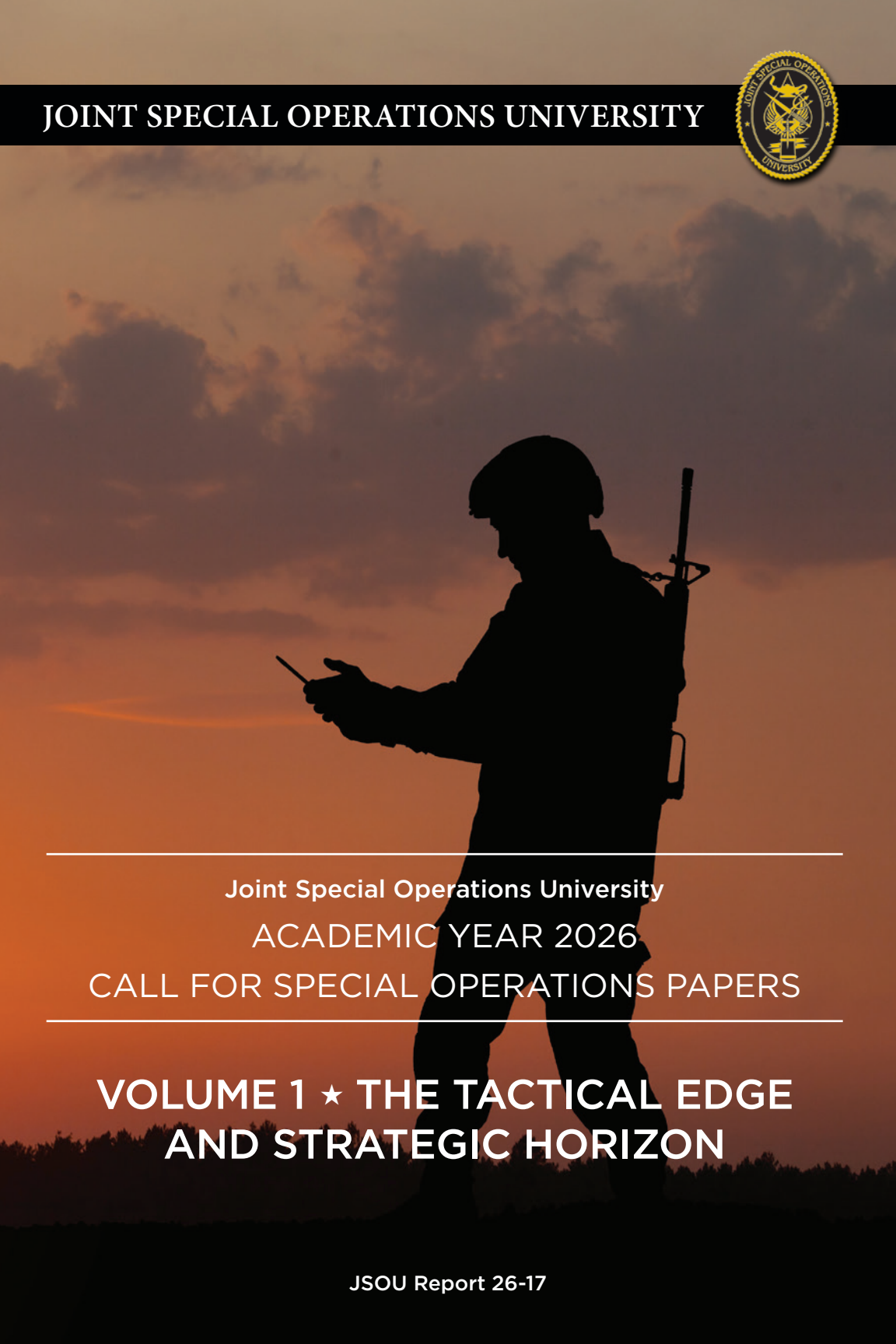
JOINT SPECIAL OPERATIONS UNIVERSITY



Joint Special Operations University

ACADEMIC YEAR 2026

CALL FOR SPECIAL OPERATIONS PAPERS

VOLUME 1 ★ THE TACTICAL EDGE AND STRATEGIC HORIZON

JSOU Report 26-17

JSOU PRESS
JOINT SPECIAL OPERATIONS UNIVERSITY

Joint Special Operations University

ACADEMIC YEAR 2026
CALL FOR SPECIAL OPERATIONS PAPERS

Volume 1 ★ The Tactical Edge and Strategic Horizon

JOINT SPECIAL OPERATIONS UNIVERSITY
MacDill Air Force Base, Florida | November 2026

JSOU Report 26-17

On the cover: A silhouette of a soldier using a drone and laptop computer for scouting during a military operation. Source: hamara/ Adobe Stock

The views expressed in this work are entirely those of the author and do not necessarily reflect the views, policy, or position of the U.S. Government, Department of War, United States Special Operations Command, or the Joint Special Operations University.

JSOU PRESS

Melanie Casey, Editor in Chief
Beth DeGeorge, Editor
Alina Alvarez Perez, Editor
Arianna Czesler, Designer
Rebecca Kurk, Designer

This work was cleared for public release; distribution is unlimited.

Published November 2026

ISBN 978-1-941715-89-5

jsou.edu/press

Table of Contents

Foreword. 1

Acknowledgements 3

Categories 5

Chapter 1

Optimizing Drone Use and Counter-Unmanned Aircraft Systems Strategies 7

Beyond the Golden Hour: Autonomous Logistics and Air-Ground Teaming in Denied-Access Environments

Irakli Kharebashvili. 9

From Proxy Drone Warfare to Sahelian Adaptation: The Partner Defense Gap SOF Cannot Ignore

Maj. Imad Ammouri 29

"Truly Cheap" Uncrewed Systems for Great-Power Competition: Strategic Relevance for Special Operations Forces

AJ Rutherford, PhD 51

Chapter 2

Rapid All-Domain Fusion for SOF. 81

Architects of Fusion: A Mission-Focused Model for Rapid All-Domain Fusion for SOF

Maj. Scott C. Hall 83

Meritocracy Resourcing

Cmdr. J. A. Spector 105

A New Approach to Risk That Supports Rapid Decision-Making

Lt. Col. Michael C. Tinker. 129

Accessing Denied Digital Terrain: SOF-Enabled Access for Cyber Operations
2nd Lt. Carson Tucker 155

Chapter 3

The Space-Cyber-SOF-Strategic Command Nexus: How To Build Capabilities Greater Than the Sum of Its Individual Parts 175

Joint Special Operations Task Force 2030: Weaponizing the Nexus
Lt. Col. Michael Hagan 177

There's No One to Take Your Call at This Time: Operating Without Reachback—Decision Continuity at the Space–Cyber–SOF–STRATCOM Nexus
Ryan K. Kaono-Wedemeyer 193

Layered Global Presence and Twin Peaks: Aligning Special Operations Forces and Strategic Assets in Campaigns
Lt. Col. Jaewook "Jay" Lee 215

Advanced Resilience and Resistance in Digital Battlespaces: Countering Multiplatform Influence Operations Through Adaptive Communication Networks
Troy C. Troublefield, PhD 247

Chapter 4

Digital Force Protection: Threats and Risks to SOF 281

From Signature Reduction to Digital Force Protection: Operationalizing Counteroffensive Irregular Warfare in the Digital Domain
Christopher Moede 283

Digital Force Protection in the Age of Social Media Intelligence and Open-Source Intelligence: Threats and Risks to SOF—and a Blueprint to Counter Them
Claire Moravec 295

Frail, Fragile, or Both? An Evaluation of Cyber Resilience in Critical Infrastructure
Renita Murimi, PhD 309

Building a Complex Adaptive National Immune System: Counterintelligence—the Core of This System
Michael W. Parrott 343

Digital Force Protection: Lessons from China's Global Television Network Economic Messaging and Market Dynamics
Sonny S. Patel, PhD, MPhil, MPH, and Carol Kay Winkler, PhD, MA 377

Digital Force Protection in the Public Sensorium: A Counterintelligence Playbook for SOF Against Open-Source Intelligence Targeting, Narrative Preconditioning, and Ambient Data Trails
Chief Warrant Officer 3 (Ret.) Wayne N. Taylor, EdD, PhD(c) 413

Chapter 5

Next Generation Intelligence, Surveillance, and Reconnaissance 441

Digital Shadows in the Human Domain: How Augmented Reality and AI Could Redefine Civil Affairs
1st Sgt. Nathan Greene 443

2027 Call for Special Operations Papers 467

Foreword

The strength of the special operations forces (SOF) enterprise rests not only on advanced capabilities and exceptional people, but also on its ability to anticipate change, challenge conventional thinking, and translate innovation into operational advantage. As the strategic environment grows more complex, SOF must continue to adapt to emerging threats, integrate new technologies, and strengthen its ability to enable theater special operations commands (TSOCs) and the joint force in advancing national security objectives.

In Academic Year (AY) 2025, the Joint Special Operations University (JSOU) launched its inaugural Call for Special Operations Papers to capture innovative ideas, operational insights, and practical solutions from across the SOF enterprise. The response demonstrated a strong appetite for intellectual engagement, with 43 submissions and 15 papers selected for publication.

Building on that success, JSOU focused its AY2026 Call for Special Operations Papers on technology and its implications for special operations. Contributors were challenged to examine how emerging technologies are changing the character of competition and conflict. The response exceeded expectations: 82 submissions—a resounding success that reflects the enterprise's commitment to advancing the profession through intellectual inquiry.

Of those submissions, 47 were selected for publication. Eighteen are featured in this first volume, *The Tactical Edge and Strategic Horizon*. Collectively, these papers explore next-generation intelligence, surveillance, and reconnaissance; the SOF nexus; digital force protection; rapid all-domain fusion; and unmanned systems. Each addresses challenges and opportunities with direct implications for SOF readiness, operational reach, decision advantage, and the ability to integrate effectively with the joint force.

These contributions are particularly important as SOF operates across increasingly contested, complex, and interconnected environments. Technology offers significant potential to improve situational awareness, accelerate decision-making, enhance force protection, and strengthen the integration of capabilities across domains. Realizing that potential, however, requires more than acquiring new tools. It demands an understanding of operational requirements, the ability to integrate capabilities into existing formations and processes, and the capacity to translate technological advances into practical solutions that support TSOC missions and joint force objectives.

We encourage readers to consider not only the individual arguments presented in these papers, but also how their insights can inform operational planning, capability development, professional military education, and force integration.

The future of special operations will be shaped not simply by the technologies we develop, but by how effectively we integrate them, employ them, and prepare our people to turn innovation into operational advantage.

Command Sgt. Maj. Justin Johnson
Command Senior Enlisted Leader
Joint Special Operations University

Paul D. Brister, PhD
President
Joint Special Operations University

Acknowledgements

When JSOU launched its first Call for Special Operations Papers in the fall of 2024, we had no idea what to expect. At the time, we defined success as receiving 15 submissions. We exceeded our expectations (with 42), but the true measure of success was the impact several of those papers had in generating meaningful discourse and real change across USSOCOM.

For the AY26 effort, we narrowed the focus to technology in SOF, introduced a fiction category, and hoped to continue the momentum of the previous year. The response this year exceeded even our most ambitious expectations: 82 papers were submitted across four categories, what we jokingly refer to as "catastrophic success."

Reviewing and evaluating these submissions to identify category winners and high-scoring, publishable papers was no small undertaking. My sincere thanks to the reviewers whose dedication, expertise, and willingness to carve time out of already demanding schedules made this effort possible: Maurice "Duc" DuClos, Chris Greenfield, Janine Hargrett, Doug Jordan, Gessica Lillitch, Jeremiah "Lumpy" Lumbaca, Ian MacClure, Michael Parrott, John Pennell, Christiane Thompson, and Rob West. You are all rock stars.

Once the judging process concluded and category winners were selected, the small-but-mighty JSOU Press editorial team took over. From mid-April through May, Beth DeGeorge and Alina Alvarez Perez worked tirelessly to edit and digitally design the top three papers in each category in time for SOF Week, where the winners were recognized by USSOCOM Commander Adm. Frank M. Bradley. Additional high-scoring papers then entered the editorial queue, and the team, supported by contract editor Kelly Alves, turned its attention to editing the remaining 35 papers and preparing them for publication.

Our new press designer, Rebecca Kurk, assisted by JSOU graphic designer Arianna Czesler, then undertook the formidable challenge of developing a three-volume print series. Countless hours were invested across the entire team in editing, reviewing, fact-checking, formatting, and designing this collection to ensure it met the high standards of both JSOU and USSOCOM. The team's commitment to academic rigor, accuracy, consistency, and readability is evident on every page. It is a privilege to work alongside such a talented and dedicated group of professionals.

Finally, I'd like to thank the authors who contributed to this volume. Their work continues to advance the thinking, capabilities, and effectiveness of the special operations community.

Melanie Casey
JSOU Press Editor in Chief
October 2026

JSOU AY26

Call for Special Operations Papers

Categories

Categories for AY26 submissions were similar to the AY25 call, with one addition—fiction.

Top papers are listed first in their chapter and identified on the title page.

Category 1 Military practitioners and professional military education students

Category 2 International allies and partners

Category 3 Academic faculty and scholars

Category 4 Fiction

Chapter 1

Optimizing Drone Use and Counter-Unmanned Aircraft Systems Strategies

The rapid proliferation of unmanned aircraft systems (UAS) is transforming the character of conflict. This creates new opportunities for SOF, but it also introduces unprecedented operational challenges. Tactical reconnaissance and low-cost drone swarms are reshaping how military power is projected and contested across domains.

The papers in this section explore how SOF can harness these capabilities to enhance operational effectiveness while developing resilient counter-UAS approaches. Contributors examine advances in autonomous logistics and air-ground teaming, the growing role of proxy drone warfare, and the use of uncrewed systems as instruments of strategic competition. Collectively, these studies assess how SOF can integrate, adapt, and innovate to maintain operational advantage in increasingly contested and dynamic environments.

Beyond the Golden Hour: Autonomous Logistics and Air-Ground Teaming in Denied-Access Environments

By Irakli Kharebashvili

This is the JSOU AY2026
Call for Special Operations Papers

Category 2

First-Place
Winner

Digital Version

Abstract

Special operations forces (SOF) planning has long rested on a working assumption: that air or ground support will be available at the critical moment. Operational reality, however, consistently exposes the fragility of that assumption. When a mission exceeds its ideal scenario and a team finds itself isolated in denied territory—cut off by an adversary's integrated defense architecture—conventional extraction methods become catastrophically inadequate. In conditions where the enemy maintains layered anti-access capabilities, dispatching any piloted platform, whether aircraft or heavily armored ground vehicle, places its crew at mortal risk. Armor can absorb rounds; it cannot absorb the political and human cost of losing the people inside it.

This research analyzes the operational dead end created by that dependency and proposes a paradigm shift: a move away from piloted heroic rescuers toward autonomous expendable systems. The argument is that the solution is not better armor but the systematic replacement of human operators with robotic platforms capable of functioning in GPS-degraded environments, and whose destruction does not constitute mission failure.

Introduction: The Operational Impasse and the Survival Paradox

The history of special operations is written in tactical brilliance, but its most painful chapters record the moments when Plan A failed. When a small team is encircled deep in enemy territory, the immediate demand is for emergency resupply or extraction. Conventional doctrine responds with the deployment of Quick Reaction Forces (QRF). In modern conflicts where adversaries field high-precision targeting systems, however, the act of sending a

The most protected vehicle on the battlefield still carries people inside it, and a precisely delivered weapon can kill them regardless of the steel surrounding them.

rescue force frequently generates a larger tragedy than the crisis it was dispatched to resolve.

The historical precedents are unsparing. In June 2005, during Operation RED WINGS in Afghanistan's Kunar Province, the QRF dispatched to reach four encircled operators was carried by an MH-47 Chinook—call sign Turbine 33. A single RPG-7 round brought it down, killing all 16 special operations personnel aboard.[1] A decade earlier, in the October 1993 Battle of Mogadishu—the Black Hawk Down engagement—the ground convoys sent to recover downed pilots and isolated soldiers found themselves channeled into kill zones in the city's narrow streets. Despite operating in armed high mobility multipurpose wheeled vehicles (HMMWVs), the convoy suffered serious casualties; the lead vehicle's driver being hit was enough to stall the entire column and convert it from a rescue force into a stationary target.[2]

These cases share an underlying failure mode. They reveal a systemic flaw in how logistical and casualty-evacuation doctrine has been constructed: a structural dependency on piloted platforms that, once inserted into a denied environment, become liabilities rather than assets. When a situation deteriorates, commanders face a choice between two bad options: abandon the isolated force or send additional crewed platforms into the same threat environment. Armor offers no escape from this paradox. The most protected vehicle on the battlefield still carries people inside it, and a precisely delivered weapon can kill them regardless of the steel surrounding

them. One hit does not merely destroy the machine; it creates new casualties and demands a new rescue operation.

The logical conclusion, which this research develops at length, is that the only durable solution is the removal of human beings from the last mile of logistics and evacuation. SOF units must transition to multifunctional, modular robotic systems—platforms in the class of the THeMIS unmanned ground vehicle (UGV)—capable of operating without satellite navigation in degraded electromagnetic environments.

These platforms should not be conceived narrowly as carriers. They are, properly understood, autonomous combat units whose functional portfolio includes:

Logistics and evacuation: delivering heavy cargo and extracting wounded personnel from complex terrain without exposing human operators to direct fire.

Fire support: remote-controlled weapon stations mounting heavy machine guns or grenade launchers, enabling an isolated team to generate suppressive fire without breaking cover.

Multi-domain strike: the ability to launch loitering munitions or deploy ground assault robots directly from the forward position, converting a survival situation into an active offensive posture.

The primary advantage of this architecture is not technological but ethical and strategic. When a robot is destroyed, the mission loses metal and circuitry, not elite soldiers. That distinction is the only sustainable path through the constraints the golden hour imposes and through the far more demanding constraints that a peer-competitor threat environment now creates.

Part I: The Historical Imperative—An Anatomy of Failure

Contemporary SOF doctrine rests on the premise that technological superiority and professional excellence can compensate for numerical disadvantage. Three decades of operational data, however, consistently show that this equation breaks down when the operational environment shifts into denied-access territory. The heaviest SOF casualties across that period have accumulated not during the objective phase of operations but during logistical support, exfiltration, and—most alarmingly—during the rescue operations triggered by those failures. The two cases examined below are not merely historical curiosities; they are the foundational evidence for the argument.

The Tyranny of Terrain: Operation RED WINGS and the Communications Vacuum

Operation RED WINGS, conducted in June 2005 in Afghanistan's Kunar Province, is a precise illustration of how mountain terrain dismantles high-technology advantage. A four-man reconnaissance team was inserted onto the steep, fractured ridgelines of the Hindu Kush at elevations approaching 3,000 meters above sea level.[3]

The first and decisive failure was the line-of-sight problem. The team's primary communications equipment, Army/Navy Portable Radio Communications (AN/PRC)-148 radios and satellite phones, proved useless in the shadow of the rock massifs. The terrain physically blocked radio frequency signal propagation to the operations center and to orbiting satellites. To attempt communications, the team was forced to abandon their concealed position and move to an exposed, elevated location. That movement was the act that led to their compromise and eventual encirclement.

Operators are forced to risk their lives simply to establish communications, and commanders are compelled to commit aviation into environments where the probability of survival is minimal.

The tragedy compounded when standard rescue protocols were activated. The QRF dispatched aboard MH-47 Chinooks encountered an adversary that possessed the high-ground advantage, used terrain for concealment, and needed only a shoulder-fired rocket-propelled grenade (RPG)-7 to bring Turbine 33 down. The slow, acoustically conspicuous approach of a heavy helicopter into a confined mountain landing zone is among the most predictable and targetable events in modern warfare.

The outcome: a rescue mission launched to reach four men resulted in the deaths of 16 more. Operation RED WINGS is evidence of what happens in the absence of autonomous relay and logistics systems. Operators are forced to risk their lives simply to establish communications, and commanders are compelled to commit aviation into environments where the probability of survival is minimal.

The Urban Trap: The Mogadishu Lesson and the Vulnerability of Convoys

Where Red Wings illustrates the dangers of mountain terrain, the Battle of Mogadishu on October 3 and 4, 1993—the Black Hawk Down engagement—reveals the logistical nightmare of urban operations. The downing of two UH-60 Black Hawks converted a tactical raid into a large-scale rescue operation in a matter of minutes.[4]

Urban environments create what analysts call "urban canyons"—corridors between high buildings that restrict maneuver and create ideal conditions for vertical ambush from rooftops and upper floors.[5] The ground relief convoy, commanded by Lt. Col. Danny McKnight and composed of armed HMMWVs and cargo trucks, moved into these corridors and found itself in exactly that situation.

Despite being mechanized, the convoy was critically dependent on its human crews. Drivers and gunners were the primary targets. When the lead vehicle's driver was hit, the entire column stopped—transforming a moving force into a stationary one—and casualties multiplied. The logistical convoy dispatched to save lives became itself a generator of mass casualties.

Mogadishu exposes a fundamental paradox: in urban combat, the attempt to evacuate casualties using crewed vehicles, even armored ones, frequently costs more in resources and lives than the original loss. Crews experience performance degradation under fire, make navigational errors (as happened repeatedly that night), and require protective armor at a level that reduces the vehicle's mobility and compounds its problems in confined streets.

The Blood Price and the Negative Feedback Loop

Despite their geographic and operational differences, both cases reveal the same statistical anomaly: the casualty multiplication effect in rescue operations. Data from U.S. Department of Defense after-action reviews, dating from Vietnam through the conflicts of the post-9/11 era, show that combat search and rescue (CSAR) and QRF operations consistently produce losses among rescuers alongside or in addition to those among the people being rescued.[6]

In the hybrid conflict environment of today, where adversaries routinely field inexpensive but effective anti-tank guided missiles and man-portable air defense systems (MANPADS), the use of

piloted platforms for logistics and evacuation generates what can be characterized as a negative feedback loop:

- An isolated team requests assistance.
- A piloted platform—helicopter or armored vehicle—is dispatched.
- The platform is destroyed on approach.
- A second rescue operation is required, this time to recover the rescuers.

This cycle continues until the supporting force commits overwhelming firepower or abandons the operation. The golden hour—a standard from trauma medicine describing the window of maximum intervention effectiveness—becomes a tactical trap. The existing record makes the conclusion unambiguous: as long as last-mile logistics and evacuation depend on human physiology and crewed platforms, SOF operations in denied environments will remain perpetually exposed to catastrophic loss. What is required is not an incremental improvement but a structural replacement: a system whose loss is measured in procurement budgets, not in body bags.

Part II: The Denied Environment and Its Technological Constraints

Part I examined cases in which failure was driven principally by terrain complexity and tactical miscalculation. This section addresses a categorically different and more severe problem: technological and strategic blockade. The term "denied environment" has become a term of art in contemporary military doctrine. It describes a combat space in which coalition forces lack air superiority and freedom of maneuver—not because of bad decisions but because the adversary has fielded systems specifically designed to deny

them. In the era of Great Power competition, where potential adversaries possess sophisticated integrated defense architectures, reliance on conventional air assets or even aerial drones is not merely ineffective; it constitutes operational self-defeat. The three factors examined below explain why any approach built around air dependency is without prospect.

The Anti-Access/Area-Denial Canopy and the Closure of Airspace

The most consequential development in modern conflict is the mass proliferation of anti-access/area denial (A2/AD) strategies. Russian S-400 and Chinese HQ-9 type integrated air defense systems generate layered defensive envelopes within which any non-stealth aircraft becomes an immediate targeting solution. Detection ranges, engagement altitudes, and response times have been transformed to a degree that makes traditional CSAR platforms operationally irrelevant.

