “Modern Electromagnetic Spectrum Battlefield,” 129; Andreas Turunen, “The Broader Challenge of Russian Electronic Warfare Capabilities,” *Improvisation and Adaptability in the Russian Military* (2020): 13; Jeremy Hofstetter and Adam Wojciechowski, “Electromagnetic Spectrum Survivability in Large-Scale Combat Operations,” *Infantry*, 109 (4), 21-24 (2020): 21.

³⁸ Mark Pomerleau, “The Army Has Big Plans for Electronic Warfare Procurement in Fiscal 2024,” *DEFENSESCOOP*, <https://defensescoop.com/2023/04/04/the-army-has-big-plans-for-electronic-warfare-procurement-in-fiscal-2024/>.

³⁹ Povilas M., “Ukraine Destroyed yet Another Very Expensive Russian EW System,” *TECHNOLOGY.ORG*, <https://www.technology.org/2025/10/10/ukraine-destroyed-yet-another-very-expensive-russian-ew-system/>.

⁴⁰ Ricciardi and Souque, “Modern Electromagnetic Spectrum Battlefield,” 135; Huang et al., “Space-Based Electromagnetic Spectrum Sensing and Situation Awareness,” 2; Anton O Belousov et al., “UAVS Protection and Countermeasures in a Complex Electromagnetic Environment,” *Complexity* 2022, no. 1 (2022): 1-2; Patricia Frost, Clifton McClung, and Christopher Walls, “Tactical Considerations for a Commander to Fight and Win in the Electromagnetic Spectrum,” *The Cyber Defense Review* 3, no. 1 (2018): 15.

⁴¹ Kateryna Stepanenko, “Russian Drone Innovations Are Likely Achieving Effects of ^{Battlefield} Air Interdiction in Ukraine,” (2025), <https://understandingwar.org/research/russia-ukraine/russian-drone-innovations-are-likely-achieving-effects-of-battlefield-air-interdiction-in-ukraine/>.

⁴² *Ibid.*

⁴³ M., “Ukraine Destroyed yet Another Very Expensive Russian EW System.”

⁴⁴ Bronk, Justin and Jack Watling, *Mass Precision Strike: Designing UAV Complexes for Land Forces* (RUSI, 2024), 23-30.

Human, Machine, War: How the Mind-Tech Nexus Will Win Future Wars

By Nicholas Wright, Michael Miklaucic,
and Todd Veazie

ISBN: 9781585663347

Reviewed by Dr. Robert J. Bunker



This future war focused essay is divided into two parts: first, a traditional review of the important book *Human, Machine, War: How the Mind-Tech Nexus Will Win Future Wars* and second, due to the significance of the work, an epochal change construct critique of the book. The latter will analytically challenge the underlying assumptions utilized in the book across four thematic areas. The intent of these analytical challenges is to spur reflection and debate in terms of U.S. Department of War (DOW) perceptions of the magnitude of the military revolution taking place related to the emergent ‘Mind-Tech Nexus’ now well underway.

BOOK REVIEW

The anthology is edited by Nicholas Wright, Michael Miklaucic, and Todd Veazie. Dr. Wright is a defense community neuroscientist (and artificial intelligence specialist) with extensive professional experience both in the U.S. and the UK; Mr.

Miklaucic is a senior fellow of the National Defense University (NDU) and the PRISM editor-in-chief emeritus; and Mr. Veazie serves as the director of the Strategic Multiyear Assessment (SMA) office in the U.S. Joint Staff’s Operations Directorate with considerable special warfare and SEAL team experience. This edited collection was recently published by the DOW, via the Air University Press. It represents an authoritative resource, given the expertise and high caliber of its editors and contributors, on human-machine convergence—what the book terms the “Mind-Tech Nexus” (p. vii).

The work is 391 pages in length and divided into six parts encompassing eighteen chapters. of the book opens with a foreword by GEN James E. Rainey, Commander, U.S. Army Futures Command; a second foreword by Sir Lawrence Freedman, Emeritus Professor of War Studies at King’s College London, and an introduction by the editors. The book is divided into themes focused

Dr. Robert J. Bunker is a Research Fellow, Future Security Initiative (FSI), Arizona State University (ASU) and the Director of Research and Analysis and a Managing Partner at C/O Futures, LLC. An international security and counterterrorism professional, he was Futurist in Residence at the Behavioral Science Unit (BSU) at the Federal Bureau of Investigation (FBI) Academy in Quantico, VA, and Minerva Chair at the Strategic Studies Institute (SSI) of the U.S. Army War College, Carlisle, PA. He can be reached at rbunker1@asu.edu and docbunker@cofutures.net.

upon 1) innovation and ethics; 2) command, control; and intelligence; 3) performance enhancement; 4) Chinese and Russian programs; 5) human aspects (the will to fight, degraded performance); and 6) conclusions.

According to the authors, the ‘Mind-Tech Nexus,’ is broadly defined as what human factors (e.g., will to fight, skill, daring, perception) will interface and converge with the technologies of our time (e.g., digital, quantum computing, neuroscience) to help shape the character and the outcomes of competition... (p. 2). Additionally, the twenty-four contributors (and editors) are ‘world-leading experts’ on this subject matter and have been brought together to provide:

- the latest thinking on minds and technology (e.g. neuroscience, artificial intelligence (AI), or quantum computing) and how they interface and converge;
- the implications of this Mind-Tech Nexus at every level of U.S. national security, from the individual warfighter at the tactical level to leaders at the operational and strategic levels of war; and
- how the Mind-Tech Nexus matters not only for the US and its allies alone but also in the context of key competitors (p. 3).

For a work that focuses on a cutting-edge and futuristic subject, the writings are, for the most part, constrained, practical, and reinforce status quo “thinking.” We see this in the paragraph penned by Rainey in the initial preface:

“We must also develop the capability to fight with AI-enabled systems of systems, including human-machine integrated ground combat formations. The goal is not to replace humans with machines but to offload risk and work with machines. Doing so frees humans to do what they do best,

including exercising judgement, deciding when to use lethal force, and practicing the art of command. We will develop this capability through formation-based transformation (p. viii).”

This vision is in line with the enduring primacy of the human soldier on the battlefield, U.S. Department of War (DOW) Directive 3000.09, “Autonomy in Weapon Systems,” and Army mission command concepts.¹ The editors used more than just a 1920s-1930s operational level of change perspective that focused on revolutionizing military affairs at scale; they also incorporated 1950s Offset 1 nuclear weapons and 1990s Offset 2 precision strike capability strategies. This is now followed by 2015 Offset 3 AI, cyber capabilities, and unmanned systems (p. xv).

The five main sections of the work include fifteen fascinating chapters covering a wide range of subjects and topical areas. Given the importance of John Boyd’s Observe, Orient, Decide, and Act (OODA) loop concept to modern warfighting, Dr. Timothy Grayson’s Chapter 5 deserves mentioning. The piece initially provides a short overview of the iterated steps of the OODA loop and then a discussion of how AI can share the cognitive workload with humans. Acceleration of the operational and strategic level OODA loops is then explored. The intent of the essay to ensure that U.S. warfighters retain their advantage of speed—as a force multiplier—while cycling through these steps regarding their opponents.

One omitted area which could have been explored is internal mind-technology interfaces rather than solely wearable ones—though technical maturity and interface issues do exist—trending suggests synthetic-biology will become increasingly prevalent. Furthermore, another chapter worth mentioning in more detail is Samuel Bendett’s (Chapter 11) which provides a crucial overview of “Russian military attempts to enhance human

capabilities using modern technologies” (p. 211). The neural helmet concept and short discussion of Russian experimentation with virtual, augmented, and mixed reality were important from this reviewer’s perspective, especially since they align with advanced dimensionality (cyber and hyper, 5th dimensional space-time warfighting constructs) developments. Full spectrum reality overlays over humans will become a critical component of future warfighting capabilities.

Given the ongoing competition between the U.S. and China, which has sometimes led to the brink of conflict over China’s claims in the South China Sea and its stance on Taiwan, Chapter 12 by Josh Baughman deserves special attention. It is excellent. He discusses China’s views on the cognitive domain and systems-of-systems warfare both from destruction (offensive) and survival (defensive) perspectives along with their views on the utility of generative artificial intelligence (GEN AI), cyber realities, and brain-computer interface technology.