In such conditions, the MH-60 Black Hawk and CH-47 Chinook—the workhorses of SOF extraction—lose their functional value entirely. These are large, slow platforms with high radar and infrared signatures. In local conflicts, the dominant threat is short-range MANPADS; in an A2/AD environment, the threat begins at hundreds of kilometers' distance. When a special operations team is operating deep in denied territory, dispatching a helicopter for extraction is impossible without first conducting a large-scale suppression of enemy air defenses—an operation that requires hours or days, which the crisis does not permit. The conclusion is direct: aerial evacuation, as a reliable capability, is not available in a denied environment.

Physics and Energy: The Limits of Aerodynamics

A common rejoinder to this problem is that piloted aviation can be replaced by unmanned aerial systems of small or medium scale. The laws of physics and thermodynamics impose strict limits on the validity of that argument.

Payload deficit: Overcoming gravity continuously is energetically expensive. A vertical take-off and landing drone capable of evacuating a single combat-loaded soldier—carrying approximately 90-100 kg of equipment—requires large rotors and powerful motors. A platform with those specifications approaches the size of a light helicopter and presents a comparable radar signature. Smaller drones simply lack the physical capacity to carry meaningful logistical loads.

Energy density: Lithium-ion battery technology has not yet enabled extended flight under load. A tactically relevant cargo drone typically has 20 to 30 minutes of flight endurance at capacity—wholly insufficient for exfiltration from operational depth. A ground vehicle, by contrast, expends zero energy while stationary, which radically extends the autonomous operating time available to a UGV.

Environmental conditions: High-altitude terrain—the Caucasus range being a relevant example—is characterized by unpredictable meteorological conditions. High winds, descending air currents, and snowfall regularly render aerial drones inoperable. Ground robotic systems maintain operational capability in conditions where flying platforms physically cannot function.

The Invisible Front: Electronic Warfare

The third and perhaps most critical constraint is electromagnetic spectrum control. Modern peer-competitor conflict is in large part an electronic warfare contest, and the absolute majority of both

commercial drones and military platforms depend critically on GPS signals for navigation.

Adversary systems such as the Krasukha-4 and Zhitel jammers generate powerful interference fields that not only suppress satellite signal (jamming) but also transmit false coordinate data (spoofing). Under spoofing, a drone receives incorrect positional information, loses orientation, and experiences what operators call "fly-away events"—uncontrolled flight toward obstacles. In a denied environment, satellite navigation is wholly unreliable. For an aerial drone, GPS loss is often catastrophic because the platform cannot maintain positional stability in the air without it. For a ground-based autonomous system, the same event is a manageable interruption: the platform can halt safely and transition to satellite-independent navigation using visual-inertial odometry, camera arrays, and LiDAR technology.

The combined effect of A2/AD coverage, aerodynamic energy limits, and intensive electronic warfare creates an environment in which the sky is closed. Opening and maintaining a logistical corridor is only possible with systems that operate firmly on the ground: platforms with high mobility, energy efficiency, and independence from space-based infrastructure.

Part III: The Technical Solution—The "Mother Platform" and Autonomous Teaming

The physical and technological constraints identified in the preceding sections make one thing clear: supporting an isolated SOF team in a denied environment using conventional single-unit piloted platforms is no longer viable. The only path to operational continuity in a denied environment runs through decentralized, robotic, and multifunctional architecture. The answer is not a single universal

machine; it is a coordinated team of specialized autonomous systems built around what this research calls the "Mother Platform."

This section details the technical and operational mechanisms through which multifunctional UGVs integrate with each other, exercise autonomous decision-making, and deliver logistical fire support and communications capabilities in a fully autonomous operational mode.

The Multifunctional Concept and Team Symbiosis

When an isolated SOF team requires immediate support, what is dispatched is not a single platform but a networked group of interconnected robotic systems. The Mother Platform concept is built on modularity: the base chassis is common, but the payload configuration determines the platform's role in any given mission. An optimally composed support team consists of three distinct functional profiles:

Logistics and evacuation platform: This system's primary mission is heavy cargo transport—delivering ammunition, water, and medical supplies directly to the point of contact, then transitioning automatically to evacuation mode to extract casualties from the position.

Fire support and strike platform: This is the direct combat module, equipped with remote-controlled or autonomous heavy machine guns (12.7mm caliber class) and anti-armor systems. Critically, the Mother Platform also functions as a mobile launch platform as containerized tubes for loitering munitions are integrated into the chassis. When the team is encircled, this platform opens suppressive fire while simultaneously releasing loitering munitions against enemy sniper positions or ambush elements, creating the maneuver corridor the isolated team needs.

Communications and relay platform: This system's sole mission is signal continuity. It carries high-power antenna arrays, signal amplifiers, and cryptographic modules, and functions as the network's backbone node when terrain would otherwise sever communications.

The combined operation of these three systems creates a synergy in which each robot compensates for the others' limitations, without placing human beings in the path of any of the threats that make the environment denied.

Intelligent Coordination and the Mesh Communications Architecture

The tragedy of Operation RED WINGS traces directly to signal blockage by terrain. The technological solution to that failure is a closed, decentralized mesh network connecting the autonomous platforms to each other and to the team they are supporting.

Unlike standard communications architectures in which signals must reach a headquarters antenna or satellite directly, in a mesh network, every robot constitutes an independent node. When the support group approaches difficult terrain—a deep valley, an urban canyon, or a forested ridgeline—the system makes an automatic tactical decision. The communications platform does not descend into the valley; it stops on an elevated feature and assumes the role of a relay node. The logistics and fire support platforms continue moving toward the isolated team along the valley floor. The data they collect—video feeds, voice communications, sensor readings—are relayed to the communications platform on the ridge, which forwards that signal to command or to a satellite.

If any node in the network is destroyed by enemy fire, the mesh network's self-healing capability automatically reroutes the signal through the remaining nodes; communications are not interrupted.

This approach eliminates the communications vacuum that proved fatal in the Hindu Kush, even in the most constrained and enclosed geographic areas.

Hybrid Vision: Air-Ground Integration and Autonomous Route Generation

The central navigation challenge for autonomous systems is operating in pathless, chaotic terrain. The Mother Platform is equipped with LiDAR, thermal cameras, and other sensor arrays, but ground-level sensor coverage is always limited by natural obstacles: rock faces, buildings, dense vegetation.

This is where the platform's mothership function becomes fully apparent. When the ground robot encounters an impassable obstacle or cannot identify a safe route to the objective, it does not wait for an operator's instruction. The system automatically opens a hatch in the upper chassis and deploys its integrated reconnaissance quadcopter. This small drone, which may operate on a tethered cable for unlimited power supply or in free-flight mode, rises to 50–100 meters above the ground.

From that altitude, it conducts a 3D terrain scan and streams topographic data in real time to the Mother Platform below. The system's onboard AI—using object recognition architectures trained to classify enemy positions, mined areas, and natural barriers—processes the aerial view in seconds. Drawing on the resulting data, the UGV autonomously generates a new safe route. This is absolute air-ground hybrid coordination: the ground machine uses its own embedded aerial eye to perceive the operational space and makes its navigational decision on the ground, without operational delay.

> *The Mother Platform architecture is not, in any useful sense, a remote-controlled truck. It is a cognitive, multilayered system capable of resolving navigation problems through air-ground synergy, constructing a resilient communications mesh across the most demanding terrain, and serving as the strategic link between the point of contact and the joint force.*

Strategic Synchronization and Integration with Joint Forces

The capabilities of the Mother Platform and its robotic team are not confined to the immediate support of an isolated group. Under current doctrinal thinking, this autonomous team constitutes an active forward node of the global combat network: the Joint All-Domain Command and Control (JADC2) architecture.

When a UGV detects an adversary position through its own sensors or through data from its aerial drone (i.e., enemy artillery, an air defense emplacement, a logistics hub) it does not rely solely on its own weapons. The platform's computational core automatically calculates the target's precise geolocation, accounting for elevation, distance, and movement vector. This targeting data is transmitted in milliseconds through the mesh network not only to the central command post but also directly to other combat systems operating in the region.

In practice, this means a ground robot can function as a fully capable Joint Terminal Attack Controller. It can establish direct data links with F-35 aircraft overhead or with rear-area rocket artillery systems, such as HIMARS, and supply precisely refined coordinates for air or artillery strikes. A robotic team originally dispatched on

a logistics mission becomes, through this synchronization, the coordinating center for massive firepower delivery in the adversary's rear area.

The Mother Platform architecture is not, in any useful sense, a remote-controlled truck. It is a cognitive, multilayered system capable of resolving navigation problems through air-ground synergy, constructing a resilient communications mesh across the most demanding terrain, and serving as the strategic link between the point of contact and the joint force. This approach fundamentally reshapes the paradigm of rescue and support operations—establishing technological autonomy as the primary guarantee of combatant survival.

Conclusion and Strategic Recommendations

The analysis of contemporary combat operations and the technological realities of Great Power competition point to a structural truth that is no longer comfortable to ignore: air superiority and continuous communications are no longer guaranteed inputs to operational planning. Historical precedents have demonstrated, with substantial loss of life, that conducting rescue and logistics operations in complex terrain or urban environments using piloted platforms regularly ends in catastrophic casualties.[7] The attempt to preserve the golden hour for isolated personnel—at the cost of human operators, in environments saturated by A2/AD systems and intensive electronic warfare—is a strategic dead end.

The way out of that dead end is not the incremental modernization of existing methods but a radical paradigm shift. SOF must relinquish the human operator from the logistics and evacuation chain and transition to fully autonomous, decentralized robotic ecosystems. As this research has argued, reliance on aerial

drones alone is rendered ineffective by the hard constraints of physics and energy. The future belongs to multifunctional ground systems—autonomous Mother Platforms operating on principles of team symbiosis.

These intelligent systems are not simply cargo carriers. They are modular combat units that construct their own resilient mesh communications architecture independent of terrain, provide substantial fire support, and function as mobile launch platforms for reconnaissance or loitering munitions delivered directly from the hot zone. Through the integration of AI and air-ground hybrid vision, they are capable of autonomous navigation under complete GPS denial and real-time transmission of targeting data to the joint force network: JADC2.

The ultimate value of this technological transition is not tactical but ethical and strategic: it is expandability. When an operation exceeds its ideal scenario, and an elite team finds itself isolated in a denied environment, we must send metal and algorithms to save human beings. The destruction of a robot is a procurement cost. The death of a rescuer is a national tragedy.

Recommendation: The United States Special Operations Command and the armed forces of partner nations should redirect research and development priorities of the coming decade toward integrated, multifunctional ground-air ecosystems. Immediate doctrinal revision is needed to establish Mother Platform teams as the standard primary response and evacuation capability in critical situations. This is the only instrument capable of securing advantage in the asymmetric, technologically saturated conflicts of the future.

About the Author

Irakli Kharebashvili is a security researcher and robotics engineer based in Tbilisi, Georgia. He holds a Bachelor of Business Administration from Ilia State University and a Master of Security Studies from the National Defence Academy of Georgia.

Irakli has over seven years of professional experience within Georgia's public service and government structures, specifically in the security sector. His tenure has been focused on operational and technical matters, providing him with deep tactical knowledge and practical experience that complements his theoretical research.

He is the co-founder and Lead Systems Architect at KineCore, where he manages the R&D center dedicated to the development of autonomous ground systems. His technical work involves hardware engineering and the deployment of Edge AI and computer vision models on NVIDIA Jetson modules for GNSS-denied environments. By integrating his academic, tactical, and technical expertise, Irakli provides a unique, multi-dimensional perspective on the strategic implications of autonomous systems and AI on global security.

Notes

1. Marcus Luttrell and Patrick Robinson. *Lone Survivor: The Eyewitness Account of Operation Redwing and the Lost Heroes of SEAL Team 10* (Little, Brown, and Company, 2007).
2. Mark Bowden, *Black Hawk Down: A Story of Modern War* (Atlantic Monthly Press, 1999).
3. Luttrell and Robinson, *Lone Survivor*.
4. Bowden, *Black Hawk Down*.
5. Bowden, *Black Hawk Down*.
6. U.S. Joint Chiefs of Staff, *Joint Concept for Robotic and Autonomous Systems* (*JCRAS*) (Department of Defense, 2018); Paul Scharre. *Army of None: Autonomous Weapons and the Future of War* (W. W. Norton & Company, 2018).
7. Joint Chiefs of Staff, *JCRAS*; Scharre, *Army of None.*

From Proxy Drone Warfare to Sahelian Adaptation: The Partner Defense Gap SOF Cannot Ignore

By Maj. Imad Ammouri

This is the JSOU AY2026
Call for Special Operations Papers

Category 2

Second-Place
Winner

Digital Version

AI disclaimer: *This manuscript was drafted by the author and subsequently refined using AI-assisted tools for editing, vocabulary, and stylistic consistency. All ideas, arguments, structural choices, and factual content are the author's own.*

Executive Summary

Drone warfare capabilities have reached the Sahel not through a direct Iranian supply corridor, but through horizontal diffusion: operational templates established by Iranian proxy networks subsequently spread via jihadist knowledge transfer and unrestricted commercial platform access. The Islamic State Sahel Province (ISSP) and Jama'at Nusrat al-Islam wal-Muslimin (JNIM) represent distinct tracks within this process. ISSP integrated one-way attack capability within 18 months through structured trainer transfer from the Middle East. JNIM built a sustained cross-border campaign across Mali, Burkina Faso, and Niger using modified commercial quadcopters and open-source tactical learning drawn from the Ukraine conflict. Conflating these two groups into a single problem produces special operations forces (SOF) advising programs calibrated to neither.

Current SOF partner advising has not kept pace with this diffusion. Three structural failures account for the gap: an economic asymmetry that renders U.S.-standard counter-drone architectures unaffordable for African partner forces; institutional learning cycles that operate far more slowly than adversary adaptation; and program discontinuity that erodes capability the moment external support ends. This research documents each failure, distinguishes the acquisition paths that demand separate responses, and proposes six recommendations calibrated to the operational and fiscal realities of African partner forces, addressing the counter-drone gap and the underutilized potential of partner drone employment in equal measure.

Introduction

The attack on Eknewan in May 2025 did not emerge in isolation. Armed with one-way attack drones, fighters from the ISSP struck a military position in Niger and killed 64 soldiers in a single operation.[1]

The tactical signature, coordinated strike, low-cost airframes, and ground assault integration reflected an operational model developed and refined in other theaters before appearing in adapted form in the Sahel. What made Eknewan significant was not its scale. It was its speed: a capability integrated in under 18 months, by a group without direct state sponsorship, on a continent where no SOF advising program had been designed to anticipate it.

The conventional framing of this problem centers on hardware: Iranian Shahed-136 drones deployed in Yemen and Ukraine, first-person view (FPV) drones improvised from commercial quadcopters in the Donbas, and DJI Matrice platforms modified for payload drop in Mali. That framing, while technically accurate, misdiagnoses the threat. The airframe is not the problem. The logic behind the airframe—saturation at low cost, intelligence, surveillance, and reconnaissance (ISR)-strike integration, exploitation of the cost asymmetry between cheap offensive platforms and expensive defensive systems—is the problem. That logic has diffused globally, and no direct supply chain from Tehran to Gao is required to explain its presence in the Sahel.

Two arguments follow from this observation. First, drone warfare capabilities reached the Sahel through horizontal diffusion, not a direct state-to-group transfer chain. Iran built an operational model through documented transfers to Hezbollah and the Houthis; that model's logic subsequently spread through jihadist knowledge networks and commercial platform access, without a proven material corridor between Iran and JNIM.

ISSP-linked groups accessed drone expertise through trainer networks originating in the Middle East, a structurally similar mechanism but analytically distinct. Second, SOF partner advising has not kept pace with this diffusion. Three structural failures account for the gap: doctrine calibrated for high-resource

environments that does not transfer to Sahelian fiscal realities, institutional learning cycles that operate more slowly than adversary adaptation by design, and programs whose operational relevance dissolves once external advising presence ends.

The academic literature has documented the mechanisms of horizontal transfer and the economic asymmetry challenge in general terms.[2] What it has not produced is the operational translation: which counter-drone architectures are locally sustainable for African partner forces, how advising cycles can be restructured to track diffusion in near-real time, and how partner drone employment integrates into the same advisory framework as counter-drone defense. This research addresses each of these gaps from the perspective of a practitioner operating within the broader security environment affected by this diffusion.

From Proxy Laboratory to Global Template: How Iran Institutionalized Drone Warfare

Iran's emergence as a drone proliferator was deliberate, not the byproduct of surplus transfers to convenient proxies. Open-source reporting and sanctions guidance establish that the Islamic Revolutionary Guard Corps (IRGC) developed deliberate institutional mechanisms for drone development, procurement, and transfer to partner forces. That architecture, refined across two decades, transformed early surveillance platforms into one-way attack munitions capable of striking targets beyond 1,500 kilometers.[3] The purpose was strategic: deniable power projection through proxy forces whose capabilities could be enhanced without exposing Iran to the attribution costs of direct military action.[4]

Hezbollah was among the earliest non-state armed groups to operationalize this support. Iranian-supplied reconnaissance platforms were integrated into Hezbollah operations through the

A model built on globally available components and commercially accessible knowledge is inherently more exportable than one dependent on state-controlled hardware.

mid-2000s, and Iranian drone and missile assistance shaped the group's conflict posture against Israel.[5] The transfer to the Houthis in Yemen followed a similar pattern at greater scale and with more mature platforms. Forensic analysis of Iranian technology transfers to Yemen confirmed physical evidence of that chain: components traceable to Iranian manufacturing, assembly techniques consistent with IRGC-affiliated methods, and airframe families derived from Iranian defense production.[6] Treasury department sanctions guidance subsequently documented the networked supply chain enabling those transfers: intermediaries across multiple jurisdictions exploiting dual-use components, many manufactured in the U.S. and allied nations.[7]

The sophistication of that supply chain matters for how diffusion is understood. The components reaching proxy forces were not surplus equipment handed across a border; they were precision electronics sourced through layered commercial and gray-market networks, assembled through iterative combat development cycles. Similar component-tracing patterns have been documented in Russian-employed Iranian unmanned aerial systems (UAS) in Ukraine, where globally sourced electronics flow into ostensibly localized strike architectures through networks that state sanctions struggle to fully interdict.[8] A model built on globally available components and commercially accessible knowledge is inherently more exportable than one dependent on state-controlled hardware.[9]

What those transfers produced operationally was a grammar—saturation tactics employing waves of low-cost munitions to overwhelm defensive interceptors; ISR platforms operating ahead of strike packages; propaganda documentation of every successful strike generating deterrence and recruitment effects beyond the immediate kinetic result. The economic logic of that grammar was not incidental: Shahed-series airframes are estimated at $20,000 to $35,000 each, while the interceptors fielded against them cost orders of magnitude more.[10] For non-state groups observing that exchange on social media, it was a proof of concept.

Houthi and Hezbollah campaigns served as live operational laboratories, broadcast in near-real time to audiences worldwide. This model no longer requires its originator to sustain it. Once operational templates are demonstrated in combat, they circulate through channels Iran neither controls nor can revoke. The Sahel is the most consequential current proof of that dynamic.

Horizontal Transfer: How Drone Warfare Logic Reached the Sahel

The progression of drone use across the Sahel since 2023 represents the most significant tactical development in the region since the spread of vehicle-borne improvised explosive devices.[11] JNIM and ISSP reached comparable operational sophistication through entirely different acquisition paths. Understanding that divergence is not a taxonomic exercise; it determines which threat indicators SOF advising programs should track and which counter-drone architectures are appropriate to each context.

The JNIM trajectory reflects commercial-platform adaptation reinforced by transregional learning. Reporting linked to the Armed Conflict Location and Event Data Project (ACLED)-reporting indicates at least 89 drone-related incidents attributable to JNIM

between 2023 and 2025, including 69 armed strike events.[12] By mid-2024, the group had progressed from initial ISR sorties to complex assault sequences integrating reconnaissance, ground movement, and explosive effects.[13] The platforms are overwhelmingly commercial: DJI Matrice 30T and DJI Mavic series quadcopters, available through civilian retail channels, require no specialized supply chain for acquisition and only basic mechanical skills for payload modification.[14] Open-source observation of Ukrainian FPV tactics appears to have accelerated this learning, with practitioners reportedly monitoring Telegram video channels and incorporating assault sequences derived from that observation.[15]

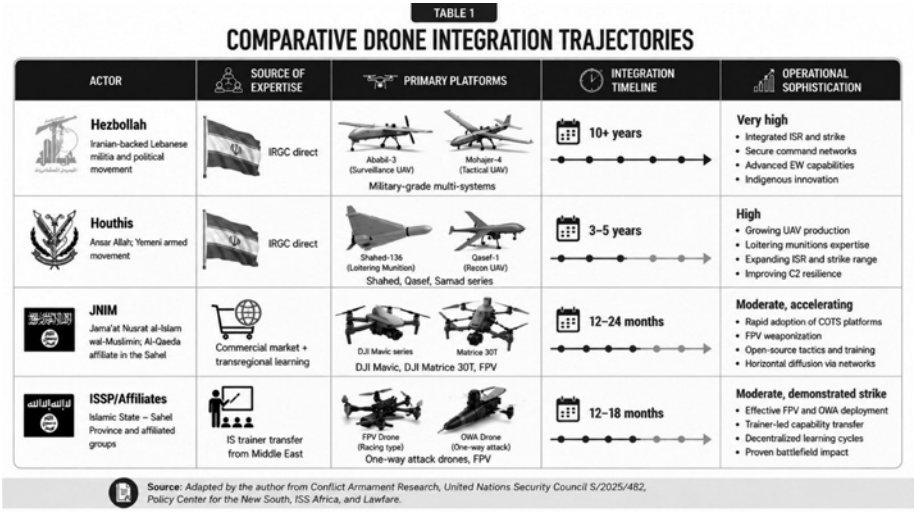
The ISSP trajectory reflects a different channel: structured trainer transfer. The United Nations Security Council Monitoring Team documented the arrival of 13 Islamic State (IS) trainers from the Middle East in the Lake Chad Basin in late 2024, specifically tasked with facilitating drone acquisition, assembly, and deployment among affiliated groups.[16]

This transfer was not of hardware. It was of human expertise: operators, technicians, and instructors who had accumulated experience in theaters where drone warfare had already matured. The mechanism is structurally analogous to how the IRGC institutionalized expertise within its proxy networks, though operating at smaller scale and through less visible pathways. The Eknewan attack of May 2025 was the product of that transfer.

Sahel militant groups are not waiting for state-level support; they are acquiring commercial platforms, adapting them with locally available skills, and deriving tactical doctrine from open-source observation of ongoing conflicts.

Table 1 maps the four acquisition vectors and separates the analytically distinct cases that earlier analysis tended to conflate. See Table 1.

Table 1. Comparative Drone Integration Trajectories



Source: Adapted by the author from Conflict Armament Research, United Nations Security Council S/2025/482, Policy Center for the New South, ISS Africa and Lawfare

The compression of the integration timeline—from a decade to under two years—is the central operational fact. Sahel militant groups are not waiting for state-level support; they are acquiring commercial platforms, adapting them with locally available skills, and deriving tactical doctrine from open-source observation of ongoing conflicts.[17] The diffusion channel is open-access. The response channel is not. See Figure 1.