The final area of the book is focused on conclusions. In fact, the double conclusion to the work is one of its major innovations and is utilized as a ‘proof of concept’ of the influence of GEN AI on scholarship and analysis. Chapter 16 presents the editors’ conclusions, emphasizing ethical standards, avoiding the pitfalls of 21st-century Maginot lines, taking interfaces seriously, and focusing on agile processes. It also highlights the emergence of new vulnerabilities that can be exploited and the importance of maintaining a strong will to fight. Chapter 17, written by David Vernal, introduces us to GEN AI related to large language models (LLMs) followed by the national security implications of such models. Finally, the second conclusion, Vernal’s Chapter 18, provides a GEN AI written analysis of the book via GPT-4 and Claude 3 Opus. The author does this through a series of specific text promptings along with a foreign language (Japanese) hypothetical email to the Japanese Self-Defense Force to

collaborate on an open-source intelligence (OSINT) effort. To the reviewer’s knowledge, this has not been done before in a DOW-linked publication. However, it is expected that this analytical technique will become more common in the future.

EPOCHAL CHANGE CRITIQUE

Given the significance of the work and the integral importance of the editors, particularly those affiliated with institutions and activities like Defense Advanced Research Projects Agency (DARPA), National Defense University (NDU), and SMA, four analytical challenges are being directed at it, as it could potentially have significant impacts on DOW policies regarding future wars and conflicts. These challenges are not leveled at the individual chapters themselves but rather at the underlying paradigm of change and constructs the work has accepted as analytical working assumptions.

The intent is not to get into a theoretical future war “bar fight” with the editors but rather to provide some civil analytical challenges to their working assumptions, which appear to be in alignment with current DOW perceptions. Getting future war wrong—or at least more wrong than our opponents—would have devastating consequences for DOW and the nation it defends. Since silence in such important matters is not an option, it is far better to speak truth to authority (recognized DOW expertise) in order to allow alternative perspectives to see the light of day.

An unexpected ally appeared from one of its contributing authors—Lt. Gen. (LTG) John (Jack) N. T. Shanahan, USAF, Retired who was the inaugural director of the DOW Joint Artificial Intelligence Center (JAIC). He firmly stands out with his dissenting perceptions related to the book’s working assumptions. His statements, “We are now witnessing the early outlines of the third major revolution in our species’ history—a digital revolution” (p. 127); and “While I do not expect that AI will change the nature

of war—if *nature* is defined as the reasons some humans decide to fight other humans, which always come down to varying combinations of fear, honor, interest, and culture—it will” (p. 139), squarely place him in the Galilean-like ‘And yet it moves’ philosophical camp when faced with what may be considered ritualized DOW thinking, if not, dogma.

While LTG Shanahan’s paradigmatic perceptions are squarely Tofflerian derived, this critique, on the other hand, draws upon epochal change constructs which have existed since the late 1980s.² These constructs concern classical, medieval, and modern civilizational change in the Western world, energy sequences, modal warfare analysis, and a number of other qualitative variables which portray the advancement of humanity’s activities in peaceful and warlike pursuits from roughly 500 BC into the twenty-first century AD.³

The first two analytical challenges are highlighted in Table 1 related to the work’s assumptions concerning the characteristics of war (conflict) derived from its nature and its conduct. They are as follows:

- *Analytical Challenge 1—Nature of War:* This characteristic of war—per the Colin Gray information box is “is universal and eternal and does not alter...” (p. 4). Further, “Strife, conflict, and war are essentially the permanent, inevitable struggle over the terms of coexistence—an interaction between humans and their psychologies” (p. 4). Where issue is taken with this assumption is that it presupposes that war (and conflict) is eternally human-based. Hence humans (essentially old stock ones) will always be in, if not on, the loop as warfare is conducted. Generative (and other forms of) AI, as they rapidly mature, are challenging such perceptions. An alternative view is that later-stage (future) engagements with humans on the loop may see OODA loop cycles of such speed that humans cannot hope

to effectively monitor AI decision-making and response cycles. This will force humans into off-the-loop position for command and control (C²) purposes as AI battle management systems go directly up against each other. Further, a “no loop” condition may arise—based on human and machine convergence—per the book’s subtitle “How the Mind-Tech Nexus Will Win Future Wars.” This nexus portends the emergence of augmented humans via the brain-computer interface (BCI) and other modalities. It is straight out of the old Cyberpunk genre of ‘wetware,’ where advanced technology and their human nervous system interfaces take place.⁴ When war is being waged by either autonomous machines (humans “off the loop”) and/or augmented (“no loop”) humans who have interfaced with advanced technology and AI, it begs the question as to whether the very nature of war itself has not changed. War has now moved beyond the basic “interaction between humans and their psychologies” (p. 4) cited earlier.

- *Analytical Challenge 2—Conduct of War:* Time and time again, the work returns to the perception that the level of change now taking place with the advent of advanced technology emergence and integration is equivalent to the 1920s and 1930s (for example, see pages 16 and 325). This perception is based on the Soviet-influenced Military-Technical Revolution (MTR) and Revolution in Military Affairs (RMA) debates that took place within the DOW and the broader defense academic community in the 1980s and 1990s. This level of change is viewed as being ‘in paradigm.’ That is within the modern military system, paradigm which is industrial, hierarchical, and state soldier dominated. The change is equivalent to the advent of strategic bombing, carrier operations, amphibious landings, and armored (blitzkrieg)

Table 1: Mind-Tech Nexus War Assumptions

	RMA/Ops Level (In Modern Paradigm)	Epochal/Civilizational Level (Out of Modern Paradigm)	
Nature of War	<p>Book Premise (Universal-Eternal)</p> <p>... an interaction between humans and their psychologies</p> <p>Human In the Loop Human On the Loop (Early) Old Stock Humans</p>	<p>Alternative Premise (Discontinuous Event)</p> <p>An interaction between humans (and their psychologies) and GEN (Learning) AI</p> <p>Human On the Loop (Late) Human Off the Loop No Loop (Convergence) Augmented Humans</p>	Analytical Challenge 1
Character of War	<p>Book Premise (Always in Flux)</p> <p>1920s & 1930s Equivalent Modern Military Institutions Can Adapt</p> <p>Industrial/Hierarchical State Soldiers</p>	<p>Alternative Premise (Always in Flux)</p> <p>Medieval to Modern Equivalent Modern Military Institutions Can Not Adapt</p> <p>Informational/Networked Mercenaries/PMCs</p>	Analytical Challenge 2

Source: author.

warfighting. The basic assumption is that the level of change taking place is essentially operational in scale and readily accommodated by modern military institutions which will adapt to it. The challenge to this construct is that the level of change taking place should instead be considered ‘out of paradigm’—equivalent to the shift from the classical to the medieval eras in Western civilization. This level of change ushered in technologies and advanced forms of warfighting which could not be accommodated and integrated into the prevailing feudal military system that then existed. The concern is that the advanced technologies represented by GEN AI and other forms of AI, including autonomous robots, hyperkinetic weapons, and the like, are directed energy, informational, and networked-based. These technologies far exceed the capacity of an industrial and hierarchical-based military to effectively exploit through its force structure and doctrine. The challenge thus lies in the fact that the scale of change assumed by the work is overly conservative and reinforces the status quo. Further, it does not account for the fact that mercenaries and private military corporations (PMCs) are

returning to the battlefield in mass due to the breakdown of the nation-state (Westphalian) form. It may likely be that these entrepreneurial non-state soldiers are the ones that will initially achieve the ‘mind-tech nexus’ rather than the increasingly ritualized soldiers fielded by nation-states.

The next two analytical challenges are highlighted in Table 2, which discusses the assumptions made about the paradigm in which democratic and authoritarian warfighting will occur. Some overlap exists with the initial two challenges, so redundancies exist based on the in and out of paradigm constructs discussed. However, in this instance, governance type, ethics, and morality come into play. They are as follows:

- *Analytical Challenge 3—Democratic Opportunity:* The work, given its 1920s and 1930s equivalent RMA operational-level change assumptions, views the ‘Mind-Tech Nexus’ as a challenge to which modern military institutions can readily adapt. This adaptation is considered an integration rather than a ‘bolt on’ of the technology to the present force structure. Further, and many would likely agree,