The Structural Gap: Three Institutional Failures in SOF Partner Advising

Three structural failures in SOF partner advising account for the counter-drone gap in the Sahel. None of them are primarily



Figure 1. Horizontal diffusion model and structual failures in SOF partner advising. Source: Author analysis

technological. Each is embedded in how advising programs are designed, resourced, and sustained. Each would persist regardless of which drone platform adversaries chose to employ.

The Economic Asymmetry Problem

SOF counter-drone doctrine, as codified in the 2021 Department of Defense Counter-Small Unmanned Aircraft Systems Strategy, presumes access to layered sensor networks, trained operators, and a range of kinetic and non-kinetic defeat mechanisms.[18] That architecture was designed for environments where the defending force holds a resource advantage. In the Sahel, that assumption does not hold. The cost exchange between modified commercial drones and the surveillance, electronic-warfare, and intercept layers needed to counter them is prohibitive at scale; the disparity runs across multiple orders of magnitude at every tier of the engagement chain.[19] Burkina Faso, Mali, and Niger, the three states most actively targeted by JNIM drone operations, operate on defense budgets that

No SOF partner advising program should be designed so that its continued effectiveness depends on the physical presence of the advising force.

leave limited margin for dedicated counter-drone procurement, let alone sustained operations.[20] Advising them to build architectures modeled on U.S. doctrine is not a gap in aspiration. It is a mismatch between the doctrine's resource assumptions and the fiscal realities of every partner force it is meant to serve.

No single defeat mechanism offers comprehensive protection against the full spectrum of UAS threats; effective counter-drone defense requires multi-layered combinations of surveillance, detection, neutralization, and organizational adaptation.[21] The problem for African partner forces is not conceptual access to that framework. Every tier it recommends, from persistent wide-area ISR to electronic warfare systems, is priced for military organizations whose procurement context bears no relationship to the Sahel. The doctrine is technically sound. The resource assumptions behind it do not transfer.[22]

The Institutional Speed Mismatch

The 13 IS trainers documented by the United Nations Monitoring Team in the Lake Chad Basin arrived in late 2024 and had transferred operational drone capabilities to affiliated groups within a single fiscal year.[23] The SOF training rotation cycle (assessment, approval, deployment, execution, after-action, revision) operates on timescales that cannot match that pace by design. Formal counter-drone advising curricula require coordination across commands, legal review, security assessment, and partner nation approval

before a single training day is delivered. By the time a revised module addressing FPV threats reaches a Sahel partner force, the threat has typically already iterated.

This mismatch is structural, not a failure of individual effort or institutional will. Adversary learning cycles in non-state armed groups are compressed precisely because those groups lack the formal requirements that make SOF advising rigorous and legally defensible. The drone context reflects a broader pattern, one that has characterized coalition responses to insurgent adaptation in contemporary irregular wars, where threat evolution consistently outpaced doctrinal revision.[24] In the Sahel, the same dynamic operates at higher velocity and with a lower barrier to entry, because the platforms driving it are commercially available to anyone.

Program Discontinuity and the Hollow Advising Legacy

The withdrawals of U.S. and French forces from Mali and Niger between 2023 and 2024 disrupted advisory continuity, reduced access to external ISR and threat-update mechanisms and exposed how dependent many partner-facing programs had become on persistent foreign presence.[25] Partner units that had received counter-drone familiarization training lost points of contact, access to updated threat assessments, and linkages to the intelligence networks that fed tactical adaptation. What remained were institutions that retained the structure of programs built around external support, without the engagement that had given those programs relevance.

The operational implication is narrower than a general critique of redeployment decisions. No SOF partner advising program should be designed so that its continued effectiveness depends on the physical presence of the advising force. Programs built on personal relationships, undocumented institutional knowledge, and access

to classification levels unavailable to partner nation personnel are programs whose effectiveness erodes the moment the adviser boards the aircraft home. Building durability into program design from the outset—rather than as an afterthought at rotation's end—is the structural correction this pattern calls for.

Partner Drone Employment and Counter-Drone Defense

African partner militaries face the same commercial drone environment that their adversaries exploit. The same platforms that JNIM and ISSP have weaponized are available to state forces for defensive and ISR purposes at comparable cost. The most accessible gains for partner forces lie not in high-end strike systems but in the tactical applications these platforms already support: perimeter surveillance of isolated outposts, route reconnaissance ahead of convoy movement, and post-contact assessment functions including battle damage evaluation and indirect fire correction.[26] The same commercial accessibility that makes these platforms operationally dangerous in adversary hands makes them viable as force-protection and reconnaissance assets for under-resourced partners.[27]

SOF advising packages should therefore treat partner drone employment as a paired capability alongside counter-drone training, not as a separate line of effort. The hardware requirement is minimal. Commercially available quadcopters, simplified maintenance protocols, and operator training that can be sustained without continued external support are sufficient for the tactical applications that matter most. A partner force that learns to see the battlefield from above is harder to ambush, better positioned to adapt its defensive posture, and less reliant on externally provided ISR that may be withdrawn without notice. These are not aspirational outcomes. They are achievable with platforms that most partner forces can already procure—the same platforms their adversaries are already using against them.

Closing the Gap: Six Recommendations for Recalibrated SOF Partner Advising

Because the failure is institutional, the response cannot be reduced to procurement. Each recommendation addresses a specific structural weakness identified in the preceding analysis. Together, they constitute a baseline package for a partner advising model calibrated to diffusion speed.

1: Develop a Frugal Counter-Drone Module Purpose-Built for African Partner Forces

Adapting U.S. doctrine for partner use produces training products that are technically sophisticated but operationally inaccessible. A purpose-built module would prioritize radio frequency (RF) detection using commercial spectrum analyzers, acoustic detection assembled from available materials, and passive countermeasures: camouflage, dispersion, and hardening of high-value positions. Electronic warfare options available below classified thresholds, including commercial RF jammers and drone-detection software suites, should be incorporated where host-nation legal frameworks permit. Delivery through Theater Security Cooperation Programs under U.S. Africa Command provides an existing vehicle without requiring new programmatic authorities.

2: Integrate a Compact Partner Drone Employment Package

Alongside counter-drone training, SOF advisers should deliver a paired concept for partner drone employment at the tactical level: perimeter surveillance, route reconnaissance, post-contact assessment, and indirect fire correction using commercially available platforms. This closes an advisory gap that current programs leave open and leverages hardware that partner forces can already

access independently. The two capabilities reinforce each other; the partner that understands how drones are used offensively is better positioned to defend against them.

3: Create a Tactical Diffusion Surveillance Mechanism Within Advising Intelligence Cycles

The 13 IS trainers in the Lake Chad Basin were documented after their effect was already visible in the field. A proactive mechanism within Joint Intelligence Support Elements deployed alongside SOF advising teams would track known drone instructors moving through jihadist networks, monitor open-source channels where tactics are shared, and feed that tracking into curriculum updates on a rolling basis. The model exists for IS counterterrorism tracking in the Middle East; applying it to drone tactical diffusion in Africa requires reorientation of existing analytic capacity, not new institutional architecture.

4: Adopt an Economic Defense Doctrine for Counter-Drone Partner Advising

The correct objective for an African partner force is not to intercept every drone; that standard is unachievable at available price points and frames the problem incorrectly. The objective is to degrade the adversary's ability to execute drone-enabled complex attacks at operationally relevant tempo. Acoustic and RF detection enabling early warning, combined with dispersion and hardening of defended positions, can achieve this at a fraction of the cost of kinetic intercept. SOF advising curricula should state this explicitly: the objective is denial of effect, not defeat of airframe.

5: Design Programs for Continuity Without Physical Presence

Every counter-drone advising program delivered to a Sahel partner force should include a transfer-of-authority package: threat assessments updated through unclassified channels, locally executable training curricula that do not require a foreign adviser to deliver, and a designated point of contact within the partner organization accountable for program continuity. Building self-sustaining institutional capacity is the structural change that makes partner advising durable. Capacity contingent on sustained external presence is not capacity at all.

6: Establish a Regional Counter-Drone Knowledge Exchange Network in West Africa

No single Sahelian state has the resources, geographic reach, or information access to track drone tactical diffusion across the region independently. A structured forum connecting regional security forces focused on threat reporting, solution sharing, and joint training coordination, would aggregate information that no individual partner currently holds. States with established security partnerships in the region, including Morocco, Mauritania, and Senegal, are well-positioned to contribute to such a network. SOF could facilitate its establishment without owning or operating it.

Conclusion

Eliminating production sites does not eliminate a model once that model has been observed, adapted, and localized. The operational grammar of low-cost drone warfare now circulates through trainers, open-source communities, and commercially accessible platforms. The Sahel is no longer a downstream recipient

of someone else's conflict; it is an active theater of drone adaptation in its own right.

The threat that killed 64 soldiers in Niger in May 2025 will not diminish because of disruptions to any single country's production capacity. The underlying logic is now independent of any single state originator, and partner forces in the Sahel are confronting a learning cycle that current SOF advising structures were not designed to match. That is a solvable problem—but only if the institutional response operates at the speed the diffusion demands, not at the speed that formal approval cycles permit.

The six recommendations in this paper address the structural failures, not the symptoms. Their value lies not in novelty but in combination and calibration: frugal detection, economic defense doctrine, partner drone employment, program continuity, and regional knowledge networks. The package is sized for the fiscal and operational realities of African partner forces that cannot wait for doctrine designed for better-resourced environments to eventually reach them. The response SOF partner advising needs is not more sophisticated—it needs to be faster, more durable, and better matched to the constraints of the partners it is meant to serve.

About the Author

Maj. Imad Ammouri is a senior officer of the Royal Gendarmerie of the Kingdom of Morocco, where he serves in a command staff role within the special operations enterprise. He holds a master's degree in international, strategic, and security studies from Mohammed V University in Rabat, where his thesis examined low-cost drone proliferation and the reconfiguration of hybrid warfare, addressing doctrinal disruption, state adaptation, and emerging governance challenges.

He is completing a PhD in strategic and military studies at Abdelmalek Essaâdi University in Tangier, where his research focuses on the integration of AI in autonomous weapons systems across multi-domain operations, with attention to strategic transformation, power dynamics, and governance frameworks. Ammouri is a graduate of the Joint Special Operations University Special Operations Combating Terrorism course in Tampa, Florida, and an alumnus of the George C. Marshall European Center for Security Studies Program on Terrorism and Security Studies in Garmisch-Partenkirchen, Germany.

The analytical perspective of this paper draws on the intersection of his master's research on drone proliferation, his doctoral work on autonomous systems governance, and his professional exposure to the partner advising dynamics and resource asymmetries that define the counter-drone challenge in the Sahel.

Notes

1. "64 Soldiers Killed in Niger Drone Strike," *The Defense Post*, May 27, 2025, https://thedefensepost.com/2025/05/27/niger-drone-strike-64-soldiers-killed; Hassane Koné and Fahiraman Rodrigue Koné, "Sahel Militants Turn Civilian Drones into Deadly Weapons," *ISS Today*, July 8, 2025, https://issafrica.org/iss-today/sahel-militants-turn-civilian-drones-into-deadly-weapons; Rueben Dass, "African Non-State Actors Put Drones on the Attack," *Lawfare*, October 19, 2025, https://www.lawfaremedia.org/article/african-non-state-actors-put-drones-on-the-attack.

2. Matt Plichta and Amos Rossiter, "A One-Way Attack Drone Revolution? Affordable Mass Precision in Modern Conflict," *Journal of Strategic Studies* 47 (2024): 1001–1031, https://doi.org/10.1080/01402390.2024.2385843; Bárbara Morais Figueiredo, *The Use of Uncrewed Aerial Systems by Non-State Armed Groups in Africa* (UNIDIR, 2024), https://unidir.org/wp-content/uploads/2024/01/UNIDIR_Use_of_Uncrewed_Aerial_Systems_by_Non_State_Armed_Groups_Africa.pdf.

3. U.S. Department of the Treasury, Office of Foreign Assets Control, *Guidance to Industry on Iran's UAV-Related Activities* (2023), https://ofac.treasury.gov/media/931876/download?inline=; Center for Strategic and International Studies, "Iran's Support of Hezbollah in Lebanon," https://www.csis.org/analysis/irans-support-hezbollah-lebanon.

4. Shahram Akbarzadeh and Arash Naeni, "Iranian Drones at the Service of Authoritarian Geopolitics," *Geopolitics* 30 (2025): 2312–2336, https://doi.org/10.1080/14650045.2025.2468769.

5. Center for Strategic and International Studies, "Iran's Support of Hezbollah in Lebanon"; CSIS Missile Defense Project, "Iranian Missile Threat," https://missilethreat.csis.org/.

6. Conflict Armament Research, *Iranian Technology Transfers to Yemen* (CAR, March 2017), https://www.conflictarm.com/wp-content/uploads/2017/03/Iranian-Technology-Transfers-to-Yemen.pdf.

7. U.S. Department of the Treasury, Office of Foreign Assets Control, *Guidance to Industry on Iran's UAV-Related Activities*.

8. International Institute for Strategic Studies, *Tracking the Components of Missiles and UAVs Used by Russia in Ukraine* (IISS, September 2025), https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2025/09/pub25-094-tracking-the-components-of-missiles-and-uavs-used-by-russia-in-ukraine.pdf.

9. Plichta and Rossiter, "A One-Way Attack Drone Revolution?" (2024), 1001–1031.

10. Center for Strategic and International Studies, "Drone Saturation: Russia's Shahed Campaign," May 13, 2025, https://www.csis.org/analysis/drone-saturation-russias-shahed-campaign.

11. Samuel Davies, Thérèsa Pettersson, and Magnus Öberg, "Organized Violence 1989–2021 and Drone Warfare," *Journal of Peace Research* 59, no. 4 (2022): 593–610, https://doi.org/10.1177/00223433221108428.

12. Al Jazeera, "Are Drones, AI Making It Harder to Fight Armed Groups in the Sahel?" February 11, 2026, https://www.aljazeera.com/amp/news/2026/2/11/are-drones-ai-making-it-harder-to-fight-armed-groups-in-the-sahel.

13. Niccola Milnes and Rida Lyammouri, *Countering JNIM Drone Proliferation in the Sahel, Policy Paper 24/25* (Policy Center for the New South, July 14, 2025), https://www.policycenter.ma/publications/countering-jnim-drone-proliferation-sahel.

14. United Nations Security Council, *Thirty-Sixth Report of the Analytical Support and Sanctions Monitoring Team,* S/2025/482, July 24, 2025, https://documents.un.org/doc/undoc/gen/n25/176/00/pdf/n2517600.pdf; Figueiredo, *The Use of Uncrewed Aerial Systems by Non-State Armed Groups in Africa*.

15. Dass, "African Non-State Actors Put Drones on the Attack."

16. United Nations Security Council, S/2025/482.

17. Koné and Koné, "Sahel Militants Turn Civilian Drones into Deadly Weapons"; Milnes and Lyammouri, *Countering JNIM Drone Proliferation in the Sahel*.

18. U.S. Department of Defense, *Counter-Small Unmanned Aircraft Systems Strategy,* (DoD, January 7, 2021), https://media.defense.gov/2021/Jan/07/2002561080/-1/-1/0/DEPARTMENT-OF-DEFENSE-COUNTER-SMALL-UNMANNED-AIRCRAFT-SYSTEMS-STRATEGY.pdf.

19. NATO Joint Air Power Competence Centre, *A Comprehensive Approach to Countering Unmanned Aircraft Systems* (JAPCC, 2020), https://www.japcc.org/wp-content/uploads/A-Comprehensive-Approach-to-Countering-Unmanned-Aircraft-Systems.pdf.

20. Stockholm International Peace Research Institute, "Military Expenditure Database," https://www.sipri.org/research/armaments/milex/milex_database.

21. JAPCC, *A Comprehensive Approach to Countering Unmanned Aircraft Systems*; Honggu Kang, Jingon Joung, Jinyoung Kim, Joonhyuk Kang, and Yong Soo Cho, "Protect Your Sky: A Survey of Counter Unmanned Aerial Vehicle Systems," *IEEE Access* 8 (2020): 168671–168710, https://doi.org/10.1109/access.2020.3023473.

22. Chenyang Lyu and Renjun Zhan, "Global Analysis of Active Defense Technologies for Unmanned Aerial Vehicle," *IEEE Aerospace and Electronic Systems Magazine* 37, no. 2 (2022): 6–31, https://doi.org/10.1109/maes.2021.3115205; Vittorio U. Castrillo, Angelo Manco, Domenico Pascarella, and Gabriella Gigante, "A Review of Counter-UAS Technologies for Cooperative Defensive Teams of Drones," *Drones* 6, no. 3 (2022): 65, https://doi.org/10.3390/drones6030065; Jian Wang, Yuhang Liu, and Houbing Song, "Counter-Unmanned Aircraft System(s) (C-UAS): State of the Art, Challenges, and Future Trends," *IEEE Aerospace and Electronic Systems Magazine* 36, no. 3 (2020): 4–29, https://doi.org/10.1109/maes.2020.3015537.

23. United Nations Security Council, S/2025/482.

24. David H. Ucko and Thomas A. Marks, "Violence in Context: Mapping the Strategies and Operational Art of Irregular Warfare," Contemporary Security Policy 39, no. 2 (2018): 206–233, https://www.tandfonline.com/doi/full/10.1080/13523260.2018.1432922.

25. Koné and Koné, "Sahel Militants Turn Civilian Drones into Deadly Weapons"; Milnes and Lyammouri, *Countering JNIM Drone Proliferation in the Sahel*.

26. Folake Okpaleke, Bright Nwosu, Chukwuma Okoli, and Emeka Olumba, "The Case for Drones in Counter-Insurgency Operations in West African Sahel," *African Security Review* 32, no. 4 (2023): 351–367, https://doi.org/10.1080/10246029.

2023.2217158; Figueiredo, *The Use of Uncrewed Aerial Systems by Non-State Armed Groups in Africa*.

27. Milnes and Lyammouri, *Countering JNIM Drone Proliferation in the Sahel*.

“Truly Cheap” Uncrewed Systems for Great-Power Competition: Strategic Relevance for Special Operations Forces

By AJ Rutherford, PhD

Abstract

As global competition intensifies between the United States and near-peer adversaries such as China and Russia, the strategic utility of low-cost uncrewed systems (UxS) has emerged as a critical enabler for special operations forces (SOF). This research examines how mass-produced, attritable UxS platforms, particularly first-person view (FPV) drones, loitering munitions, and uncrewed surface vessels (USVs), are reshaping operational paradigms. Drawing lessons from the Russo–Ukrainian War and parallel developments in Taiwan, the analysis explores the doctrinal, logistical, and acquisition challenges inhibiting SOF's ability to rapidly adopt and field these systems. Emphasis is placed on the necessity of cultural adaptation, rapid prototyping, commercial partnerships, and distributed manufacturing to meet the demands of denied environments and gray-zone conflict. The paper proposes actionable recommendations, including the institutionalization of a SOF-specific Rapid Drone Cell, development of swarm-based tactics, and interoperability through digital twin integration. Ultimately, this research argues that adopting a mindset of iterative innovation and embracing the disposability of UxS is essential for maintaining operational advantage in an era defined by scale, tempo, and technological asymmetry.

Introduction

The character of warfare is undergoing a fundamental transformation as great power competition accelerates the adoption of low-cost, attritable uncrewed systems across the air and maritime domains. Rather than relying exclusively on exquisite, high-cost platforms optimized for survivability, contemporary conflicts increasingly demonstrate that operational mass, adaptability, and rapid innovation can generate strategic effects disproportionate to system cost. The Russo–Ukrainian War provides the clearest

contemporary example of this shift, where commercially available first-person-view (FPV) drones and improvised uncrewed surface vessels (USVs) have been employed at scale to conduct intelligence, surveillance, reconnaissance (ISR), precision strike, electronic warfare, and maritime attacks against conventionally superior forces. These platforms have enabled Ukraine to generate operational and strategic effects through volume, rapid adaptation, and expendability rather than technological superiority alone.[1] Simultaneously, the U.S. Department of War's Replicator initiative reflects institutional recognition that future conflicts will require thousands of affordable, attritable autonomous systems capable of offsetting adversary numerical advantages through distributed, all-domain operations rather than reliance on small numbers of exquisite platforms[2].

These developments have significant implications for United States Special Operations Forces (SOF). Traditionally, SOF have emphasized precision, survivability, and small-team autonomy supported by highly capable but expensive platforms. While these capabilities remain essential, they are increasingly complemented by inexpensive uncrewed systems that reduce operational risk, enable persistent ISR, extend mission reach, increase tactical redundancy, and permit operations in denied or politically sensitive environments where the loss of an individual platform carries limited strategic or financial consequence. Moreover, the rapid development cycles enabled through commercial off-the-shelf (COTS) technologies, open architectures, additive manufacturing, and software-defined capabilities allow uncrewed systems to evolve at a pace that traditional defense acquisition processes often struggle to match. Consequently, the integration of cheap, expendable air and maritime systems represents not simply technological advancement but a broader doctrinal shift toward distributed lethality, scalable force employment, and accelerated operational innovation.

> ***Integration of cheap, expendable air and maritime systems represents not simply technological advancement but a broader doctrinal shift toward distributed lethality, scalable force employment, and accelerated operational innovation.***

Against this backdrop, the purpose of this research is to evaluate the operational, logistical, and doctrinal implications of integrating low-cost uncrewed air and maritime systems into SOF operations. Specifically, the study examines how FPV drones, small loitering munitions, and maritime USVs can enhance operational effectiveness within contested, denied, and politically sensitive environments while simultaneously reducing logistical burden and increasing organizational adaptability. Operationally, the analysis considers how these systems support disaggregated ISR, precision strike, electronic warfare, deception, and risk-distributed force projection. Logistically, it examines how modular design, commercial manufacturing, simplified sustainment, and expendability fundamentally alter traditional supply chain and maintenance models. Doctrinally, the study explores how widespread employment of attritable systems challenges long-standing assumptions regarding survivability, force structure, mission planning, human-machine teaming, and acceptable operational risk.

The scope is intentionally limited to low-cost aerial and maritime uncrewed systems because these capabilities have demonstrated the greatest operational relevance for SOF missions while providing the strongest empirical evidence from contemporary conflict. The discussion emphasizes commercially derived and rapidly adaptable technologies rather than high-end autonomous weapons systems, focusing on capabilities that can be fielded quickly, modified

locally, and employed in sufficient numbers to create operational mass. Lessons derived from Ukraine's employment of FPV drones and USVs provide the principal operational context, while the Department of Defense's Replicator initiative illustrates the growing institutional emphasis on affordable, attritable autonomous systems as an enduring component of future military capability. Collectively, this focused examination provides a practical framework for understanding how SOF can institutionalize cheap, expendable uncrewed systems to maintain operational overmatch, accelerate innovation, and sustain mission relevance throughout an era of strategic competition.

Background

Strategic Environment Shift

Rise of Near-Peer Competition with China and Russia

The global strategic environment has undergone a marked transformation with the resurgence of near-peer competitors, particularly China and Russia, challenging the long-standing unipolar dominance of the United States. China's aggressive military modernization and assertive actions in the South China Sea, along with Russia's use of hybrid warfare and destabilization campaigns in Europe, exemplify a significant escalation in near-peer competition challenging U.S. strategic dominance.[3] This shift represents more than a return to great power politics; it signals the erosion of the liberal international order and a move toward a multipolar system defined by contested domains, particularly cyber, space, and the information environment. The operational convergence of conventional, gray zone, and asymmetric strategies employed by both nations necessitates a reevaluation of deterrence frameworks, alliance structures, and force readiness across the U.S. and NATO. This new strategic calculus also blurs the lines between peace and conflict, creating persistent competition below the threshold of

armed conflict. Understanding and adapting to the reemergence of near-peer competition is imperative for defense planners and policymakers aiming to maintain strategic stability, preserve deterrence, and safeguard democratic norms in an increasingly contested international system.

Limitations of Conventional Force Projection in Gray-Zone Warfare

The contemporary strategic environment reveals the inadequacy of conventional force projection in addressing gray-zone warfare, which operates below the threshold of open conflict. Hal Brands, a professor of global affairs at the Johns Hopkins School of Advanced International Studies (SAIS) and one of the leading scholars in strategic studies and great power competition, argues that gray-zone conflict consists of coercive activities deliberately designed to remain below the threshold of conventional interstate war. Rather than seeking decisive military confrontation, these campaigns employ cyber operations, disinformation, election interference, proxy forces, economic coercion, and paramilitary activities to achieve strategic objectives while avoiding a conventional military response. Brands contends that this ambiguity complicates deterrence because traditional military force is often ill-suited to counter actions intentionally calibrated to remain below the threshold of open conflict.[4]

This mismatch reflects a broader challenge in strategic planning: Adversaries like China and Russia have optimized their strategies to exploit gaps in Western legal frameworks, alliance structures, and response protocols. Aircraft carriers or mechanized units offer limited deterrent value against disinformation or economic leverage. Thus, relying solely on traditional military strength risks strategic inertia, allowing adversaries to achieve incremental gains without triggering formal conflict. To remain competitive, U.S. and allied

defense strategies must integrate tools suited to countering gray-zone threats, such as cyber resilience, strategic communications, and irregular warfare capabilities, alongside conventional deterrence.

Lessons from Ukraine

Impact of Mass-Produced First-Person View Drones, Loitering Munitions, and Maritime Uncrewed Surface Vessels

The Ukraine conflict provides decisive insights into the disruptive impact of low-cost, mass-produced unmanned systems, specifically FPV drones, loitering munitions, and maritime USVs, on contemporary tactical and operational warfare. Laviniu Bojor and Laurențiu Grigore, researchers at the "Nicolae Bălcescu" Land Forces Academy in Sibiu, Romania, whose work focuses on military innovation, network-centric warfare, and lessons learned from the Russo-Ukrainian War, argue that FPV drones have evolved into tactically decisive precision-strike platforms that are fundamentally reshaping modern warfare. Their analysis contends that the large-scale employment of FPV drones in Ukraine demonstrates a transition toward decentralized, network-centric operations in which inexpensive, attritable systems overwhelm conventional defenses through distributed maneuver, rapid decision cycles, and saturation rather than technological superiority alone.[5] These platforms showcase how affordability and scalability can offset technological shortcomings. FPV drones enable distributed, adaptive strikes, while loitering munitions provide covert precision targeting. Maritime USVs project naval power asymmetrically, bypassing traditional vessel defenses. Together, they reshape force projection by enabling decentralized, layered pressure across multiple domains. To remain operationally relevant, defense planners must adjust doctrines to integrate these unmanned systems, investing in counter-drone measures and doctrinal changes that reflect the proliferation of autonomous warfare technologies.

Democratization of Intelligence, Surveillance, Reconnaissance, and Kinetic Strike via Cheap, Decentralized Tools

The war in Ukraine has demonstrated the democratization of ISR and kinetic strike capabilities through inexpensive, decentralized tools like commercial drones and loitering munitions. Matlack et al. highlight how Ukraine's drone ecosystem, spanning grassroots innovation, volunteer builders, and military stakeholders, enabled rapid deployment of FPV drones and swarm loitering munitions across the front lines, leveraging scale, speed, and agility to impactful effect.[6] This transformation shows that effective ISR and precision strike no longer require centralized, high-cost platforms. Instead, battlefield advantage now hinges on modular, networked systems fueled by local innovation. Ukraine's model, distributing production among civilian and military actors, has subverted conventional power dynamics by enabling decentralized, adaptive tactics that can outpace traditional procurement and deployment cycles. Defense policymakers must now adapt by embracing doctrine and acquisition frameworks that support distributed, rapidly fieldable drone systems, prioritizing flexibility and ecosystem fostering over centralized capability development.

Current SOF Acquisition Models

High-Cost, Long-Tail Procurement Not Suited for Cheap Systems

The ongoing conflict in Ukraine has underscored the misalignment between existing SOF acquisition models and the demands of modern, decentralized warfare. According to Business Insider, Ukraine's defense sector has revolutionized wartime production by embracing rapid prototyping and mass production of cheap, attritable systems like drones, demonstrating the battlefield effectiveness of agile, decentralized procurement over traditional, expensive, long-tail defense acquisitions.[7] This model starkly

Ukraine's model, distributing production among civilian and military actors, has subverted conventional power dynamics by enabling decentralized, adaptive tactics that can outpace traditional procurement and deployment cycles.

contrasts with Western SOF acquisition strategies, which often rely on years-long procurement cycles for costly, bespoke systems. Such approaches are ill-suited for the rapid adaptation required in dynamic environments dominated by cheap ISR assets and loitering munitions. Ukraine's wartime innovations reveal that speed and scale, rather than elite precision, may be decisive in future conflicts. To maintain battlefield relevance, SOF acquisition processes must be restructured to mirror agile procurement models that prioritize affordability, adaptability, and distributed lethality over traditional, high-end platforms.

Cultural and Bureaucratic Friction in Adopting Expendable Technologies

The Ukraine conflict exposes the deep cultural and bureaucratic resistance within Western SOF acquisition systems when attempting to adopt expendable, low-cost technologies. According to Kunertová, Western militaries struggle to integrate commercial drone capabilities and other low-cost autonomous systems due to entrenched bureaucratic inertia, risk aversion, and legacy acquisition frameworks favoring large, long-lifecycle platforms.[8] This systemic resistance manifests in multi-year procurement cycles, heavy compliance requirements, and an organizational bias toward multi-million-dollar assets. As a result, SOF units are slowed down in adapting battlefield innovations like FPV drones or loitering munitions, technologies proven effective in Ukraine. The friction

between innovation on the battlefield and conservatism in the acquisition process highlights a concerning mismatch that can erode tactical edge. To remain effective in modern conflict, SOF acquisition must evolve: streamlining processes, reducing bureaucratic barriers, and embracing agile, low-cost systems revealed as critical in Ukraine's rapidly adaptive warfare environment.

Discussion

Operational Value of "Truly Cheap" Systems

Tactical Flexibility and Expendability

Truly cheap unmanned systems, such as low-cost commercial drones, enhance tactical flexibility and accept attrition, providing forces with resilient, scalable options in dynamic battlefields. Oleksandra Molloy, a researcher with the Australian Army Research Centre specializing in contemporary land warfare and lessons learned from the Russo–Ukrainian War, explains that commercially available DJI Mavic drones costing approximately US$500 rapidly became indispensable ISR platforms for Ukrainian forces. Their affordability, immediate availability, and ability to provide real-time battlefield intelligence enabled decentralized units to identify targets, accelerate decision cycles, and maintain operational effectiveness despite high equipment attrition.[9] These low-cost systems differ fundamentally from legacy platforms because they can be risked and lost without strategic consequence, enabling "swarm" tactics, experimentation, and fast iteration. Units can dynamically deploy them during complex operations, while diminished effectiveness due to losses is offset by low replacement costs. This expendability empowers tactical innovation and endurance under persistent pressure. Adopting such expendable systems within force structures requires a doctrinal shift: Procurement and operational frameworks must support rapid replacement, unit-level autonomy, and velocity, principles

proven effective in Ukraine, to meet the demands of future contested environments.

Mass and Saturation Versus Precision

Combat in Ukraine has demonstrated that overwhelming defenses with mass-produced, low-cost drone swarms can be as, or more, effective than relying on few high-precision systems. Benjamin Jensen, Director of the Futures Lab at the Center for Strategic and International Studies (CSIS) and a recognized scholar of future warfare, military strategy, and artificial intelligence in conflict, together with Yasir Atalan, a researcher specializing in quantitative conflict analysis and military innovation, argue that Russia's large-scale employment of inexpensive Shahed drones represents a deliberate strategy of drone saturation designed to overwhelm Ukrainian air defenses through volume rather than individual platform effectiveness. Their analysis concludes that Russia employs low-cost uncrewed aerial systems in persistent nightly attacks to exhaust expensive interceptor inventories, degrade civilian resilience, and impose cumulative operational and economic costs on Ukraine's defensive architecture.[10] This approach imposes a war of attrition where each $20–50K drone forces the defender to expend far more expensive interceptors. The pressure created by saturation attacks stresses defense systems and generates psychological damage, showing that scale can substitute for sophistication. In contrast, elite precision weapons are more limited in number and slower to deploy, making saturation tactics strategically disruptive. Armed forces must therefore blend mass and precision, fielding doctrinally integrated swarms alongside targeted high-end systems, to stay resilient against future combined-arms threats like those witnessed in Ukraine.

Psychological and Disinformation Effects

Truly cheap unmanned systems deliver not only physical effects but also potent psychological and disinformation leverage, amplifying operational value far beyond their cost. U.S. Army Training and Doctrine Command highlights that the continual buzz and presence of cheap drone swarms in Ukraine, hundreds per night, induces anticipatory anxiety and stress, disrupting both military and civilian morale.[11] These drones act as sonic and visual stressors, akin to sonic weapons, that fray resolve and hinder movement. Their persistent visibility, amplified by social media and live streaming, spreads fear beyond the battlefield, enhancing disinformation narratives and reinforcing adversaries' perceptions of omnipresent threat. This psychological saturation amplifies the operational impact of systems costing only a few hundred dollars each. Commanders and defense planners must thus recognize that cheap lethality paired with psychological leverage can deliver strategic effects at scale. Incorporating these tools into doctrine requires acknowledging the cognitive terrain and legitimizing "cheap" systems as indispensable instruments of modern influence warfare.

Rapid Risk-Tolerant Deployment in Denied Environments

The conflict in Ukraine validates the operational value of truly cheap unmanned systems through rapid, risk-tolerant deployment in denied environments. A *Small Wars Journal* analysis reports Ukrainian volunteers and small workshops produced inexpensive FPV drones at scale, quickly fielding frontline systems within days to bypass contested zones and exploit enemy vulnerabilities.[12] These low-cost tools permit erratic, courageous deployment in high-risk areas where traditional assets cannot operate safely. Their affordability means losses are acceptable, enabling experimentation, saturation tactics, and decentralized missions. This flexibility allows commanders to seize fleeting opportunities

and adapt quickly, bypassing adversary control. Western SOF and allied forces must overhaul acquisition and deployment strategies, empowering distributed units with fast-access, attritable systems designed for immediate use in denied spaces, and complex operational environments.

Rapid Prototyping and Acquisition Reform

Challenges with Traditional Procurement Timelines

Traditional military procurement timelines significantly hinder the rapid fielding of truly cheap systems, limiting operational agility in contested environments. A study by CSIS highlights how Ukraine streamlined its acquisition process, reducing timelines from years to weeks, by integrating commercial tech and decentralizing procurement, directly contrasting with protracted traditional systems.[13] Conventional procurement persists in linear, compliance-heavy processes tailored to high-value platforms, ill-suited for emergent, low-cost tools that require near-immediate deployment. This systemic inertia prevents forces from adapting to evolving battlefield demands, as seen in Ukraine. In contrast, Ukraine's model shows that agile acquisition, guided by frontline needs rather than bureaucracy, accelerates innovation and resilience. To stay relevant in future conflicts, Western SOF and military acquisition agencies must reform by enabling rapid, modular procurement pathways that prioritize responsiveness and operational feedback over bureaucratic orthodoxy.

Importance of Leveraging Commercial Hobbyist and Startup Ecosystems

Ukraine's experience highlights the critical importance of integrating commercial hobbyist and startup ecosystems to enable rapid prototyping and acquisition reform, bridging the gap between battlefield need and technological delivery. A recent

Military forces seeking operational agility must institutionalize maintenance-centric doctrines alongside modular commercial, off-the-shelf design, shifting focus from replacement to rapid repair to sustain combat effectiveness in high-intensity environments.

Massachusetts Institute of Technology innovation ecosystem analysis shows how Ukraine harnessed its vibrant commercial and academic tech community, including startups, university labs, and hobbyist workshops, to develop and scale drone technologies from bedrooms and garages into frontline systems, overcoming traditional procurement barriers.[14] By leveraging decentralized innovation, Ukraine bypassed legacy bureaucratic constraints and dramatically compressed development cycles from years to weeks. COTS components, entrepreneurial agility, and direct military feedback fostered iterative design and rapid field deployment. This decentralized model not only met urgent battlefield demands but also formed a resilient industrial base capable of both scaling production and sustaining technological momentum. To meet the demands of future contested environments, Western forces must formally integrate commercial hobbyist and startup ecosystems into acquisition strategies, embracing modular prototyping, distributed innovation, and agile feedback loops to match the operational tempo of modern warfare.

Logistical Scaling and Sustainment

Benefits of Modularity and Commercial, Off-the-Shelf Components

The use of modular COTS drone components in Ukraine has significantly enhanced logistical scalability and sustainment by

allowing fast production and straightforward maintenance. The Georgetown Security Studies Review reports that Ukraine's drone industry scaled from near-zero to over 200,000 units produced monthly by standardizing modular designs and COTS parts, enabling rapid repairs and simplified supply chains in austere environments.[15] This modularity reduces dependency on bespoke supply chains and allows frontline repair teams to replace individual components, like motors or flight controllers, without specialized tools. As a result, sustainment becomes decentralized, cost-effective, and resilient to disruption, ensuring continuous drone availability despite attrition and contested logistics conditions. To improve force readiness, military planners must integrate modular and COTS-based systems into doctrine and procurement, reinforcing a logistics model built on adaptability, simplicity, and frontline empowerment.

Maintenance Versus Replacement Mentality

Adopting a maintenance-focused approach to unmanned systems, rather than immediate replacement, enhances logistical efficiency and system longevity in combat environments. Field reports indicate that Ukrainian units, leveraging modular drone designs and readily available spare parts, prioritized repairing malfunctioning drones at the front rather than replacing them, significantly reducing downtime and sustaining operational tempo.[16] This maintenance-first mentality ensures high availability of systems under fire, minimizes logistical strain, and conserves resources.

By repairing rather than discarding, units avoided replenishment delays inherent in replacement models. This resilience proved especially valuable in contested environments with restricted supply lines, allowing frontline operators to keep more systems airborne and functional. Military forces seeking operational agility must institutionalize maintenance-centric doctrines alongside modular

COTS design, shifting focus from replacement to rapid repair to sustain combat effectiveness in high-intensity environments.

Distributed Manufacturing: 3D Printing and Microfabrication at Forward Sites

Distributed manufacturing, embodied by forward-deployed 3D printing and microfabrication, offers critical advantages in scaling, sustainment, and resilience for military operations. Dass[17] observes that frontline Ukrainian forces have deployed portable 3D printers to produce munitions casings ("candy bombs"), tourniquet components, and vehicle parts locally, bypassing disrupted supply lines and reducing delivery delays in contested zones. This on-site manufacturing approach drastically shortens the production-to-use timeline, enabling units to respond swiftly to emergent needs without awaiting distant logistics hubs. By turning digital designs into tangible parts on the spot, forces gain unprecedented operational autonomy. The ability to print replacement parts, medical supplies, or urgent ordnance in forward areas transforms sustainment from a centralized process into a distributed capability, bolstering mission resilience amid adversarial disruption. Military logistics doctrine must integrate distributed manufacturing into tactical planning, fielding compact 3D printers, maintaining digital libraries of critical parts, and training operators in microfabrication, to ensure sustainment agility in future high-threat environments.

Doctrinal Shifts

The Need to Rethink Force Structure: Drone Swarms and Human-Machine Teams

Emerging combat dynamics demand a fundamental rethinking of force structure to integrate drone swarms and human-machine teaming as core components of modern operations. Haider and Schmidt argue that the absence of a formal doctrinal definition

for swarms hinders the effective integration and deployment of drone swarms within the U.S. military; they highlight that defining swarms is essential to unlocking scalable autonomy and team-based operations across human and machine elements.[18] Without a doctrinal foundation, efforts to build human-machine teams and drone swarms risk remaining siloed and tactical rather than strategic. A standardized doctrine would enable interoperability, coherent command and control frameworks, and meaningful mission integration, allowing swarms to support dismounted, maritime, and air operations seamlessly. This doctrinal clarity is vital to evolving force structures that leverage autonomous systems without undermining human oversight. Defense planners must codify drone swarm and human-machine teaming concepts in doctrine and force organization, enabling training, procurement, and operational planning to reflect the integrated, augmented force illustrated in recent conflicts.

Ethical and Policy Concerns of Autonomy and Expendability

The deployment of autonomous or expendable systems introduces ethical and policy concerns that must be urgently addressed, particularly regarding human oversight and accountability in lethal scenarios. The Center for a New American Security highlights emerging principles aimed at preserving "human judgment and responsibility" in the use of autonomous weapon functions to minimize unintended engagements, especially involving noncombatants.[19] These principles underscore critical ethical tensions such as how to reconcile missions demanding rapid, low-cost autonomous platforms with the enduring requirement for oversight. Expendability increases risk of misuse, unintended escalation, or lowered thresholds for lethal action. Without clear norms, autonomous systems, even if inexpensive, can automate grave decisions, shifting culpability away from

operators and raising accountability gaps. Moreover, eroding human control risks damaging public trust and international legal standing. Doctrinal frameworks must incorporate ethical guardrails, such as meaningful human control, predictable system behavior, and transparent engagement rules, to legitimize and regulate the use of autonomy in future operations.

Mission Planning Evolution: Small-Unit Intelligence, Surveillance, Reconnaissance, Decoy, Electronic Warfare, and Kinetic Support

Modern mission planning must evolve to integrate small unit capabilities like ISR, decoys, electronic warfare (EW), and kinetic strike into cohesive, multifunctional tactical packages. A Royal United Services Institute study observes that small drones now conduct frontline ISR, decoy operations, EW jamming, and immediate precision strikes in Ukraine, practices once reserved for separate specialized units, now executed routinely by small teams in combined arms fashion.[20] This convergence empowers frontline squads with organic, multidomain tools, dramatically shortening sensor-to-shooter cycles and reducing dependence on higher headquarters or specialized assets. Integrating ISR, EW, decoys, and strike into a single unit enhances surprise, resilience, and selfsufficiency, while complicating enemy defenses through multivector attacks that exploit cognitive and physical layers simultaneously. Doctrine must adapt to this tactical reality by formalizing combined arms planning at the squad and platoon levels, training soldiers to network small drones, deploy decoys, contest the electromagnetic spectrum, and call precision fires in a single, integrated mission flow.

Recommendations

1. Institutionalize a SOF-Specific Rapid Drone Cell

Focus on Short-Cycle Acquisition and Field Testing

A dedicated SOF-specific rapid drone cell, focused on short-cycle acquisition and field testing, is critical for maintaining the technological edge in fast-evolving operational environments. According to *National Defense Magazine,* USSOCOM is actively working with industry to modernize uncrewed aerial systems, acknowledging that traditional acquisition takes "a year, two years, three years sometimes" to deliver and that drone operators must treat UAVs like "rounds or bullets" given high attrition rates in conflict zones like Ukraine.[21] This reinforces the necessity for a lean, empowered team within SOF to prototype, test, and field drones rapidly. By bypassing layered bureaucracy and deploying modular, expendable systems quickly, such a cell can respond to emergent threats with speed and battlefield relevance, unlike slow acquisition cycles that lag behind active combat needs. SOF acquisition strategy should formally embed a rapid drone cell structure, empowered to conduct fast-turn validation, operator feedback loops, and agile procurement, ensuring resilience and innovation align directly with contemporary operations.

2. Develop Tactical Doctrine for Low-Cost Uncrewed Systems Swarming

Operations for Electronic Warfare, Decoy, Intelligence, Surveillance, Reconnaissance, and Strike Missions

Doctrine must evolve to operationalize low-cost unmanned systems by embedding swarm tactics across EW, decoy, ISR, and strike missions at tactical levels. The Modern War Institute highlights that drone swarms increasingly incorporate specialized nodes, such as relay drones for communications, decoys to saturate

defenses, ISR drones for reconnaissance, and attack drones for lethal strikes, demonstrating a multi-role, doctrinally consolidated swarm architecture.[22] By treating swarms as integrated systems with distinct functional roles, forces can disrupt enemy defenses, gather intelligence, and deliver effects simultaneously. Decoys protect valuable assets, ISR nodes build situational awareness, EW drones counter enemy jamming, and strike drones apply lethal force, all coordinated within a unified swarm doctrine. Without such doctrinal integration, deployments risk being ad hoc and inefficient, reducing strategic impact. Formalizing swarm doctrine, defining roles, command structures, tactics, and training, will enable forces to fully exploit low-cost uncrewed systems (UxS) capabilities and scale combined effects across contested operational environments.

3. Create a Modular, Exportable Training Pipeline

Accessible Uncrewed Systems Training for Teams Across USSOCOM and Joint Partners

A modular, exportable training pipeline for unmanned systems is essential to standardize and rapidly deploy UxS capabilities across USSOCOM and allied/joint forces. The Colorado Army National Guard's Drone Warfare Cell (DWC) offers a compelling model: Since 2022, it has trained over 400 service members in small, unmanned aircraft systems/counter unmanned aircraft systems operations and embedded advisors with deployed units, blending technical training, field advising, and hands-on integration in real-world missions.[23] This initiative demonstrates how a mobile, modular training unit can bridge capability gaps across diverse forces. By combining classroom instruction, on-the-ground advising, and dynamic redteaming, the DWC ensures that both SOF and conventional units rapidly master drone employment. Its scalable, exportable model fosters interoperability, accelerates skill proliferation, and institutionalizes UxS tactics and procedures across coalitions.

> ***By treating swarms as integrated systems with distinct functional roles, forces can disrupt enemy defenses, gather intelligence, and deliver effects simultaneously.***

USSOCOM should adopt this model by establishing a rapid drone training pipeline—a dedicated mobile cell that delivers modular curricula, certifies teams, and embeds with units across the force. This would create a ready, unified training framework adaptable to evolving UxS requirements and mission sets.

4. Prioritize Interoperability and Digital Twin Integration

For Mission Rehearsal and Scalable Simulations

To enhance mission rehearsal and scalability, interoperability and digital twin integration must be prioritized in training pipelines for unmanned and manned systems. Aerospace & Defense Review highlights that digital twins now enable comprehensive mission rehearsal, simulating battlefield conditions, troop movements, and system interactions, to optimize tactics and logistics ahead of deployment.[24] By linking live and virtual environments, interoperable digital twins allow units to rehearse complex operations under realistic conditions without endangering personnel. This enhances preparedness, validates integration between UxS and human teams, and ensures systems operate cohesively in joint and coalition settings. It also elevates scalability, enabling large-scale, distributed simulations critical for digital-age wargames and contingency planning. Doctrine should formally integrate digital twins and interoperability standards, such as the Multilateral Interoperability Programme (MIP) and the Live, Virtual, and Constructive Integrating Architecture (LVC-IA), into mission rehearsal and acquisition

frameworks, ensuring scalable simulation becomes a cornerstone of operational readiness and cross-domain interoperability.