Table 2: Mind-Tech Nexus Paradigm Assumptions

	RMA/Ops Level (In Modern Paradigm)	Epochal/Civilizational Level (Out of Modern Paradigm)	
Ethical/Moral (Democratic)	Book Premise (U.S. Opportunity) 1920s & 1930s Equivalent New Operational Forces (Not Bolt Ons) Ethics is Our Strength	Alternative Impact of Human-Machine Convergence Medieval to Modern Equivalent Technology / Weaponry Too Advanced for Military System Adaptation	Analytical Challenge 3
Unethical/Amoral (Authoritarian)	Book Premise (Threat/China – Russia) 1920s & 1930s Equivalent New Operational Forces (Not Bolt Ons) Amoral Tech Integration	Alternative Threat Representation Medieval to Modern Equivalent Knight/Castle Defeated by Firearm/ Cannon	Analytical Challenge 4

Source: author.

democratic ethics are viewed as our strength rather than as a vulnerability or weakness. Still, concerns readily exist from an epochal change perspective that human-machine convergence is too advanced for our military system. It represents modern to post-modern (out of paradigm) change. The level of change derived from the advanced nature of the technology and weaponry is likely too advanced for modern military system adaptation. It is like trying to integrate a medieval host of knights and their retainers with early modern weapons, such as firearms and cannons, which their institutions simply could not accommodate. Hence, our modern system is too primitive to fully accommodate or integrate GEN AI and other advanced technologies into it. Our prevailing morality may also come into play in this regard. During the Medieval age money was considered sterile—it could not breed like animals—and usury (the charging of interest) was considered a sin and an affront to Church law. The pre-existing civilizational type could not ethically accept the advent of early capitalism and later mercantilist economic principles. Bans on firearms and other forms of

advanced weaponry also took place. Presently, our democratic values and how we envision war to be legally waged requires humans in or on the loop. Situations where humans are off the loop or where the loop disappears (due to human-machine integration) stemming from warfighting imperatives driven by technological advances will bring our democratic values and perceptions into question.

- *Analytical Challenge 4—Authoritarian Threat:* The work recognizes that the authoritarian state threats we will face in the future—with Russia and China of direct concern given that their mind-tech is discussed in dedicated chapters—will readily engage in unethical and/or amoral technology integration and weaponry fielding. This is moderated by the fact that it is taking place only within a paradigm at the operational level of change derived from a 1920s and 1930s equivalence magnitude. The challenge is that this threat will be using technology and weaponry that is out of paradigm and so advanced that it may require what we would consider to be unethical or amoral integration of it to achieve the ‘Mind-Tech Nexus’ required to effectively ‘Win Future Wars.’ Early

modern cannons effectively ended a millennium of Byzantine Empire (East Roman Empire) rule in 1453 at the walls of Constantinople. By 1494, they had also rendered medieval castles as effective defensive structures obsolete in the West. Thus, China, as a peer competitor (and the others challenging us), may benefit in their integration of these advanced technologies stemming from the amoral values that they hold. This may turn our liberal democratic values—the morality that guides us—into that which inhibits us from engaging in effective warfighting against authoritarian states. This raises the question of how to fight against such states without becoming just like them in the process. If we encounter an existential threat stemming from our inability to achieve the ‘Mind-Tech Nexus,’ a crucial post-modern warfighting capability, we will face a crisis.

SUMMARY

Human, Machine, War: How the Mind-Tech Nexus Will Win Future Wars represents a pioneering work

on an extremely important subject pertaining to U.S. national security and future warfighting. The editors Nicholas Wright, Michael Miklaucic, and Todd Veazie did a masterful job of creating the work and editing it. The reviewer readily agrees that the contributors to the work are world-class in their subject matter expertise and passion for the material that they present. The lingering question—and only time and events, both near-term and longer-term, will be the judge of this—is whether the DOW approach taken in articulating the magnitude of the warfighting (and human) impacts of the Mind-Tech Nexus is accurate. Do these technologies exist solely within the modern paradigm at the operational level or is the epochal change critique provided closer to the current reality taking place? That is to say, is an out-of-paradigm (post-modern) shift at the civilizational level now evident? This level of change is not only beyond the current perceptions of the DOW status quo but will eventually herald the emergence of an era where augmented humans (*augmentus sapiens*) begin to replace the old stock humans (*homo sapiens*) on the battlefield.⁵

Notes

¹ Kathleen Hicks. 2023. “DOD DIRECTIVE 3000.09 AUTONOMY in WEAPON SYSTEMS.” <https://www.esd.whs.mil/portals/54/documents/dd/issuances/dod-d/300009p.pdf>.