5. Partner with Ukraine, Taiwan, and Commercial Innovators

Drive Cross-Theater Lessons Learned and Accelerate Design Feedback Loops

To rapidly integrate battlefield innovation and stay ahead of evolving threats, strategic partnerships with Ukraine, Taiwan, and commercial innovators are essential for accelerating design feedback and cross-theater learning. The DoW's "Industry Partnerships for Crises" report highlights Ukraine's Rapid Capability Group and Taiwan's UNIT[25] City innovation park as exemplary models, leveraging commercial-tech clusters and cross-border collaboration to fast-track prototype development and deployment of unmanned systems. These ecosystems enable iterative, frontline-informed prototyping cycles, breaking enduring silos between lab and theater. By tapping into local startups and academic innovators, and sharing lessons across allied theaters, defense agencies can validate concepts rapidly, reduce technical risk, and tailor systems to actual operational contexts. This accelerates capability delivery far beyond conventional acquisition methods. To capitalize on this agility, DoW and USSOCOM should formalize structured partnerships with Ukrainian and Taiwanese innovation hubs, pairing them with commercial venture networks to sustain a fast, iterative "fight-learn-field" feedback loop across peer-theater contexts. See Table 1.

Conclusion

In sum, the future operating environment demands that SOF evolve beyond legacy paradigms and embrace a more agile, technology-driven posture. Low-cost, modular, and expendable

Table 1. Summary of Recommendations for Integrating Low-Cost Uncrewed Systems into U.S. Special Operations Forces

Recommendation	Primary Focus	Expected Operational Benefit	Strategic Priority
Institutionalize a SOF-specific rapid drone cell	Rapid acquisition, prototyping, operator feedback, and agile procurement	Accelerates capability development, reduces acquisition timelines, and enables rapid adaptation to emerging operational requirements	High
Develop tactical doctrine for low-cost, uncrewed systems swarming	Electronic warfare; decoy operations; intelligence, surveillance, and reconnaissance; strike missions, and swarm tactics	Standardizes employment of low-cost uncrewed systems, increases operational effectiveness, and enables coordinated multi-domain effects	High
Create a modular, exportable training pipeline	Standardized training, certification, mobile instructor teams, and coalition interoperability	Rapidly expands operator proficiency across U.S. Special Operations Command, the joint force, and allied partners while improving interoperability	High
Prioritize interoperability and digital twin integration	Digital twins, mission rehearsal, live-virtual-constructive simulation, and interoperability standards	Improves mission planning, rehearsal realism, system integration, and joint operational readiness	Medium-high
Partner with Ukraine, Taiwan, and commercial innovators	Battlefield innovation, commercial technology, rapid prototyping, and lessons learned	Accelerates technology maturation, shortens design feedback loops, and incorporates operational lessons into future capabilities	High

Source: Author

uncrewed systems are no longer supplemental tools but essential components of operational advantage in contested and gray-zone conflicts. As recent battlefields demonstrate, the decisive edge will belong to the forces able to rapidly iterate, integrate human-machine teaming, and adapt under constant pressure. By modernizing acquisition pathways, leveraging commercial innovation, and institutionalizing experimentation, SOF can maintain relevance and resilience in great-power competition. Ultimately, the units

> ***Low-cost, modular, and expendable uncrewed systems are no longer supplemental tools but essential components of operational advantage in contested and gray-zone conflicts.***

that out-learn and out-field their adversaries will define the next era of deterrence and conflict, and SOF is uniquely positioned to lead that transition.

About the Author

AJ Rutherford, PhD, is a retired U.S. Marine Corps Special Operations Team Chief and an overseas defense and security consultant specializing in special operations, counter-uncrewed aerial systems (C-UAS), human systems integration (HSI), artificial intelligence, and emerging defense technologies. He holds a PhD in information security and assurance and an MA in strategic intelligence.

In addition to his consulting work, Dr. Rutherford serves as a professor at American Military University, where he teaches undergraduate and graduate courses in cybersecurity, biometrics, operating systems security, and graduate capstone research. He also teaches graduate cybersecurity courses at Norwich University and mentors doctoral candidates at the University of the Cumberlands, specializing in information governance and cybersecurity research.

Dr. Rutherford's research focuses on the integration of artificial intelligence, autonomous systems, HSI, and cognitive performance into special operations and modern defense enterprises. His work explores the operational employment of autonomous systems, human-autonomy teaming, digital transformation, and the evolution of special operations forces in the context of great-power competition and fifth-generation warfare. As both an academic researcher and operational practitioner, he bridges emerging technologies with real-world military applications to improve training, operational effectiveness, organizational learning, and enterprise capability development.

Dr. Rutherford actively collaborates with government, industry, and academia and welcomes opportunities to conduct research, advise defense organizations, and present on artificial intelligence, autonomous systems, Human Systems Integration, and the future of special operations.

Notes

1. Jack Watling and Nick Reynolds, *Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine* (Royal United Services Institute, 2023), https://www.rusi.org/explore-our-research/publications/special-resources/meatgrinder-russian-tactics-second-year-its-invasion-ukraine.

2. Kelly M. Sayler, *DOD Replicator Initiative: Background and Issues for Congress*. CRS In Focus IF12611 (Congressional Research Service, January 21, 2026), https://www.congress.gov/crs-product/IF12611.

3. Kristan Stoddart, "Russia's Cyber Campaigns and the Ukraine War: From the 'Gray Zone' to the 'Red Zone,'" *Applied Cybersecurity & Internet Governance* 3, no. 1 (2024): 5–33, https://doi.org/10.60097/ACIG/189358.

4. Hal Brands, *Paradoxes of the Gray Zone* (Foreign Policy Research Institute, 2016), https://www.fpri.org/article/2016/02/paradoxes-gray-zone/.

5. Laviniu Bojor and Laurențiu Grigore, "Tactical Network-Centric Warfare in Practice: FPV Drones and the Architecture of a New RMA," *Knowledge-Based Organization* 31, no. 1 (2025): 30–45, https://doi.org/10.2478/kbo-2025-0004.

6. Jon-Wyatt Matlack, Sebastian Schwartz, and Oliver Gill. *Ukraine's Drone Ecosystem and the Defence of Europe: Lessons Lost Can't Be Learned* (LSE IDEAS, London School of Economics and Political Science, 2025), https://www.lse.ac.uk/ideas/publications/research-reports/ukraines-drone-ecosystem-and-the-defence-of-europe-lessons-lost-cant-be-learned.

7. Rebecca Rommen, "Ukraine's Rapidly Scaling Defense Industry Is Changing How the West Thinks About Future Wars," *Business Insider*, July 9, 2025, https://www.businessinsider.com/ukraine-defense-industry-changing-how-west-thinks-about-war-russia-2025-7.

8. Dominika Kunertová, "Embracing Drone Diversity: Five Challenges to Western Military Adaptation" in *Drone Warfare, Paper 29*, (Freeman Air and Space Institute, King's College London, April 2025), https://www.kcl.ac.uk/warstudies/assets/paper-29-dr-dominika-kunertova.pdf.

9. Oleksandra Molloy, *Drones in Modern Warfare: Lessons Learnt from the War in Ukraine. Occasional Paper 29*, (Australian Army Research Centre, 2024), https://researchcentre.army.gov.au/library/occasional-papers/drones-modern-warfare.

10. Benjamin Jensen and Yasir Atalan, "Drone Saturation: Russia's Shahed Campaign." *Center for Strategic and International Studies*, May 13, 2025, https://www.csis.org/analysis/drone-saturation-russias-shahed-campaign.

11. Anthony Pino and Scott Pettigrew. "Drones Having Psychological Impact on Soldiers." *Red Diamond*, U.S. Army Training and Doctrine Command (TRADOC) G-2, December 11, 2024, https://oe.t2com.army.mil/site-content/OEE/Red%20Diamond/TRADOC_11DEC2024_Drone_Psychological_Impact_Peno_Pettigrew.pdf.

12. Davied Kirichenko, "Ukraine's Battlefield Drone Innovations Are Influencing Europe's Militaries," *Small Wars Journal*, June 11, 2025, https://smallwarsjournal.com/2025/06/11/ukraines-battlefield-drone-innovations/.

13. Kateryna Bondar, *How Ukraine Rebuilt Its Military Acquisition System Around Commercial Technology*, Center for Strategic and International Studies, January 13, 2025, https://www.csis.org/analysis/how-ukraine-rebuilt-its-military-acquisition-system-around-commercial-technology.

14. Jon Harper, "SOCOM Searching for Reconfigurable 'Drone in a Box' Systems That Can Fly and Drive," *DefenseScoop*, March 10, 2025, https://defensescoop.com/2025/03/10/socom-drones-uas-ugv-robots-reconfigurable-sof-sofwerx/; Daryna Ostafiichuk et al., *Building & Leveraging Ukraine's Drone Capabilities in Conflict & Beyond: Assessing the Defense/Security Innovation Ecosystem*. White paper, MIT Sloan School of Management and Kyiv School of Economics, March 2025. https://murray-lab.org/wp-content/uploads/2025/03/UkraineDroneEcosystem-Analysis_2025.pdf.

15. Mariam Halstian. "A First Point View: Examining Ukraine's Drone Industry." *Georgetown Security Studies Review*, May 15, 2025, https://georgetownsecuritystudiesreview.org/2025/05/15/a-first-point-view-examining-ukraines-drone-industry/.

16. Gheorghe Minculete, "Military Logistics Drones: The Innovative Solution for Transportation Challenges on the Battlefield," *Land Forces Academy Review* 30, no. 2 (2025): 342–354, https://doi.org/10.2478/raft-2025-0033.

17. Rueben Dass, "3D-Printing in Conflict Zones: A Game-Changer?" *Global Network on Extremism and Technology (GNET)*, October 14, 2024, https://gnet-research.org/2024/10/14/3d-printing-in-conflict-zones-a-game-changer/

18. Andre Haider and Andreas Schmidt, "Defining Swarm: A Critical Step Toward Harnessing the Power of Autonomous Systems," *Military Review Online Exclusive*, U.S. Army Combined Arms Center, May 29, 2025, https://www.armyupress.army.mil/journals/military-review/online-exclusive/2025-ole/defining-swarm/

19. Robert O. Work, *Principles for the Combat Employment of Weapon Systems with Autonomous Functionalities*, Center for a New American Security, April 28, 2021, https://www.cnas.org/publications/reports/proposed-dod-principles-for-the-combat-employment-of-weapon-systems-with-autonomous-functionalities.

20. Jack Watling and Noah Sylvia, *Competitive Electronic Warfare in Modern Land Operations*. Occasional Paper, Royal United Services Institute, January 30, 2025, https://www.rusi.org/explore-our-research/publications/occasional-papers/competitive-electronic-warfare-modern-land-operations.

21. Allyson Park, "Special Operations Command Needs Industry Help Upgrading Uncrewed Systems," *National Defense Magazine*, June 20, 2025, https://www.nationaldefensemagazine.org/articles/2025/6/20/aerial-threats-special-operations-command-needs-industry-help-upgrading-uncrewed-systems.

22. Zachary Kallenborn, "Swarm Talk: Understanding Drone Typology," *Modern War Institute at West Point*, December 10, 2021. https://mwi.westpoint.edu/swarm-talk-understanding-drone-typology/.

23. Melissa Escobar-Pereira, "Colorado Army Guard's Drone Warfare Cell Reshapes Warfighting," *U.S. National Guard*, July 25, 2025, https://www.nationalguard.mil/News/Article-View/Article/4219472/colorado-army-guards-drone-warfare-cell-reshapes-warfighting/.

24. "Digital Twins in Defense: A New Era for Military Strategy and Operational Effectiveness," *Aerospace & Defense Review*, January 16, 2026, https://www.aerospacedefensereview.com/news/digital-twins-in-defense-a-new-era-for-military-strategy-and-operational-effectiveness-nwid-2158.html.

25. Defense Business Board, *Industry Partnerships for Crises*, Study Report FY25-01, U.S. Department of Defense, November 22, 2024. https://dbb.defense.gov/Portals/35/Documents/Reports/2025/Industry%20Partnerships%20for%20Crises%20Study%20Report_CLEARED_%2022%20Nov_red.pdf.

Chapter 2

Rapid All-Domain Fusion for SOF

Future operating environments will demand a level of integration, agility, and cross-domain synchronization that few organizations are positioned to provide. SOF are increasingly involved in complex missions that span physical, cyber, and information domains. As strategic competition intensifies and operational challenges become more interconnected, SOF must be able to coordinate effects across military and civilian organizations while maintaining the flexibility to adapt to evolving mission requirements.

The papers in this chapter explore the concepts, organizational models, and capabilities required for SOF-led integration across domains. Contributors examine approaches to joint force structuring and resourcing, the decision-making processes needed to enable faster and more effective operations, and the challenges of securing and maintaining access for cyber activities. Together, these studies provide insights into how SOF can enable more cohesive, responsive, and strategically effective operations in contested environments.

Architects of Fusion:
A Mission-Focused Model for Rapid All-Domain Fusion for SOF

By Maj. Scott C. Hall

This is the JSOU AY2026
Call for Special Operations Papers

Category 1

Third-Place
Winner

Digital Version

Introduction

The joint force is not short on technology. It is short on command structures built to turn that technology into operational advantage before a crisis outruns the headquarters (HQ) trying to manage it. For more than a decade, the Department of War has advanced concepts such as joint all-domain command and control and multi-domain operations to connect sensors, shooters, and decision networks across land, air, maritime, cyber, and space.[1] Rapid advances in AI, commercial space capabilities, and global interconnectivity have dramatically expanded the joint force's ability to collect, process, and disseminate information.[2] Yet in practice, integration still too often depends on ad hoc coordination, liaison officers, and capabilities pulled together only after a problem has already broken loose.

Despite progress, the joint force continues to struggle with a fundamental problem: technology has outpaced organizational structure. The ability to connect systems has not translated into the ability to command them coherently across domains. Integration often depends on ad hoc coordination, typically through liaison officers, rather than persistent organizational frameworks constructed for cross-domain campaigning.[3] Combatant commands and service components possess capabilities in cyber, space, intelligence, and information operations, but these capabilities frequently reside in separate organizational stovepipes, synchronized only episodically during exercises or thrown together during national crises.

Despite progress, the joint force continues to struggle with a fundamental problem: technology has outpaced organizational structure.

That gap is no longer theoretical. China and Russia are already competing through systemic approaches designed to disrupt decision-making, fracture cohesion, and narrow U.S. decision space before large-scale combat begins.[4] The problem is not whether the joint force can connect systems. It can. The problem is whether it can command across domains fast enough, with enough unity of effort, to force adversaries into multiple dilemmas and preserve freedom of maneuver. That is not a technology problem. It is a command problem.

Special operations forces (SOF) provide the best foundation for solving it. Historically, SOF and its predecessors have excelled when the mission required integrating intelligence, irregular warfare (IW), influence, and maneuver into one scheme of action. From OSS and Jedburgh teams to joint special operations command's (JSOC's) fusion model, the lesson is consistent: advantage comes not merely from possessing capabilities but from organizing them to act in one operational rhythm. The joint force should build on that tradition by institutionalizing modular SOF fusion cells: standing, multidisciplinary teams that can bake cross-domain integration into campaigns rather than sprinkling it on in crisis. By institutionalizing this architecture now, the United States Special Operations Command (USSOCOM) can transform ad hoc convergence into persistent cross-domain command, delivering a decisive advantage before conflict begins.

The Return of Systemic Warfare

Great power competition is increasingly decided by which side can disrupt the other's system before shots are exchanged at scale. Modern adversaries are not seeking advantage only through superiority in one domain. They are trying to fracture the links between sensing, deciding, communicating, and acting. The goal is

not simply to destroy forces in detail. It is to paralyze the adversary's ability to coordinate action, preserve cohesion, and impose will.[5]

China's concepts of systems confrontation and systems destruction warfare reflect that logic. Chinese military theorists emphasize that modern military power depends on interconnected systems that link sensors, communications networks, command structures, and weapons platforms.[6] Rather than engaging U.S. forces symmetrically, Chinese doctrine prioritizes identifying and disrupting the key nodes that enable these systems to function. The objective is not to destroy enemy forces in detail but to paralyze the adversary's ability to coordinate action. This conceptual approach is reflected in organizational reform. The establishment of the People's Liberation Army Strategic Support Force consolidated cyber, space, electronic warfare, and psychological operations (PSYOP) capabilities into a unified command structure designed to enable cross-domain operations.[7] China has institutionalized the amalgamation that the U.S. continues to pursue episodically.

Russia has pursued a related approach by combining cyber operations, disinformation, proxy forces, and conventional military pressure. Often described as hybrid warfare, this model endeavors to achieve strategic objectives without triggering large-scale conflict.[8] Operations in Crimea and eastern Ukraine demonstrated how coordinated information operations and irregular forces could produce decisive strategic effects before conventional military responses could be mobilized.[9] Russian doctrine treats information warfare not as a supporting function but as a primary line of effort, synchronized with military operations from the outset.

In both cases, the objective is the same: create multiple dilemmas, compress the adversary's decision space, and shape the fight before conventional combat fully develops. These approaches illustrate a fundamental shift in warfare where the advantage is no

The joint force has world-class capabilities across all domains but lacks an organizational design and command architecture to bake those capabilities into campaigns and crisis action planning to make them operationally relevant.

longer derived from dominance within a single domain but from the ability to coordinate and synchronize effects across multiple domains simultaneously. The side that integrates faster, fusing intelligence, cyber, space, information warfare, and maneuver into campaigns and real-world operations, gains a decisive decision advantage over an adversary still coordinating through known comfortable processes of the last war.

The U.S. has recognized the need for all-domain integration through concepts such as Joint All-Domain Command and Control and Multidomain Operations. However, these efforts often assume the existence of organizational structures capable of integrating capabilities at operational speed. In practice, such structures remain insufficiently developed, as capability planners are confined by frigid staff structures and processes, the tyranny of distance, and read-ons, and coordination visibility gaps. The joint force has world-class capabilities across all domains but lacks an organizational design and command architecture to bake those capabilities into campaigns and crisis action planning to make them operationally relevant. Our strategic competitors have built the organizational structures to fight systemically; the U.S. must do the same.

Historical Foundations of SOF Convergence

Synchronizing multiple domains is not a new concept. Long before modern terminology emerged, SOF were already conducting

Under General Stanley McChrystal, joint special operations command collapsed these barriers by embedding intelligence analysts, signals intelligence specialists, and operational planners within a single unified command structure.

integrated campaigns that combined intelligence, IW, and influence operations into unified efforts.

During the Second World War, the Office of Strategic Services (OSS) developed a model of warfare that fused intelligence collection, sabotage, and PSYOP into unified campaigns supporting Allied objectives.[10] OSS teams coordinated resistance movements, conducted sabotage operations, and directed airpower against enemy logistics networks, demonstrating the operational value of integrating a wide range of capabilities under a single organizational framework. The OSS did not exclusively collect intelligence or conduct raids; it synchronized multiple forms of power to achieve strategic effects.

The Jedburgh program represents one of the most effective examples of this approach. Small three-man teams, comprising an American, a British officer, and a French national, were inserted into occupied Europe to coordinate resistance networks, enabling sabotage operations, intelligence collection, and support to conventional forces.[11] These teams served as operational bridges, linking indigenous forces with Allied command structures and increased the effects of conventional operations through integrated IW.

Jedburgh teams operated with minimal guidance, exercising mission command in non-permissive environments where communication with higher HQ was intermittent at best. Their

success depended not on technological overmatch but on organizational design: small, integrated teams empowered to synchronize multiple capabilities toward common objectives.[12] The success of OSS and Jedburgh operations demonstrated a core principle that is still relevant today: small, integrated teams capable of coordinating multiple forms of power can generate disproportionate operational impact. This principle, integration through organizational architecture rather than technological connectivity alone, forms the foundation for modern SOF fusion concepts.

The Joint Special Operations Command Fusion Model

Modern SOF operations have reaffirmed this principle. During counterterrorism campaigns in Iraq and Afghanistan, JSOC developed an operational model that fused intelligence and operations into a continuous loop, demonstrating that organizational architecture creates operational speed. Early operations revealed that traditional intelligence processes were too slow to support dynamic targeting against networked adversaries. Intelligence collection, analysis, and operational planning were conducted in separate organizational structures, creating delays that allowed adversary networks to regenerate and resynchronize.[13] The problem was not a lack of information but an inability to translate it into action at the required speed.

Under General Stanley McChrystal, JSOC collapsed these barriers by embedding intelligence analysts, signals intelligence specialists, and operational planners within a single unified command structure.[14] Rather than passing information through lumbersome staff processes, JSOC created a shared operational environment wherein intelligence and operations personnel worked

side by side, permitting continuous refinement of operational understanding and action.

This action enabled the development of the "find, fix, finish, exploit, analyze, and disseminate" cycle. Captured materials and communications data were analyzed in near real time, supporting rapid identification of follow-on targets. Each operation generated intelligence that fed into the next, creating a self-sustaining cycle that dramatically boosted operational tempo.[15] JSOC was able to dismantle complex networks not just through superior firepower but through superior synchronization.

JSOC's advantage was not some hidden technical edge. It was the decision to reorganize around the problem. By collapsing intelligence and operations into one battle rhythm, JSOC reduced delay, accelerated learning, and turned each action into the start point for the next one rather than the end of a discrete event. The lesson is not that technology is irrelevant. The lesson is that technology without the right command structure produces only episodic coordination. JSOC moved faster because it fused people, authorities, and workflows around the fight. That lesson applies directly to all-domain fusion today.

Why SOF Is the Natural Integrator

SOF is the logical force to lead this effort because integration is already how it fights. SOF missions routinely operate at the seams between intelligence, partner forces, influence, cyber, and maneuver. Unlike formations optimized primarily for mass in a single domain, SOF has long depended on combining diverse capabilities in ambiguous environments where access is limited, authorities are constrained, and decisions must be made at speed. For SOF, integration is not an added requirement. It is how small formations generate outsized operational effects.[16]

SOF also brings something the broader joint force often struggles to maintain: persistent relationships. Its global networks with allies, partners, and interagency organizations create access, awareness, and options that can be turned into operational advantage before crisis turns into conflict. These relationships matter because cross-domain fusion is not just a technical exercise. It is a command-and-trust problem that depends on people who already know how to work across organizational, geographical, and political boundaries.[17]

Just as important, SOF culture already aligns with the demands of this fight. It values mission command, adaptability, decentralization, and operating with incomplete information. Those traits matter in a contest where planners must shorten friendly decision cycles while forcing the adversary into multiple dilemmas. This cultural orientation aligns directly with the demands of rapid all-domain fusion, where decision cycles must compress, and authority must be distributed.[18] Strategic competition with China and Russia unfolds largely below the threshold of open war, in the same contested space where SOF has long operated. That makes SOF more than merely capable of leading all-domain fusion. It places SOF in the part of the battlefield where fusion matters most.[19]

> ***For SOF, integration is not an added requirement. It is how small formations generate outsized operational effects.***

SOF Fusion Concepts for All-Domain Campaigning

If the joint force wants real all-domain fusion, it cannot wait until a crisis to assemble it. Ad hoc coordination is not a warfighting architecture. The force needs standing organizations that can identify opportunities, secure access, and synchronize cross-

domain effects before events outrun HQ trying to manage them. The first requirement is a theater-level organization that can operate continuously during competition, not just during crisis. Their job is to connect SOF planning with cyber, space, intelligence, and information warfare capabilities already present in theater and beyond it. The second requirement is that it needs a smaller forward element that can carry that integration into contested spaces alongside maneuver forces and partners. They give forward commanders a way to request cyber effects, pull space-enabled awareness into tactical decisions, and synchronize information activities in near real time. One without the other is incomplete. A theater hub without an expeditionary edge becomes another HQ node. A forward team without a theater backbone becomes isolated and reactive. Together, they give commanders a way to preserve continuity from campaign design to action at the point of contact.