² Toffler, Alvin, and Heidi Toffler. 1994. *War and Anti-War: Survival at the Dawn of the 21st Century*. London: Little, Brown.

³ Robert J. Bunker, “The Transition to Fourth Epoch War,” *Marine Corps Gazette* 78, no. 9 (1994): 20-32 and “Epochal Change: War Over Social and Political Organization,” *Parameters* 27, no. 2 (1997): 15-25, http://scholarship.claremont.edu/cgu_fac_pub/133/. See also Robert J. Bunker and Pamela Ligouri Bunker, “The modern state in epochal transition: The significance of irregular warfare, state deconstruction, and the rise of new warfighting entities beyond neo-medievalism.” Alex Marshall, Ed, *Small Wars & Insurgencies*, Special Issue: Proxy Actors, Militias and Irregular Forces: The New Frontier of War? 27, no. 2

(2016): 325-344.

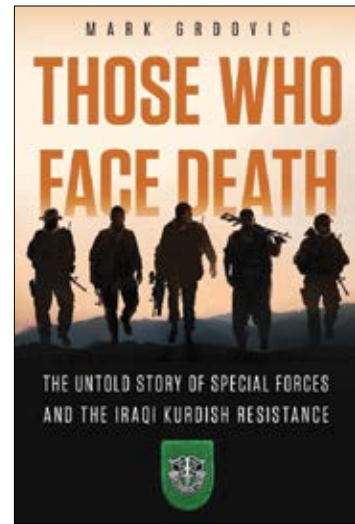
⁴ Gibson, William. 1984. *Neuromancer*. New York: Ace Books. and Stephenson, Neal. 1992. *Snow Crash*. Milano: Rizzoli.

⁵ Figure 3. 2050 Soldier Program Model portrays one vision of human, augmented, and machine soldiers’ futures. See Bunker, Robert. 2020. *Mission Command and Armed Robotic Systems Command and Control: A Human and Machine Assessment*. Land Warfare Paper 132. Arlington, VA: Association of the United States Army (AUSA): 14, <https://www.ausea.org/sites/default/files/publications/LWP-132-Mission-Command-and-Armed-Robotic-Systems-Command-and-Control-A-Human-and-Machine-Assessment.pdf>.

Those Who Face Death: The Untold Story of Special Forces and the Iraqi Kurdish Resistance

By Mark Grdovic
ISBN: 978-1963781052

Reviewed by Dr. Tom Searle



Mark Grdovic has written an excellent and important memoir about his time as a U.S. Army Special Forces soldier fighting in northern Iraq alongside the Iraqi Kurdish “Peshmerga” (Kurdish for “those who face death”) during the 2003 U.S. invasion of Iraq. Every American military officer should read this book, and it should be widely used in professional military education (PME) courses.

One reason that Grdovic’s book is so important is that it is very unusual. Military history tends to focus on big decisions at the highest strategic level, daring deeds at the most tactical level, or memoirs by former commanders. Grdovic’s *Those Who Face Death* is different. While the book includes plenty of daring deeds at the tactical level and commentary on strategic decisions, his story is about turning other people’s decisions into reality and facilitating tactical daring deeds by others. In 2003 Grdovic was a mid-career staff officer (U.S. Army Major) serving

as Operations Officer (S3) for the 3rd Battalion, 10th Special Forces Group (Airborne) (3/10 SFG).

Books like *Those Who Face Death* are vital. We do not have nearly enough of them. The overwhelming majority of an officer’s career, in peace and war, is devoted to staff work. Books that focus on national strategy or long-range sniper shots do nothing to help staff officers do their jobs, but good staff work is vital to both tactical and strategic success. Grdovic’s book is a rare and brilliant study of wartime staff work. He has a real talent for providing key details that capture what it is like to be a staff officer in extremely fluid wartime situations.

A book about staff work might sound dull, especially since the reader already knows how the story ends (Grdovic lives, Saddam Hussein is captured and executed, the Kurds continue to distrust the Baghdad government, etc.), but *Those Who Face Death* is an exciting read. Grdovic achieves this by keeping his book remarkably short, focusing on the

Dr. Tom Searle is a retired U.S. Army Special Forces officer who deployed to combat with every U.S. Army Special Forces Group. As a civilian, he has served in the Air Force Research Institute, the Joint Special Operations University, the CENTCOM J2, the SOCOM J5, and he is currently Deputy Regional Adviser for CENTCOM and SOUTHCOM in the Irregular Warfare Center (IWC).

tactical operations his staff work made possible, and providing lots of personal anecdotes that put the reader in Grdovic's boots, facing unexpected situations with inadequate information.

Grdovic is particularly good on the nerve-wracking, often surreal moments between peace and war, when everything is clouded in uncertainty. He experienced two such transitions in fairly rapid succession. First in March 2003, when he and the rest of his battalion joined the Peshmerga in northern Iraq, and again the next month, after the collapse of Iraqi Army resistance, as every Iraqi who was still alive scrambled to find their place in a new post-Saddam Iraq. In these transition moments, U.S. soldiers on the ground do not know who to trust, and about what; who to help; who to capture or kill; what promises to make, and to whom; which old promises no longer apply, etc. Months-old rules of engagement and orders from a headquarters in another country might be technically official, but such guidance can also be completely inappropriate for the current situation. In these moments, tactical decisions routinely have long-term, strategic impacts. Unfortunately, doctrine cannot prepare officers for this level of uncertainty and trying to simulate these situations in training feels artificial and contrived to the soldiers being trained. A memoir like Grdovic's is the best way to prepare officers to face these transition challenges since it provides real situations that confronted real soldiers and the messy solutions the soldiers came up with, rather than sterile, schoolhouse approved correct answers to imaginary problems.

Those Who Face Death should be assigned in PME not only for its handling of transitions between peace and war but also because it is filled with priceless gems. For example: in early May, after defeating Saddam's forces, the U.S. withdrew most of its troops from Iraq. U.S. Army Special Forces left a small stay-behind element in northern Iraq. The Special Forces battalion commander whose troops

led the stay behind force was not Grdovic's commander, but Grdovic sat in on the meeting where the battalion commander provided the following guidance: "We need to come up with a quantifiable metric for success. Something that we know we can't accomplish, and that way we will demonstrate that we're not value added and get sent home" (p. 195). Grdovic disapproved of this guidance and said so to the battalion commander, but he does not elaborate. However, this quote alone is worth a three-hour seminar discussion in any war college.

Let's consider some obvious seminar questions. The battalion commander's guidance undermines, even sabotages, the intent of Commander, U.S. Central Command (CENTCOM) in keeping forces in northern Iraq. Was that ethical or moral behavior? Given subsequent developments in Iraq, was the battalion commander correct to want the U.S. to fail quickly and leave Iraq soon? The battalion commander's officer evaluation report (OER) was not written by anyone in CENTCOM. Would he have behaved differently if CENTCOM had administrative control (ADCON) over him, and hence wrote his OER, instead of merely operational control (OPCON)? How might attitudes like those of the battalion commander enable the rise of an Iraqi insurgency? Where did the battalion commander get his "fail so we can go home" attitude? Was he responding to the belief that U.S. forces stayed too long in Bosnia in the 1990s? Was he thus "fighting the last war" (Bosnia) in a way that was counterproductive to his current task of stabilizing post-Saddam Iraq? Did a generation of U.S. Army officers "learn" equally counterproductive "lessons" from decades in Iraq and Afghanistan? What might those counterproductive lessons be and how should PME counter them? The questions are endless, fascinating, and vitally important. The answers are complex and will force PME students out of their comfort zone into the real world where there are few obvious right answers. Grdovic's book

is much too short to debate these questions, but the reader should consider them, and the book provides many gems like this worthy of careful thought and analysis.

Grdovic's book also provides valuable reminders of the consistent mistakes made in wartime. For example, the further back from the fighting a headquarters is, the more likely it is to be safe, and overwhelmingly staffed with U.S. personnel. By contrast, the further forward soldiers are, the less safe they are, and the more foreign forces and civilians are part of their daily experience. Grdovic is shocked when he leaves the front and goes to a U.S. headquarters where they believe the fighting has been easy and that the local forces do not matter. He should have anticipated this, and, more importantly, leaders in headquarters to the rear should actively guard against triumphalist attitudes that devalue allies and partners.