Concept A: Theater SOF Fusion Cells

These are persistent organizations embedded within theater special operations commands that coordinate cross-domain effects during competition and crisis. Theater fusion cells serve as integration hubs connecting SOF operational planning with cyber, space, intelligence, and information warfare capabilities resident within the theater. They maintain continuous situational awareness across domains, identify opportunities for cross-domain effects, and coordinate with national-level agencies to access capabilities beyond theater resources. Furthermore, they provide the doctrinal and technical basis for synchronizing non-lethal and non-kinetic effects, assuring these capabilities contribute directly to operational control within the theater commander's campaign design.[20]

Theater fusion cells operate during steady-state competition, not exclusively during crisis or conflict. This posture enables the development of cross-domain campaign plans, the cultivation

Expeditionary fusion cells deploy with SOF task forces conducting operations in contested or denied environments, providing organic cross-domain integration at the tactical forefront.

of relationships with cyber, space, and information warfare organizations, and the refinement of integration operations before they are tested under pressure.

Concept B: Deployable Expeditionary Fusion Cells

These are smaller, forward-deployed teams integrating cyber, space, and information capabilities alongside SOF maneuver elements.

Expeditionary fusion cells deploy with SOF task forces conducting operations in contested or denied environments, providing organic cross-domain integration at the tactical forefront. Expeditionary fusion cells translate theater-level coordination into tactical action. They enable SOF elements to request and integrate cyber effects, leverage space-based intelligence, and synchronize information operations in near real time. By embedding fusion capability within deploying forces, the architecture ensures that cross-domain integration extends to SOF teams.

Together, these concepts create a layered architecture meant to close the seam between them. Theater fusion cells provide operational-level integration and connectivity to national capabilities, while expeditionary fusion cells deliver tactical-level fusion alongside maneuver forces. This layered approach nests integration and synchronization, which are not confined to HQ but

extend throughout the operational environment to tactical units, and preserve decision space.

Modular SOF Fusion Cell Architecture

Every fusion cell should include a small group of people who can see the fight from different angles but work from the same operational problem. The SOF operational planner keeps the cell tied to maneuver, campaign objectives, and the commander's purpose. This role matters because cross-domain effects that are not linked to scheme of maneuver quickly become noise.

The cyber effects planner gives the cell a way to move beyond awareness and into options. This role helps identify where cyber access can expose, protect, disrupt, deceive, or prepare the environment without losing sight of approval timelines and escalation concerns. The cyber planner maintains connectivity with U.S. Cyber Command and theater cyber organizations.

The space integration officer prevents the cell from fighting blind. This role connects space-based capabilities, including intelligence, surveillance, reconnaissance, deep communication, and maintains awareness when adversaries try to fracture the network. Space support in this construct is not a specialty add-on. It is part of keeping the force inside the adversary's decision cycle. The space officer coordinates with U.S. Space Command, theater space organizations, and commercial space providers.

The data and AI exploitation lead turns data volume into data clarity. Modern commands are drowning in reporting, feeds, and indicators. This role manages data integration and applies AI plus machine-learning tools to accelerate decision dominance. This function addresses the growing volume of data available to

operational commanders and assures that information is translated into actionable intelligence.

The information warfare planner is what keeps the cell from reducing fusion to a cyber-space drill. This role synchronizes influence activities, deception, military information support operations, narrative competition, and perception management with physical and digital actions. The inclusion of an information warfare planner reflects the growing importance of the cognitive dimension in modern conflict.[21] The information warfare officer coordinates with the service component command J-39s and regionally aligned U.S. Army Theater Information Advantage Detachments.

The inclusion of information warfare professionals transforms the traditional SOF-cyber-space triad into a four-domain integration model that incorporates cognitive effects along with physical and digital operations. The Army's preparations to establish the Information Warfare branch underscore the need to professionalize operations in the cognitive domain.[22] Information advantage must be baked in, not sprinkled on top after maneuver has already begun. That is why this function belongs in the core, not on the periphery. Embedding this functionality within fusion cells assures that a pure focus on gaining the information advantage and obtaining decision dominance are integrated from the outset rather than addressed as an afterthought.

Fusion cells function as connective tissue between SOF maneuver elements and national-level capabilities. They provide the ability to frame the fight as one problem, not four separate staff conversations. That is what allows the command to converge effects, exploit vulnerabilities, and force adversaries into multiple dilemmas rather than reacting one stovepipe at a time. They do not replace existing organizations but provide the persistent

Legal advisors embedded within fusion cells deliver real-time guidance on the legal ramifications of proposed operations, assuring compliance with domestic and international law.

architecture needed to coordinate capabilities currently residing in separate stovepipes.

Risks, Friction, and Escalation Management

Any architecture built to move faster across domains also creates risk if it is not disciplined. Cyber and space actions can generate effects well beyond the local fight, especially when reconnaissance, preparation, disruption, and attack are hard for an adversary to distinguish in real time. The danger is not merely technical misunderstanding. It is strategic misread. A tactical action taken for access or signaling can be interpreted as the opening move of escalation.[23]

That does not argue against fusion cells. It argues for building them correctly. Clear authorities, embedded legal review, and standing coordination with national-level organizations must be part of the design from the start. Fusion cells must operate within command authorities, with appropriate oversight for operations carrying escalation risk.

Legal advisors embedded within fusion cells deliver real-time guidance on the legal ramifications of proposed operations, assuring compliance with domestic and international law. Training is just as important as structure. Fusion personnel should rehearse ambiguous situations in which the same action could be read as intelligence preparation, signaling, interference, or attack. If they do

not understand that gray zone, they will eventually create tactical gain at strategic cost. The point is not to slow the architecture down until it becomes another staff process. The point is to make speed disciplined enough to preserve freedom of maneuver rather than collapse it through miscalculation.

Institutional friction will be harder than technology. Persistent fusion cells cut across existing equities, approval chains, and command relationships. Some organizations will see them as duplication, others as encroachment. That resistance should be expected. The answer is not another concept brief. It is demonstrated value: shorter decision cycles, better synchronized options, and visible operational payoff in competition and crisis.

Operational Illustration: Western Pacific Crisis

To illustrate how the proposed architecture functions under pressure, consider a crisis scenario in the Western Pacific.

Intelligence indicators indicate Chinese amphibious forces are mobilizing in coastal areas opposite Taiwan. Satellite imagery reveals increased naval activity, while cyber intelligence detects probing of regional communications networks. The situation is ambiguous. None of that alone proves invasion. But taken together, it creates a problem commanders cannot afford to read too slowly. The danger is not only surprise. It is miscalculation under ambiguity.

A theater SOF fusion cell embedded within Special Operations Command Pacific pull satellite imagery, signals intelligence, cyber indicators, and partner reporting into one picture, then use data tools to compare the activity against historical baselines. The point is not simply to collect more information. It is to determine what kind of problem the command is actually facing early enough to act with discipline instead of reacting with panic.

If the assessment shows a coercive demonstration rather than imminent invasion, that distinction matters operationally. It means the right answer is not immediate kinetic action. It is a synchronized response that exposes hostile intent, protects allied networks, reinforces partner confidence, and changes Beijing's calculus before the situation hardens into conflict. That is where fusion earns its keep.

Rather than recommending kinetic options that might accelerate escalation, the fusion cell develops an integrated response combining multiple domains. The information warfare planner coordinates with interagency partners to expose Chinese disinformation narratives, undermining Beijing's information campaign. The cyber planner coordinates defensive measures to protect allied communications networks while positioning capabilities for potential offensive operations if authorized. The space integration officer provides continuous surveillance coverage and coordinates with commercial providers to supplement military assets.

Simultaneously, an expeditionary fusion cell deployed with a SOF element in the Philippines coordinates with partner forces, positioning capabilities to demonstrate allied resolve while avoiding provocative actions. The cell integrates partner intelligence, coordinates information operations messaging, and maintains connectivity with the theater fusion cell.

The point in such a crisis is not to win a dramatic exchange. It is to get inside Beijing's decision-making cycle early enough to prevent the situation from hardening into a military confrontation. The decision advantage created by fusion cells is not a single capability but the ability to turn information into coordinated action across several domains before the adversary can lock in its preferred narrative or tempo. That gives commanders a better chance to frame

> *If the assessment shows a coercive demonstration rather than imminent invasion, that distinction matters operationally. It means the right answer is not immediate kinetic action.*

problems correctly, expose hostile activity, impose doubt, preserve allied freedom of maneuver, and de-escalate from a position of strength rather than from delay.

Conclusion

Better networks alone will not solve this problem. The joint force already has no shortage of platforms, sensors, and technical means. What it still lacks is a standing command structure that can turn those capabilities into unified campaign effects across domains before a crisis outruns the staff processes built to manage it. Adversaries have recognized that modern war is fought by attacking systems, decision cycles, and cohesion, not merely by trading firepower. The U.S. must organize accordingly.

SOF's history points to a practical answer. From the OSS and Jedburghs to JSOC, the lesson is consistent: small, integrated teams that combine intelligence, influence, and maneuver can create disproportionate operational advantage when they are organized to act in one rhythm. That legacy should not remain a historical reference point. It should be institutionalized for the modern fight. Modular SOF fusion cells provide a practical way to do that by connecting theater-level integration with forward expeditionary execution.

The debate is no longer whether all-domain fusion is necessary. Adversaries have already answered that question through their

behavior. The real question is whether the joint force will build the structure to command across domains before conflict exposes the cost of not doing so. The issue is not simply connecting systems. It is forcing adversaries into multiple dilemmas, preserving freedom of maneuver, and commanding the fight as one campaign. Fusion cells offer a credible path to do that.

About the Author

Maj. Scott Hall is an information operations officer with extensive experience in maneuver operations, cyber, and operations in the information environment. His career includes multiple combat deployments to the Middle East, key command assignments, and service as an observer-coach/trainer at the National Training Center and with the Army Service component command in the European theater. He has served in pivotal joint and army roles supporting U.S. Central Command, specializing in operational-to-strategic planning for non-kinetic effects. Hall holds a bachelor of arts in military history from Norwich University and a master of business administration from Grand Canyon University. Hall is a graduate of the U.S. Army War College defense strategy course.

Notes

1. Joint Chiefs of Staff, *Summary of the Joint All-Domain Command and Control (JADC2) Strategy* (Department of Defense, 2022), 1–4.
2. Ben Buchanan and Andrew Imbrie, *The New Fire: War, Peace, and Democracy in the Age of AI* (MIT Press, 2022), 45–67.
3. David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd ed. (CCRP Publication Series, 2000), 87–112.
4. Frank G. Hoffman, "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges," *Prism* 7, no. 4 (2018): 30–47.
5. Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare* (RAND Corporation, 2018), 7–15, https://www.rand.org/pubs/research_reports/RR1708.html.
6. Engstrom, *Systems Confrontation and System Destruction Warfare*, 23–31.
7. Elsa B. Kania and John Costello, *The Strategic Support Force and the Future of Chinese Information Operations* (Center for a New American Security, 2020), 5–12, https://www.cnas.org/publications/reports/the-strategic-support-force-and-the-future-of-chinese-information-operations.
8. Mark Galeotti, "The Mythical 'Gerasimov Doctrine' and the Language of Threat," *Critical Studies on Security*, no. 2 (2019): 157–161, https://doi.org/10.1080/21624887.2018.1441623.
9. Michael Kofman et al., *Lessons from Russia's Operations in Crimea and Eastern Ukraine* (RAND Corporation, 2017), 12–28, https://www.rand.org/pubs/research_reports/RR1498.html.
10. Thomas F. Troy, *Donovan and the CIA: A History of the Establishment of the Central Intelligence Agency* (Center for the Study of Intelligence, Central Intelligence Agency, 1981), 417–422.
11. Colin Beavan, *Operation Jedburgh: D-Day and America's First Shadow War* (Viking, 2006), 112–145.
12. Will Irwin, *The Jedburghs: The Secret History of the Allied Special Forces, France 1944* (PublicAffairs, 2005), 67–89.
13. Sean Naylor, *Relentless Strike: The Secret History of Joint Special Operations Command* (St. Martin's Press, 2015), 156–178.

14 Stanley McChrystal, *My Share of the Task: A Memoir* (Portfolio/Penguin, 2013), 148–162.

15 Linda Robinson, *The Future of U.S. Special Operations Forces*, Council on Foreign Relations Special Report No. 66 (Council on Foreign Relations, April 2013), 13–23, https://www.cfr.org/report/future-us-special-operations-forces.

16. U.S. Army John F. Kennedy Special Warfare Center and School, "The SOF-Space-Cyber Triad," *Special Warfare: The Professional Journal of U.S. Army Special Operations Forces* 37, no. 2, (Summer/Fall 2024), https://www.swcs.mil/Portals/111/SWJ_SUMMER-FALL%2024_vol%2037%20issue%202_TRIAD_INTERACTIVE.pdf.

17. United States Special Operations Command, *SOCOM 2020 Strategy* (USSOCOM, 2020), 8.

18. Department of the Army, *Army Doctrine Publication 6-0: Mission Command: Command and Control of Army Forces* (Department of the Army, July 2019), 1–3 to 1–7.

19. United States Special Operations Command, *SOF Renaissance: People, Win, Transform* (USSOCOM, 2025), 6.

20. Scott Hall, "Synchronizing Non-Lethal and Non-Kinetic Effects for Operational Control," *Small Wars Journal*, November 7, 2025, https://smallwarsjournal.com/2025/11/07/synchronizing-non-lethal-and-non-kinetic-effects-for-operational-control/.

21. Ryan Walters, "Information Warfare: The Army's Continuous Transformation in Action," *Small Wars Journal*, January 15, 2026, https://smallwarsjournal.com/2026/01/15/army-information-warfare-transformation/.

22. Robert W. White, "Easier to Kill Than to Text: A Mandate for Information Warfare Reform," *Small Wars Journal*, March 24, 2026, https://smallwarsjournal.com/2026/03/24/easier-to-kill-than-to-text-a-mandate-for-information-warfare-reform/.

23. Martin C. Libicki, *Cyberdeterrence and Cyberwar* (RAND Corporation, 2009), 39–58, https://www.rand.org/pubs/monographs/MG877.html.

Meritocracy Resourcing

By Cmdr. J. A. Spector

Inroduction

Special operations forces (SOF) are, by design, competitive organisms. Competition is imbued in selection courses, culture, and character. It is embodied in SOF combat skills competitions that celebrate individual tactical excellence. It is reflected in U.S. Special Operations Command's (USSOCOM's) acquisition process that competes technologies to find the best of breed. Even the Global Force Management (GFM) process is, at its core, a competition for resources mediated through analytical justification.

Yet for all the competitive heritage, little is done to complete *integrated effective unit capability*: the real capability of complete units for a specific effect. Certification, verification, and validation (CV2) of capability against a unit's intended missions is practiced, but there is no competition across units to determine who is doing a certain mission the best, how they are doing it, and how others might do it better. This approach hides the functional methods the best units use against their hardest problems and squanders the competitive culture that should be driving targeted innovation. Special operations have failed to incentivize its greatest strength.

Compare this to the emerging incentive structures in the Russo–Ukrainian War. Ukraine's Army of Drones program rewards verified unit and equipment kills with points that units can exchange for new equipment.[1] It has been so successful for Ukraine's strategic objectives that Ukraine expects this program to deliver about 6–10 percent of all drone systems by the end of 2026.[2] Russia is now putting forward its own version of this program which rewards similar actions with individual bonuses and leave.[3] Both nations have found that direct, performance-based incentives are a powerful engine for effective tactical innovation and accelerating battlefield learning.

To outpace rivals, USSOCOM needs its own competitive framework that complements the current resourcing model while incentivizing and accelerating lethality-effective adaptation. Such a system must deliberately link discretionary resources to demonstrated excellence, not as an end in itself, but as the engine to speed institutional learning. By using $10M, less than 0.1 percent of USSOCOM's annual Operations and Maintenance (O&M) budget, to reward units that demonstrate superiority within a certain skill, USSOCOM can identify, codify, and disseminate best practices while incentivizing its top-performing units to push the boundaries even further.[4] USSOCOM must expand its existing competitive merit-based culture into illuminating comparably-superior unit capabilities that will accelerate collective SOF dominance on the modern battlefield.

USSOCOM's Current Competitive Environment

Acquisition: Competing for Technology

USSOCOM is the only combatant command with both operational command and acquisition authority vested in a single commander under Title 10 U.S.C. §167.[5] This arrangement allows USSOCOM to plan, resource, and acquire SOF-peculiar equipment within a single organization, with all acquisition support functions collocated at headquarters.[6] The result is a tight operator–acquirer feedback loop that is comparably significantly faster than the acquisition systems of the larger services.

These efforts can also be rapidly focused at producing results in critical areas of modern special operations warfare: countering unmanned systems,[7] contested logistics and autonomous resupply,[8] autonomy and AI,[9] and maritime intelligence, surveillance, and reconnaissance.[10] As USSOCOM's acquisition executive, Melissa Johnson, stated at SOF Week 2025: "We don't buy platforms; we

solve problems. The operator is the requirement. If it takes longer than 24 months from idea to fielding, we're doing it wrong."[11]



An experimental micro tactical ground robot during a testing event in 2025. (Photo by Army Staff Sgt. Jake SeaWolf)

While the successes of USSOCOM's acquisition system should be celebrated, so too must the shortcomings be acknowledged. A product delivered is not the same as an operational capability achieved. Even the best written requirements will evolve into only a limited number of concept prototypes that will be evaluated in a constrained environment and ultimately lead to a single winner. Even with constant operator feedback, the acquisition process remains siloed until a single winning system is delivered. While operators can provide feedback on that single system post-fielding, there is no backend competition. No mechanism exists to competitively measure that system's real-world effectiveness against alternatives at the warfighter-tech nexus. The acquisition feedback loop used by

USSOCOM, for all its celebrated speed, is incomplete: it closes the gap between requirement and procurement but leaves open the gap between procurement and operational excellence.

Individual Skills: Competing for Recognition

The U.S. special operations community runs or participates in a growing roster of combat skills competitions that test individual and small-team tactical excellence across the force. The U.S. Army Special Operations Command (USASOC) International Sniper Competition, now in its 16th year, draws three-person teams from every active and reserve Special Forces Group, the 75th Ranger Regiment, Naval Special Warfare, U.S. Marine Forces Special Operations Command (MARSOC), and allied SOF units. Designed by the instructors of the Special Forces Sniper Course at Fort Bragg, the 23-stage, five-day event is built explicitly around



Troops during the tactical lane portion of the U.S. Army Best Drone Warfighter Competition in February 2026. (Photo by Army Sgt. Aaron Troutman)

combat tasks to replicate the stress and complexity of real-world ground operations.[12]

The USASOC Best Combat Diver Competition, hosted at the Special Forces Underwater Operations School in Key West, is another example. In 2024, 12 two-person teams from Special Forces Groups, MARSOC, and Naval Special Warfare completed 10 events over three days—academic exams, physical fitness, subsurface navigation, helocasts, and over-the-beach operations.[13]

USSOCOM is also integrating into larger service competitions. SOF members participated in the Army's inaugural Best Drone Warfighter Competition in February 2026, which drew over 200 competitors for first-person view (FPV) races, tactical squad lanes, and innovation showcases.[14]

These competitions produce real value: cultural reinforcement, esprit de corps, individual career development, and a visible standard of tactical excellence. But they produce no cascading institutional effects. The winners received no increase in operational or training resources, units received no change in equipment allocations, and the SOF components incurred no mandate to proliferate what made their teams better or worse. The individual or team gets recognized, but the SOF institution learns little.

Unit Resourcing: Competing Through Justification

SOF units compete for resources through two primary mechanisms. The GFM and Program Objective Memorandum (POM) allocate units and resources through processes that are genuinely competitive, but neither competes on the basis of demonstrated unit superiority. GFM allocates forces within and across theaters in response to strategic demand signals. It can move quickly if needed but is generally a multiyear forecasted system. Importantly, the

competition within GFM is over *who needs a capability and what units can provide it*, not *who can deliver it best*.

POM operates much more slowly than GFM. POM builds component budgets years in advance through exhaustive analytical justification, locking in resource decisions long before the units receiving those resources have had a chance to demonstrate what they can do with them. Both processes are analytically rigorous and bureaucratically fierce. However, neither is designed to ask and evidentially support: Among units with comparable mission profiles, which one is employing its resources most effectively, and should that inform how the next dollar is allocated?

Two teams preparing for similar mission sets receive comparable weapons and equipment allocations regardless of whether one is demonstrably superior during workup. The closest existing mechanism to comparative assessment is the CV2 process, which evaluates units against their intended mission sets before deployment. But CV2 is a pass/fail gate, not a comparative instrument. It measures whether a unit meets a standard, not whether it exceeds its peers. It produces no ranking, triggers no resource reallocation, and generates no institutional requirement to identify or proliferate what the highest-performing units are doing differently. A unit that barely clears the bar receives the same resources as one that shatters it.

This egalitarian approach has institutional logic. It maintains force-wide readiness across diverse scenarios and prevents inter-unit competition that could be more destructive. But it does not produce an inherently evolving ecosystem, nor does it reinforce evolution when it does occur.

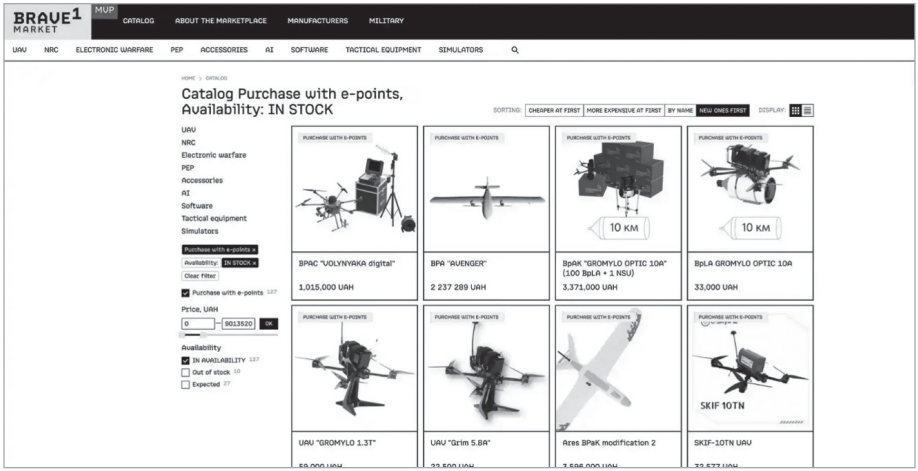
None of this is an indictment of the systems USSOCOM has built. The acquisition model fields technology faster than any comparable defense organization. The skills competitions reinforce the warrior

culture. GFM and POM allocate forces and funding through rigorous, proven processes that keep SOF responsive to global demand. These systems do what they were designed to do. However, none of them were designed to answer a specific question: Among units performing comparable missions, who is doing it best, and how does USSOCOM ensure the rest of the force learns from them? That is the gap. And other nations, under the pressure of real war, are already attempting to fill it.

The New Incentive Models

Ukraine: Equip the Unit

Ukraine's Army of Drones: Bonus system (also known as ePoints) is the first national-scale implementation of gamified, performance-based military resourcing in an active conflict. Launched by the Ministry of Digital Transformation in August 2024, the program rewards military units with points for verified destruction or damage of enemy targets using drones.[15] Units submit strike footage,



Brave1 Marketplace ("Amazon for drones"), where units exchange their points for equipment. Source: https://brave1.gov.ua/en

undergo verification, and accumulate points that they can spend on real equipment, including FPV drones, bombers, reconnaissance unmanned aerial vehicles (UAVs), and electronic warfare systems. Ukraine's Minister of Digital Transformation Mykhailo Fedorov has called it simply "the mathematics of war."[16]

The results have been transformational. In 2025, units operating within the ePoints system recorded 819,737 video-confirmed strikes, including 240,000 Russian personnel killed or critically wounded, 29,000 heavy vehicles destroyed, 62,000 light vehicles struck, and 32,000 enemy drones shot down.[17] December 2025 alone saw 106,859 confirmed strikes, a 31 percent increase over November, acceleration within an already accelerating system.[18] This increase in strikes and effectiveness is at least partially due to the system's feedback loop. Units that produce more verified results receive more equipment, which enables more strikes, which generates more points. For truly exceptional units, the effects are extreme. In 2025, the 414th Brigade—"Birds of Magyar"—logged 18,297 confirmed hits on Russian personnel, 124 on tanks, 319 on armored vehicles, 257 on artillery systems, and 4,058 on drones.[19] And this is not isolated. Other elite units (SBU Alpha, Lazarus Group, Achilles, NEMESIS) bear similar tallies.[20] The magnitude of this impact is only possible because successful units have been given the tools needed to scale their successes.

But the system does not merely reward unit performance; it provides a mechanism to incentivize immediate adaptation from the force based on strategic objectives. When the Ukrainian General Staff wants deeper strikes to disrupt Russian logistics, it adjusts point coefficients to reward longer-range engagements. When goals shift to degrading Russian drone capabilities, points are adjusted to favor targeting Russian drone operators and production capabilities. Used in this way, Ukraine's incentive structure is a tool for rapidly

translating strategy into tactical behavior without additional guidance or interpretation through echelons.

From an acquisitions perspective, there are also other benefits. Ukraine produced an estimated 4–5 million drones in 2025 and has set a target of 7 million for 2026.[21] The ePoints system is the demand signal that shapes which drones get built, which units receive them, and what those units prioritize when they fly. It provides recurrent feedback on what technology is operationally working, what is needed, and where.

Ukraine is in an existential conflict where survival demands rapid optimization to dynamic conditions. The incentive systems Ukraine built emerged out of wartime necessity. The United States, though engaged in combat operations, does not face the same extreme conditions or consequences. However, to ignore the lessons of the Russo–Ukraine War would be a great mistake. Whether conflict grows or emerges to demand it, incentive systems must be both mature and reactive enough to generate rapid adaptation when it is needed most.

Russia: Pay the Soldier and Centralize Excellence

Russia's response to the same battlefield pressure has taken a different but equally instructive form. Where Ukraine rewards units with equipment, Russia rewards individual operators with cash—25,000 rubles (approximately $330) per confirmed FPV strike on enemy personnel.[22] The incentive targets the individual, not the formation.

But Russia's more consequential approach is institutional, not financial. In August 2024, Defense Minister Andrei Belousov ordered the creation of the Rubikon Center for Advanced Unmanned Technologies, a hybrid organization that combines drone development, operator training, tactical testing, and frontline



Russian Defense Minister Andrei Belousov during a presentation by the Rubikon Center for Advanced Unmanned Technologies. (Photo credit: mil.ru)

combat into a single integrated unit with an embedded feedback loop.[23] By spring 2025, Rubikon had seven detachments of 130–150 personnel each; by November, the organization had grown to approximately 5,000.[24]

Russia also formally established an entire Unmanned Systems Forces (USF) branch, with Rubikon as its premier unit and an initial strength of approximately 87,000 personnel, with plans to reach over 200,000 by 2030.[25] Russia is not taking Ukraine's approach to allowing excellence to emerge organically; they are consolidating their most competent and elite operators into a unit that they hope

> ***A competitive resourcing model that does not structurally mandate diffusion will fracture the force it is meant to strengthen.***

will be far more exceptional. That unit is dual mandated with training and operations and well-resourced to support those tasks.

The Economics of Competition

What Tournament Theory Tells Us

Whether Russia or Ukraine has the superior model is unclear, and neither would integrate cleanly into the structure of USSOCOM. Yet there are attributes USSOCOM should not ignore. *Tournament theory*, a concept pioneered by economists Edward Lazear and Sherwin Rosen in 1981, provides the theoretical framework for understanding why these kinds of incentive systems work.[26] The core finding is straightforward: Competitive incentive structures based on relative performance increase effort, and the larger the spread between winning and losing prizes, the greater the effort participants invest. Empirical research across corporate, athletic, and sales environments has consistently validated this prediction.[27] It is also why the incentive in any USSOCOM competitive resourcing model must be meaningful; a trophy or unit citation will not change behavior; discretionary procurement funding and priority access to emerging platforms will. Tournament theory tells us that half-measures produce half-efforts.

But the same literature identifies the failure modes that must be designed against. The most critical is knowledge-sharing suppression: participants in tournament structures are incentivized to view others as competitors, discouraging cooperation and

encouraging information hoarding.[28] Ukraine's ePoints system does contain elements of this, but the problem is neither extreme nor catastrophic. Units that develop effective tactics may have rational incentives to withhold them from peers competing for the same limited resources, but they have a far greater incentive to defeat Russia, so knowledge is spread. It is, however, important to highlight that in any military context, unchecked knowledge suppression is not merely inefficient; it is operationally dangerous. A competitive resourcing model that does not structurally mandate diffusion will fracture the force it is meant to strengthen.

The second risk is *superstar discouragement*: competing against dominant performers actually reduces effort by other participants, a "why bother" effect where the perceived unassailability of top competitors causes others to disengage rather than strive.[29] This is what might be expected to be exemplified with Russia's model, where a single elite unit is being given the greatest accolades, resources, and responsibility, but again here, it is not so clear cut. But Rubikon's effect on the broader Russian USF suggests the superstar problem is not inevitable. Because Rubikon's mandate includes training other formations, its dominance elevates rather than discourages.

The key takeaway is performance-based resourcing works, but a system that incorporates it must be deliberately designed to prevent the negative pathologies that competitive structures can produce.

A Framework for Meritocratic Resourcing

USSOCOM needs its own framework—not Ukrainian, not Russian, and not a replacement for existing USSOCOM resourcing architecture. It needs a complementary resourcing system that spurs innovation, efficiency, effectiveness, and lethality. Such a

system must also encourage knowledge diffusion and be culturally aligned with the dominant characteristics of the special operations community. Properly built and with minimal funding, such a system could be one of its most powerful organizational investments and serve as an adaptation accelerant for readiness and relevancy on the evolving battlefield. Below is a proposed framework. Built on four pillars—High Incentive, Anti-Siloing, Anti-Stagnation, and Cultural Affinity—the objective is to establish a framework for meritocracy resourcing that could be quickly developed and executed.

Pillar One: High Incentive

The reward must be meaningful enough to change unit behavior. Tournament theory is unambiguous on this point: The larger the spread between winning and losing outcomes, the greater the effort participants invest. A trophy, a unit citation, or a mention at a SOF Week ceremony will not alter how a team trains, experiments, or prioritizes capability development. Discretionary procurement funding will. A notional figure of $1 million in additional procurement for a competitively verified top-performing O-5 command in a particular strategic area would likely be more than sufficient to acquire meaningful additional capability without distorting the overall component budget.

Pillar Two: Anti-Siloing Through Mandatory Diffusion

The diffusion mechanism for winning units must be explicit. There must not just be a thorough dissemination of tactics, techniques, and procedures but interactive interoperability opportunities for other SOF units in the same mission space. The reward is conditional on raising the floor, not just extending the ceiling. The principle is proven: When the Navy established TOPGUN in 1969 and required every graduate to return to fleet squadrons as an instructor, kill ratios against North Vietnamese MiGs climbed

from 2.5:1 to 13:1 within three years, not because the Navy produced better individual pilots, but because it built a system that turned individual excellence into institutional capability.[30]

The ethos of all SOF in the U.S. military is rooted in the belief that demonstrated performance determines merit.

Pillar Three: Anti-Stagnation Through Recurring Assessment

Competitive assessments must recur on defined cycles. Annual or biannual cycles keep the system dynamic, and the mandatory diffusion requirements of Pillar Two serve to ensure that other units have the knowledge base to compete effectively in subsequent cycles. Scenarios and conditions should change between cycles to prevent units from optimizing for a predictable event rather than for the operational problem the assessment is meant to represent. Assessment criteria must be composite and public—spanning TTPs, technology, and demonstrated mission impact—and evaluated by external joint assessment teams in a common competition environment.

Pillar Four: Cultural Affinity

SOF culture is built on competition: selection, qualification, advancement. The ethos of all SOF in the U.S. military is rooted in the belief that demonstrated performance determines merit. A meritocratic resourcing system extends that value into a domain where it has been conspicuously absent. Asking SOF units to compete for capability development resources aligns with the foundational belief that the best should lead, and everyone should strive to be the best. The only thing novel about this proposal is that

it attaches resources to the outcome and requires the winners to disseminate the basis of their advantage.

Application: SOF Deep Strike Against A2/AD Targets

Consider the problem of land-based deep strike against critical anti-access/area denial (A2/AD) targets. Virtually all SOF elements share the mission of infiltrating denied or contested environments to locate, target, and destroy the air defense nodes, radar installations, command-and-control facilities, and missile systems that prevent joint force access to a theater. Every component is developing some version of this capability. But we are institutionally blind to who is doing it best.

Under current models, each component develops its approach to this problem independently. SITREPs may highlight the development of innovative tactics, but a SITREP is not a mechanism to disseminate training, tactics, or procedures (TTP) or to compare effectiveness. Some approaches will be superior to others. Under the current system, there are few direct incentives to push beyond the baseline or to adopt practices from other units, if they are known at all.

Under the proposed framework, USSOCOM would designate land-based deep strike against A2/AD targets as a competitive capability area and develop a lane or exercise to compete units. The assessment is conducted by an external joint evaluation team. Finally, the top-performing unit is selected objectively, with their O-5 command receiving discretionary procurement funding (here recommended as $1 million), priority access to emerging USSOCOM platforms, and the institutional recognition that its approach represents the current standard of excellence. In return, that unit hosts training detachment rotations from other components and publishes its TTPs.

In the next assessment cycle, every unit in the competition has had access to the previous winner's methods, incorporated what works, and improved the rest. The playing field is re-leveled, and the competitive cycle recurs. The entire force has elevated its collective capability against the A2/AD problem while the competitive pressure continues to push the ceiling higher. USSOCOM, for the first time, possesses verified, comparative data on which approaches to this critical mission actually work. That data informs not only training and resource allocation but also acquisition priorities, exercise design, and operational planning.

The cost of this system is marginal. The institutional learning it produces is not.

Risks and Necessary Safeguards

Any proposal that links resources to competitive outcomes must be honest about what can go wrong. The risks are real, documented, and predictable—which means they can be designed against.

The most insidious risk is that units begin training to win the competition rather than training to win the fight. If the assessment becomes a predictable event with known criteria, units will optimize for the evaluated exercise rather than for the operational problem the exercise is meant to represent. The mitigation is assessment design: Criteria must be composite rather than single-metric, scenarios must change between cycles to prevent rehearsal, and evaluators must retain the discretion to weigh innovation and adaptability alongside measurable performance. The assessment must feel like a mission, not a test.

The objection most likely to be raised is that competitive resourcing will demoralize units and create destructive friction between component commands. But SOF culture already absorbs

> ***If the assessment becomes a predictable event with known criteria, units will optimize for the evaluated exercise rather than for the operational problem the exercise is meant to represent.***

competitive outcomes at scale without such severe outcomes. Those elements of negativity that do develop are likely to be small in population and impact, especially compared to the positive effect such a system promises. Ultimately, any major incentive system must be mandated at the USSOCOM level with sufficient endorsement to survive any potential component-level friction. The results must be framed as enterprise learning opportunities rather than command report cards.

Another concern is that over time, any competitive system risks becoming a compliance exercise that generates paperwork rather than innovation. The assessment cycle could become routine. The diffusion requirement could be seen as a checked box rather than genuine knowledge transfer. The best safeguard is simplicity: keep the assessment operationally focused, keep the reward meaningful enough that units genuinely want it, keep the diffusion requirement tied to real interactions and meaningful documentation.

Last, competitive resourcing cannot compromise mission-essential allocations. Some lower-priority sourcings will go unfunded to resource this system; that is an intentional trade. But at such a low price point, it would not come from core capabilities that units need for assigned missions. The $10 million competitive pool represents less than 0.1 percent of the USSOCOM annual operations and maintenance budget. Kept at this scale, the constraint is a condition of programmatic effectiveness and political will, not fiscal capacity.

None of these risks are novel. All of them are manageable. The greater risk is continuing to resource SOF units without any mechanism to identify, reward, or proliferate what the best of them are doing differently.

Compete for the Future Force

The U.S. special operations enterprise is the most capable irregular and special warfare force in the world. It possesses a deep cultural affinity for competition, an organizational architecture that embodies meritocratic principles at the individual level, and an acquisition system that fields technology faster than any comparable defense organization. What it lacks is a mechanism to answer the question that matters most for the fights ahead: Among the units performing our hardest missions, who is doing it best, and how does the rest of the force learn from them?

The framework proposed here is not a radical reimagining of the USSOCOM resourcing architecture. It is a competitive overlay targeted at defined capability areas; its simple, affordable, and aligned with everything SOF already believes about the relationship between competition and excellence. The only thing it adds is consequences for the outcome and a requirement to share what winning looks like. That is not a cultural departure for special operations. It is a cultural completion.

About the Author

Cmdr. Jordan Spector is an active-duty officer with advanced degrees from the Naval Postgraduate School and Johns Hopkins University School of Advanced International Studies. He has completed multiple deployments to Africa, the Middle East, Europe, and the Indo-Pacific.

Notes

1. Paul Adams, "Kill Russian Soldiers, Win points: Is Ukraine's New Drone Scheme Gamifying War?" *BBC*, July 18, 2025, https://www.bbc.com/news/articles/c80p9k1r1dlo.
2. Liubava Petriv, "Ukraine's Army of Drones Hit 820,000 Russian Targets in 2025, Defense Minister Says," *UNITED24 Media*, January 26, 2026.
3. "Russian Military Pay Bonuses for FPV Drone Strikes on Ukrainian Troops — Voloshyn," *Ukrinform*, February 24, 2025, https://www.ukrinform.net/rubric-ato/4095007-russian-military-pay-bonuses-for-fpv-drone-strikes-on-ukrainian-troops-voloshyn.html.
4. "Fiscal Year 2026 Budget Estimates, United States Special Operations Command, Operation and Maintenance," Office of the Under Secretary of Defense (Comptroller). Available at comptroller.war.gov.
5. GAO-07-620, "Defense Acquisitions: An Analysis of the Special Operations Command's Management of Weapon System Programs," Government Accountability Office, 2007.
6. GAO-07-620, "Defense Acquisitions."
7. SOFWERX, "CPO 68: OSD CUAS Test Event Phase II," April 1, 2024, https://swx-project-prod.s3.amazonaws.com/CPO_68_OSD_CUAS_Test_Event_Phase_II_FINAL_20240401.pdf.
8. SOFWERX, "USSOCOM Innovation Foundry (IF-16) Event," https://events.sofwerx.org/ussocom-innovation-foundry-if-16-event.
9. SOFWERX, "Hardware Enabled AI Acceleration," https://events.sofwerx.org/hardware-enabled-ai-acceleration.
10. SOFWERX, "Next Generation Maritime Optical Systems," https://events.sofwerx.org/next-generation-maritime-optical-systems.
11. Melissa Johnson, SOF AT&L Keynote, SOF Week 2025, Tampa, FL. Reported in "SOCOM: The Speedboat the Services Built," *Defense Acquisition* (Substack), February 2026.
12. "USASOC International Best Sniper Competition: 75th Rangers 'Lead the Way' by Securing First Place," U.S. Army, March 27, 2025.
13. "10th Special Forces Group Takes First as Best Combat Divers Across Special Operations Forces," U.S. Army, June 13, 2024.
14. Lt. Col. Vonnie Wright, "Army Announces Winners of Inaugural Best Drone Warfighter Competition," U.S. Army, February 20, 2026, https://www.army.mil/article/290645.
15. "Inside Ukraine's Drone War," *New York Times*, October 31, 2025, https://www.nytimes.com/2025/10/31/world/europe/ukraine-war-drone-game.html.
16. Adams, "Kill Russian Soldiers, Win Points."
17. Rudy Ruitenberg, "Ukraine Says More Than 80% of Enemy Targets Now Destroyed by Drones," *Yahoo! News*, January 28, 2026.
18. Illia Kabachynskyi, "Ukraine's Drone Strikes Hit Up to 100,000 Russian Troops in Late 2025—2026 Plans Aim Higher," *UNITED24 Media*, January 6, 2026.

19. Stefan Korshak, "Ukraine Drone Troops Claim Big Russian Kill Scores, Announce Expansion Plans for 2026," Kyiv Post, January 28, 2026.

20. Liubava Petriv, "Ukraine's Army of Drones Hit 820,000 Russian Targets in 2025, Defense Minister Says," *UNITED24 Media*, January 26, 2026.

21. Clara Kaluderovic, "The Coming Compute War in Ukraine," *Atlantic Council*, https://www.atlanticcouncil.org/content-series/the-big-story/the-coming-compute-war-in-ukraine/.

22. Vladyslav Voloshyn, Spokesperson for the Southern Defense Forces of Ukraine, Interview with *Ukrinform*, February 24, 2025. Reported in "Russian Military Units Receive Financial Rewards for Targeting Ukrainian Forces With FPV Drones," *UNITED24 Media*, February 2025.

23. "Drone Centre Rubikon — The proof of the Russian army's adaptability," Adapt Institute, September 16, 2025.

24. "Crossing the Rubicon: Russia's Elite Drone Force and the Evolution of Unmanned Warfare in Ukraine," Saratoga Foundation, February 5, 2026.

25. "Unmanned Systems Forces (Russia)," various sources. USF formally established November 12, 2025. 87,000 personnel reported February 2026; 210,000 target by 2030 per Ukrainian Commander-in-Chief Syrskyi.

26. Edward Lazear and Sherwin Rosen, "Rank-Order Tournaments as Optimum Labor Contracts," *Journal of Political Economy* 89, no. 5 (1981): 841–864.

27. Brian L. Connelly et al., "Tournament Theory: Thirty Years of Contests and Competitions," *Journal of Management* 40, no. 1 (2014): 16–47.

28. Connelly, "Tournament Theory."

29. Jennifer Brown, "Quitters Never Win: The (Adverse) Incentive Effects of Competing with Superstars," *Journal of Political Economy* 119, no. 5 (2011): 982–1013.

30. Christopher Papaioanu, "TOPGUN's Impact," *Proceedings*, U.S. Naval Institute, September 2019.

A New Approach to Risk That Supports Rapid Decision-Making

By Lt. Col. Michael C. Tinker

> "There are risks and costs to action. But they are far less than the long-range risks of comfortable inaction."
>
> —John F. Kennedy

Introduction

Rapid advancements of new technologies like AI, unmanned systems, and expeditionary advanced manufacturing have accelerated the rate of change on the battlefield, making deliberate military decisioning too slow. As such, military leaders, focused on maintaining information dominance, are championing the use of advanced data tools to extend decision space. The preponderance of efforts for this initiative has been sourcing, securing, and displaying military related data, most often taking the form of a common operational picture (COP). While having access to near real-time battlefield data is important, the most critical element to achieving decision advantage is a global understanding of risks. Specifically, decision makers must have the ability to weigh current investment risks against potential opportunities for return.

Even though the current joint force risk framework provides guidance on identifying, managing, and reducing risks, a revised risk methodology that reflects a business approach where decision makers focus on utilizing risks to maximize opportunities is necessary. Within commercial environments, understanding current positioning in the market and related next steps are critical to generating profits. Similarly, military leaders need to be able to look beyond mere reduction of bad outcomes to "see" the organization unfiltered in the operating environment.

Although this ambitious effort is applicable to the joint force, U.S. Special Operations Command (USSOCOM) should take on this initiative. This is because the special operations forces (SOF) enterprise is uniquely positioned to lead in this space given its distinct authorities, funding, talent, and influence. Not only is SOF

leadership proactively seeking novel technological solutions, but the enterprise already has an established data modernization program, a decision support tool in development, as well as access to necessary development platforms.

To accomplish this, USSOCOM should consider implementing two key strategies. First, and most critically, it should establish a modernized risk methodology aimed at supporting rapid decision-making. Utilizing industry best practices, this new risk framework should address concepts such as inherited (current) risks and controls, global composite risk estimates, and risk–benefit analysis. Additionally, USSOCOM should update existing risk definitions, categories, and subcategories aligned to strategic values. By adopting a modernized approach to risk, the SOF enterprise maximizes opportunities for strategic gains and mitigates potential vulnerabilities. Second, the enterprise should develop a continuous risk assessment tool known as the common risk picture. Beyond just an improved COP, the common risk picture will be an AI-assisted risk assessment tool used *in conjunction* with existing visualization applications. This new software solution should be integrated with existing intelligence, planning, and reporting systems, distilling nominal data into risk assessments that support rapid decisioning. A successful common risk picture delivers near real-time risk information in echelon that enhances situational awareness and decision-making speed.

While having access to near real-time battlefield data is important, the most critical element to achieving decision advantage is a global understanding of risks.

A Modernized Risk Framework

The joint force's current risk manual, entitled the Joint Risk Analysis Methodology (JRAM), provides a rigorous framework for assessing risk in planning and operations.[1] The document uses well-established practices to predict risks associated with uncertain futures. Though this approach is effective for deliberate planning, it reduces risk to something that must be managed, reduced, or avoided altogether. This can lead to risk avoidance, indecision, and precautionary leadership, limiting leaders' ability to make effective decisions. Moreover, current assessment frameworks produce static estimates of specific operations, typically on an annual basis, and can lag months behind current events resulting in outdated snapshots that do not reflect the dynamic nature of the operating environment.[2] However, future battlefields demand accurate and near real-time risk analysis. Even though the JRAM should still be used as a foundation, quickly distilling data into actionable risk insights requires a new methodology.

Future battlefields demand accurate and near real-time risk analysis.

Capture Knowable Unknowns. A modern risk framework should provide specific guidance on measuring the impact of knowable information that is unreported. Knowable but missing data is critical to understanding planning risks. Not only does unknown information drive uncertainty in risk estimates, it also should be considered a planning assumption and likely a commander's critical information requirement (CCIR). Knowable but unreported data should drive intelligence gathering priorities because any gap in friendly or adversary awareness is a friendly force information requirement (FFIR) or priority intelligence requirement (PIR), respectively. Operationally, friendly force actions act as investments

To maintain oversight in a future where AI dominates decision cycles, measuring unknowns will not be a luxury but a requirement.

and adversarial impacts are threats. Likewise, friendly vulnerabilities and adversary strengths further offset their respective impacts and can be estimated using the diplomatic, informational, military, and economic framework.[3] Although this effort will require significant workflow changes, to maintain oversight in a future where AI dominates decision cycles, measuring unknowns will not be a luxury, but a requirement.

Consider Positive *and* Negative Risks. The 2026 National Defense Strategy Line of Effort #4 directs the Department of War (DoW) to supercharge the defense industrial base.[4] Thus, organizations like the Economic Defense Unit are rapidly increasing capital investments in defense-related projects.[5] Furthermore, multinational corporations continue to invest in emerging markets for critical minerals and energy that require regional stability and security. This creates a dynamic where the joint force is essentially functioning as a global risk management organization for the U.S. Government's economic interests. The current risk methodology defines risk as the probability and consequence of an event causing harm to something of value, conventionally represented by the following mathematical relationship: *Risk = Probability x Consequence*. Figure 1 contains a graph depicting this relationship.

This traditional relationship, however, predicates only negative futures. Risk encompasses more than just bad outcomes. To maximize opportunities for impact, the new risk methodology should include measures for both positive and negative outcomes. Looking to industry, the International Organization for Standardization

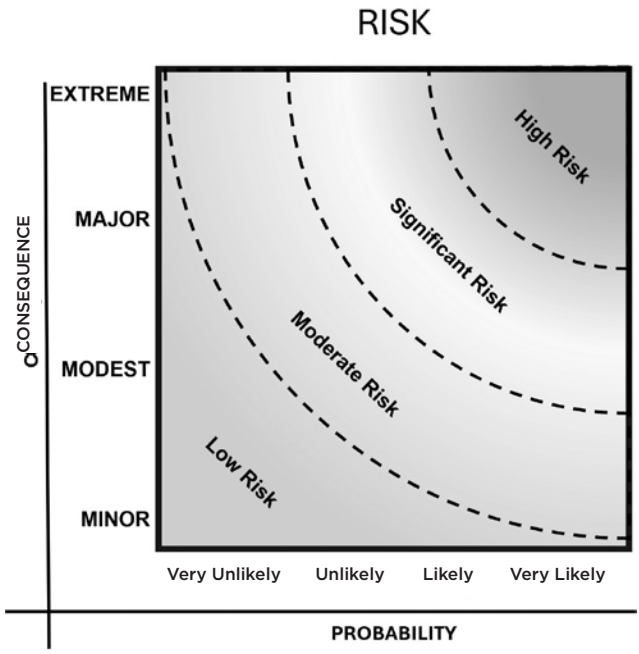


Figure 1. Joint risk analysis methodology. Source: Chairman of the Joint Chiefs of Staff manual 3105.01B, *Joint Risk Analysis Methodology* (Joint Chiefs of Staff, December 22, 2023)

(ISO) Risk Vocabulary Manual, ISO 31073, defines risk as "the effect of uncertainty on objectives, specifically, the deviation from the expected which can be positive, negative, or both."[6] Moreover, industry typically expresses risk in terms of sources, potential events, consequences, and likelihood of occurrence. To help visualize this relationship, Dr. James Kallman and Mr. John Bugalla developed the "Value Map" concept, which graphically depicts both positive and negative outcomes of risk on a single continuum.[7] Based on the Value Map concept and existing JRAM framework, the USSOCOM definition of future risk should be the probability of a future event occurring, along with the acceptability for both negative *and* positive military outcomes. Graphically, this approach maintains the existing measures of outcome probability while expanding the

Risk encompasses more than just bad outcomes. To maximize opportunities for impact, the new risk methodology should include measures for both positive and negative outcomes.

consequence component to include both positive and negative outcomes, with measures ranging from Ideal to Catastrophic. This allows for the differentiation between opportunities (positive outcomes) and threats (negative outcomes). The new mathematical relationship for forecasting risk is the difference between projected positive and negative outcomes is *Risk Forecast = [Probability x Positive Outcome] – [Probability x Negative Outcome]*. This formula is represented graphically in Figure 2.

Understand Current and Future Risks. A common complaint from senior military leaders is the inability to "see" the current state of our forces accurately. This is because a precise understanding of forces aligned against global investments is crucial for actionable decision support. To know where to go next, one must first know where they are currently. Yet the JRAM methodology only focuses on possible future events. Forecasting future events alone is not adequate to assist in decision-making, as it mainly highlights actions to avoid and does not offer a complete picture of current investments. Like assessing negative and positive outcomes, a new risk framework should also expand the temporal dimensionality of risk to include future *and* current states. Moreover, identifying risks to current operations supports the development of indicators related to progress, thereby adding rigor to evaluations. Additionally, it supports the estimation of information certainty, acknowledging unknown information.

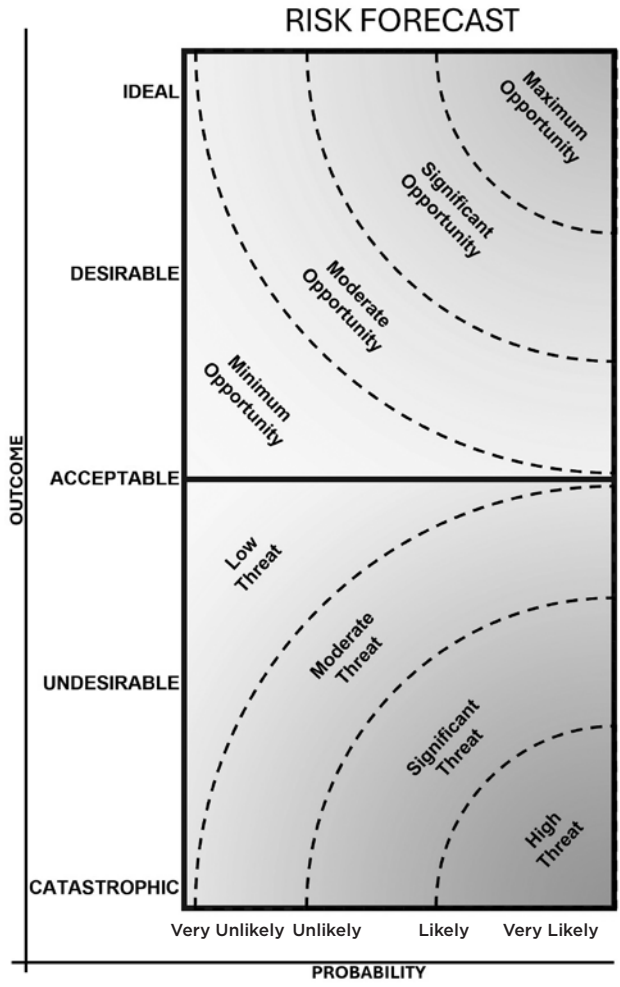


Figure 2. Risk forecast. Source: Author

This mirrors the business world's approach to risk, where decision makers focus on leveraging current drivers of risk to capitalize on future opportunities.[8] Business leaders seek information that compares current investments against possible future returns to maximize the potential for gain. In strategic terms, they gauge how far away their organization is from achieving its stated mission, enabling the determination of future objectives

based on an understanding of their current ability to leverage the market. Conceptually, current risk is similar to what industry calls inherited risk. In a military context, the status of the current operating environment is analogous to inherited risk without any controls. Any friendly investments in the operating environment act as risk controls. However, to measure how far away we are from optimized outcomes as part of the national security apparatus, the organization must clearly define mission goals that emphasize measures of progress. This allows for a comparative analysis of current impacts on both friendly and adversary forces, revealing an estimate of the net effect on the operating environment. Although this method does not link direct causation of action to changes in the operating environment, an estimated correlation can provide increased decision clarity in a chaotic environment.

USSOCOM should also strive to measure current investments in the operating environment relative to the impacts from friendly and adversary forces over time. Combining these techniques, commanders can compare threats against investments in real-time to make effective decisions. To estimate the level of current investment, we must convert the scale of probability of a future event occurring to the certainty of current information. In practice, USSOCOM should adopt existing ordinal measures of future risk to include current risk, ranging from certain to uncertain, with the y-axis scale representing both positive and negative outcomes from ideal to catastrophic. Mathematically, this relationship is like the risk forecast above, but with an additional term to account for the state of the operating environment. The graph depicted in Figure 3 visualizes the following formula: *Current Risk = [Information Certainty x Friendly Force Impact] - [Information Certainty x Adversary Force Impact] – [Information Certainty x Operating Environment]*.

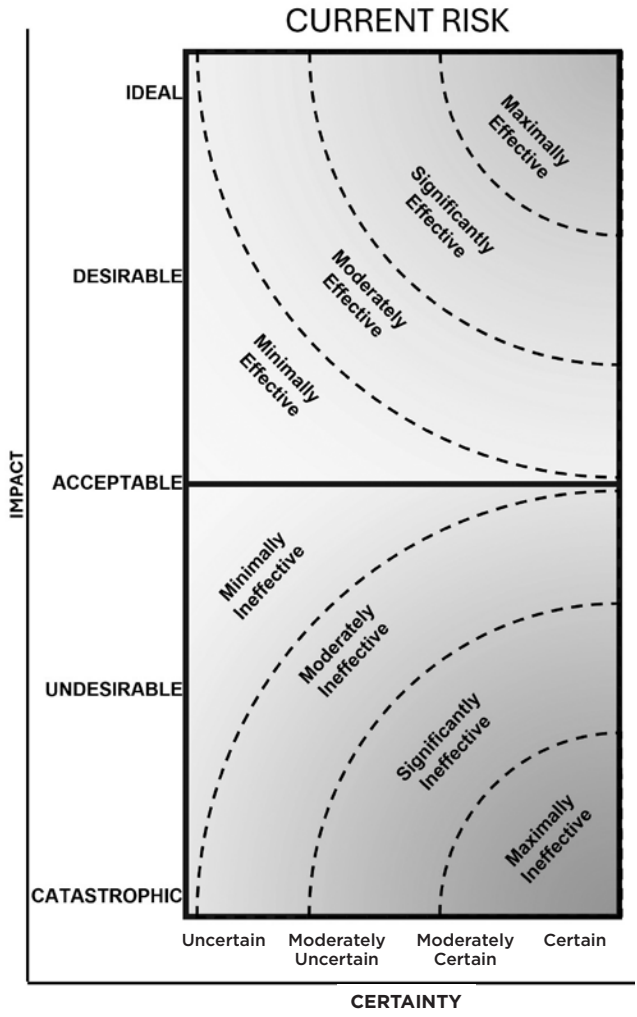


Figure 3. Current risk. Source: Author

Realign the Risk Categories. The JRAM organizes risks into two types: strategic military risk and military risk, which has its own unique categories called Risk to Mission and Risk to Force. These categories each have their own subcategories of operational, future, force management, and institutional risks, each identified by related time horizons.[9] Although categorizing risks into groups is essential

in identifying driving factors that facilitate a global risk rating, the JRAM categories are misaligned for continual enterprise risk assessment. Moreover, linking time horizons to risk subcategories prevent a composite measure of global risk.

Incorporating concepts from industry frameworks can enhance the joint force risk methodology. For instance, most corporate banking industry risk programs encompass categories aligned directly to the value they bring to their customers/shareholders, such as credit, operational, market, liquidity, strategic, compliance, and reputational risks. By combining risk measures from these categories, bank executives obtain an overall global risk rating that informs rapid decision-making in response to daily market adjustments. USSOCOM could utilize a similar approach by developing risk categories directly aligned with strategic military values.

Retired Col. Arthur Lykke's ubiquitous "legs" of military strategy (ends, ways, and means) can be used to assess military strategic risk values.[10] The underlying basis for Lykke's approach is that all three legs must be present for a complete military strategy. When applying this to an enterprise risk methodology, three topline categories emerge with individual subcategories and measures arranged in such a way that their combined values represent a global risk picture.

a. Ends = Mission Risk. Lykke defines *ends* as "objectives toward which one strives" or more simply, "military objectives."[11] Ends are military value propositions such as global security, power projection, or regional stability which is ultimately related to achieving an end state or a continuous steady state. In business terms, ends would represent the product produced, service provided, or return on investment (ROI). Although the JRAM's "Risk to Mission" category is related to the ends concept, it does not completely align.

Conversely, the concept of Mission Risk more precisely reflects the difference between the estimated current state of military objectives and the desired future outcome.

Though ROI is relatively straightforward to measure quantitatively in the business world, estimates of something related to ROI for military objectives are mostly qualitative judgements. As an alternative, USSOCOM could attempt to measure any incomplete portion of a planned military objective as a key tactical problem and a Mission Risk. If those objectives have indicators of progress, assessors could use a standards-based assessment to develop something representing quantitative measures.[12] In a standards-based assessment, end states are arranged into conditional bins, covering numerous progress states ranging from goal condition to the worst possible state. This allows evaluators to estimate the difference between the current state of the operating environment and the desired outcome.

Critically, this approach requires the planners to clearly define desired outcomes with measures of progress. As such, if the parameters of an objective are not measurable, either directly or through progress states, it should be redefined. Using the typical operations assessment focuses, the suggested subcategories for Mission Risk at all echelons are Performance (planned actions vs. completed actions) and Effectiveness (actions taken vs. desired outcomes). USSOCOM could also create additional subcategories for Mission Risk specifically based on its Title 10 Authorities and Responsibilities.[13]

b. Ways = Operational Risk. Lykke describes *ways* as "courses of action" or "methods of applying military force."[14] The concept of ways requires an organization to understand how they plan to execute, while identifying potential barriers or gaps that could prevent them from succeeding. This is similar

Fully understanding how readiness compares against the capabilities of an adversarial force in an operating environment provides clarity in military decision-making.

to corporate banking "Operational Risk" programs where key information about the organization's ability to act on their goals is carefully and continuously reported. Like the business world, fully understanding how readiness compares against the capabilities of an adversarial force in an operating environment provides clarity in military decision-making. However, corporate Operational Risk programs also consider policy, regulatory, and reputational risks. Likewise, we should include measures related to government and civilian oversight.

USSOCOM should introduce the concept of Operational Risk as a new standalone risk category to measure enterprise alignment to the mission. Conveniently, elements of the doctrine, organization, training, materiel, leadership/education, personnel, facilities, and policy (DOTMLPF-P) framework can be used as a basis for Operational Risk subcategories.[15] Measures for these subcategories include doctrine (the portion of plan aligned with existing doctrine), organization (portion of enterprise aligned to the mission), training (the portion of formation assigned to the mission who are trained and proficient), leadership/education (portion of formation with required professional development completed), and policy (objectives aligned with policy vs. total objectives planned). Apart from the DOTMLPF-P framework, additional subcategories include command and control (time of issued order vs. time of response), plans (plans required vs. plans complete), intelligence (objectives based on assumptions vs. objectives planned), readiness (available forces vs. required forces), and, if applicable, burden sharing/ interoperability (partner objectives vs. required objectives).

c. Means = Resource Risk. Lastly, Lykke defines *means* as "military resources (manpower, materiel, money, forces, logistics, etc.) required to accomplish the mission."[16] Resource Risk should replace the JRAM's "Risk to Force," expanding the scope to enable the enterprise to account for consumption of resources during operations. Like Operational Risk, elements from the DOTMLPF-P framework can be used as Resource Risk subcategories, most importantly, personnel. Suggested subcategories include materiel (amount of equipment, systems, and supplies on hand vs. amount required), personnel (manpower currently aligned to mission vs. manpower required), and facilities (fully operational facilities vs. required facilities). Additionally, and critical to rapid decision-making, USSOCOM should also include subcategories for time, as a finite resource directly connected to decision space (execution time vs. suspense), and funding (budgeted vs. required).

The subcategories and related measures for the Mission Risk, Operational Risk, and Resource Risk categories should be customizable by command echelon and type. While there will be several standardized subcategories common to all levels of command, each organization must include unique risk subcategories specific to their mission. For example, due to vastly different missions, component command risks will vary from combatant command risks greatly. Likewise, since authorities and objectives are hierarchical, risk measures from a subordinate command should be included by the next higher command. This approach allows values of the above subcategories to be linked directly to CCIRs. Specifically, significant changes to the risk estimate of friendly forces will be a FFIR. Likewise, any change in adversarial force capability is a PIR. Since a commander should be aware of any delay in critical risk information, reporting latency or information that is past relevancy presents additional uncertainty and warrants a CCIR on its own. For all subcategories of risk, reporting latency (time of

event vs. time to report) increases information uncertainty of each measure. The updated categories are represented in the Global Enterprise risk graph featured in Figure 4.

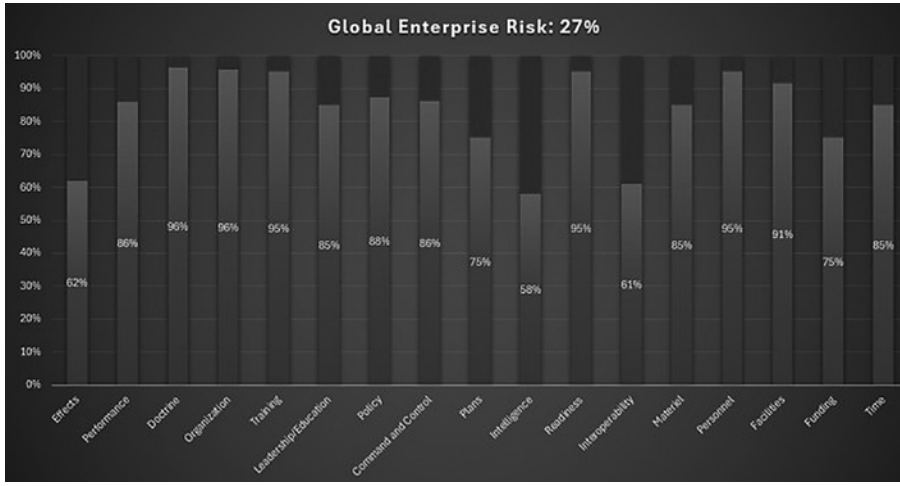


Figure 4. Global enterprise risk. Estimated subcategory status ratings are represented in blue. Outstanding objectives are represented in red and are risk drivers. Global enterprise risk is a weighted average of all subcategory risk drivers. Source: Author

Assess at the Speed of War

The rapid advancement of technology is creating a problem for military decision-making. The development of novel drone technology in Ukraine is estimated to be a mere six weeks from inception to obsolescence, much faster than traditional planning and assessment cycles.[17] Our traditional decision-making processes are inadequate for this pace of change. To maintain decision dominance, leaders are demanding more capable COP.[18] Despite continued investments from the DoW in initiatives like Next Generation Command and Control and Combined Joint All-Domain Command and Control, the most advanced COP tools will merely serve to validate disposition of forces.[19] Although a modern COP tool can provide near real-time representation of the operational

environment, without analysis the sheer amount of raw data displayed often overwhelms leaders, ultimately failing to drive decisions (see Fig. 5). Despite massive increases in information flow, leaders still require timely operational assessments to make informed decisions, but current assessment approaches result in risk assessments that are outdated upon publication and therefore do not reflect true dynamics of the modern battlefield.[20]

To close this gap and achieve decision dominance, USSOCOM should develop a continuous AI-assisted risk assessment tool known as the common risk picture. The common risk picture should be developed with the new risk management framework and fully integrated with existing COP tools. The collective joint force and interagency already possesses sensors, reporting data, and AI support tools to create a functioning common risk picture. Example data sources include mission planning documents, intelligence updates, unit readiness products, budget information, logistics materials, legal reviews, etc.

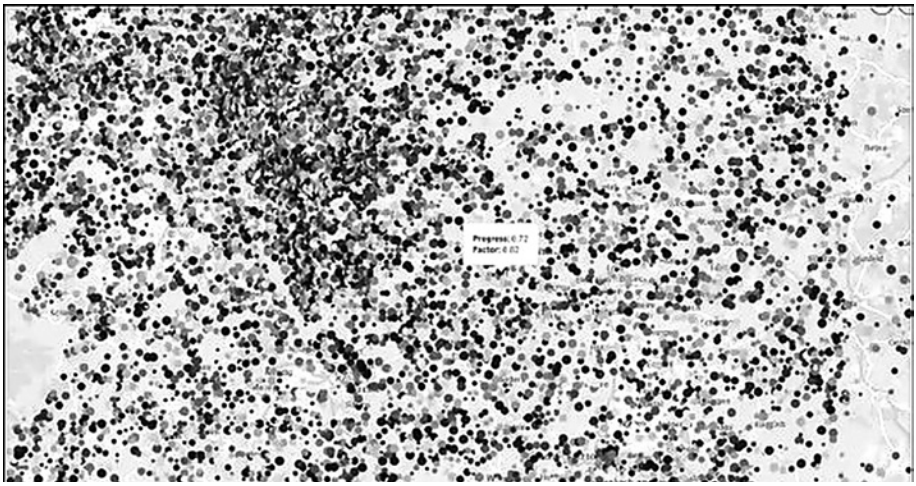


Figure 5. Example of common operational picture information overload. Source: Qlik Community, accessed March 26, 2026, https://community.qlik.com/t5/Visualization-and-Usability/Qlik-Sense-Map-is-Currently-Showing-Limited-Data-Set/td-p/1134461

The common risk picture would aggregate this data into a global risk management network, creating a customizable tool that allows each command echelon to view risk estimates.

The common risk picture would aggregate this data into a global risk management network, creating a customizable tool that allows each command echelon to view risk estimates. Combining this information with automated planning software tools can enable full integration of risk assessments across the hierarchy of military plans. Risk measures at each level would aggregate up to the next higher command, creating a comprehensive view of risk across the SOF enterprise and beyond. An AI-powered retrieval augmented generation trained on the vast catalogue of military history, lessons learned, and operations summaries could rapidly analyze data to highlight potential risks and advise mitigation strategies.

Critically, the common risk picture must display a measure of reporting latency, as a stand-alone risk metric and critical metric of information uncertainty. Moreover, the tool should link information latency directly to CCIRs, treating any delay in critical information as a risk driver. Although reporting from the battlefield will never be "real-time," the enterprise should strive to reduce lag time as much as possible. The common risk picture highlights the relationship between time and information uncertainty, or how much time is decision space available versus how much valid information is on hand. This results in a composite global risk projection, as seen in Figure 6, based on the following risk–benefit ratio formula: *Risk Benefit Ratio = Projected Benefit / Projected Risk, ratio > 1 indicates positive outcome.* This method compares historic effects, current risks, and possible future opportunities across time, and is viewable at tactical, operational, or strategic levels.

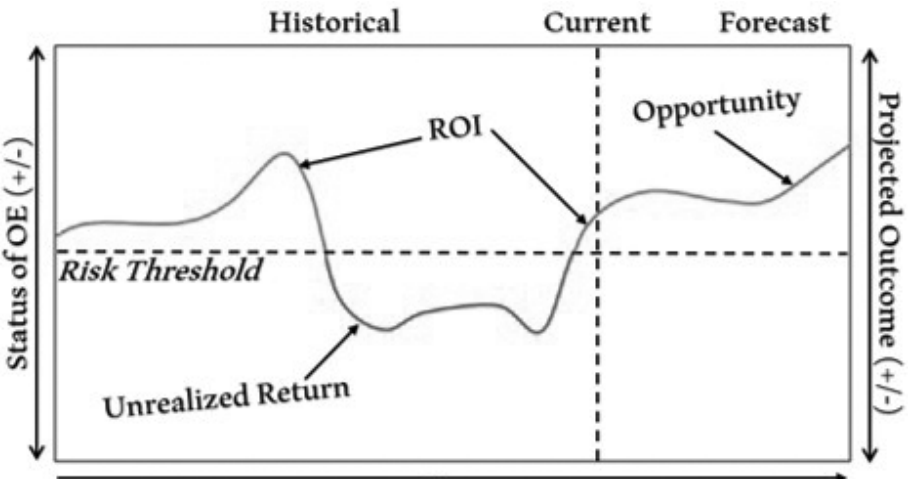


Figure 6. Common risk picture, composite global risk projection.
Source: Author

Next Steps: Establishing a new risk framework and common risk picture requires significant effort but is essential for maintaining decision dominance in the modern battlefield. USSOCOM should consider undertaking the following initiatives to advance this concept:

a. *Standardize Risk Training.* Develop a comprehensive risk training program across the enterprise to establish a common risk language and understanding.

b. *Integrate Risk-