Another enduring wartime challenge is that units new to the fight do not know what actions are dangerous, and which ones are safe. Grdovic's description of fratricide events that were barely averted and the inability of 173rd Airborne Brigade to effectively engage the Iraqi army show this struggle from the point of view of the "old timers" who know what is and is not safe. Grdovic was on the other side of this point-of-view challenge when he thought the Peshmerga needed to dig fighting positions to defend against a night counterattack and the Peshmerga laughed at the idea of a night attack. (The Pesh were right; Grdovic was wrong.)

To his credit, Grdovic is not content to merely provide a memoir of his experiences and the accomplishments of 3/10 SFG in the spring of 2003. Instead, he adds three useful sections that take the reader beyond 3/10 SFG and 2003. These three bonus sections are an epilogue and two appendices. The epilogue describes his second tour in Iraq in 2007-2008 when he was the liaison officer representing Combined Joint Special Operations Task Force

– Iraq (CJSOTF-I, commanded by a colonel) in the Headquarters of the four-star command, Multi-National Forces – Iraq (MNF-I). The epilogue connects the brief and relatively little known 2003 counter-Saddam fight in northern Iraq with the much-longer and better-known counterinsurgency fight across Iraq. It provides the perspective of a staff officer trying to connect two headquarters rather than operate in one headquarters.

The first appendix, "Why We Were Successful in Our Special Operations," identifies eight specific factors that contributed to the success of 3/10 SFG and the Patriotic Union of Kurdistan (PUK). Some, like good pre-mission training, are things the reader can try to replicate in future conflicts. Others, like Iraqi vulnerabilities or the strength of the PUK as a partner force, were outside the control of 3/10 SFG. Perhaps he should have included U.S. airpower as another fortuitous factor, but it is a credit to Grdovic that he does not merely list things he and his commander did right but also highlights good fortune that made their success possible. The second appendix, "Observations for Unconventional Warfare," seeks to draw specific lessons from his operations in northern Iraq for the larger theoretical and doctrinal debates about outside support to resistance and insurgent forces. Both appendices draw on Grdovic's years as an instructor and decades studying these issues and have obvious relevance for doctrine and PME.

Grdovic's first-person point of view is the book's greatest strength, but it comes with challenges the reader should keep in mind. For example, Grdovic was the S3 of 3/10 SFG, fighting side by side with Peshmerga from the PUK. He very rarely says anything negative about anyone in 3/10 SFG or the PUK. On the other hand, the PUK's rivals from the Kurdish Democratic Party (KDP) and U.S. forces other than 3/10 SFG are rarely mentioned in a complimentary fashion.

Grdovic's love for his comrades, and impatience with everyone else, is mostly harmless, and even charming. However, it is dangerous when he fails to assess possible weaknesses in the performance of 3/10 SFG and the PUK. For example, the assault on the Ansar al Islam stronghold near Halabja (Operation VIKING HAMMER) was a fierce battle and makes for very exciting reading. The PUK won the battle decisively, with the assistance of 3/10 SFG and U.S. air strikes. This was an enormous and extraordinary achievement since irregular forces like the PUK are ill suited to conduct a deliberate assault on a fortified position like the Ansar stronghold. Nevertheless, capturing some trenches and damp bunkers in a remote portion of the Iraq/Iran border, while significant, may have been less so than capturing or killing any terrorists assembled there. If so, then the plan should have focused on how to capture or kill the terrorists when they tried to escape into Iran. That was the lesson of Tora Bora, Afghanistan, less than two years earlier, and a lesson ignored in the fight against Ansar. Likewise, Grdovic is entirely correct to point out the flaws in the Free Iraqi Forces scheme, but his suggestion that his Kurdish PUK forces could have solved the problem by taking a large role in securing non-Kurdish areas of Iraq seems dubious, at best.

Lastly, this review concludes by giving Mark Grdovic credit for the extraordinary honesty he displays in his memoir. Most of us will only tell a story after we determine what the story means and after we have edited it to convey that meaning. Grdovic tells us what he said, heard, thought, and did, even when he is not sure what conclusion we will draw.

SUBSCRIPTIONS

To request a hard copy of *PRISM: The Journal of Complex Operations*, contact the PRISM editorial staff at PRISM@irregularwarfarecenter.org. Please include your preferred mailing address and desired number of copies in your message. Note that supplies of hard copy may be limited due to high demand.

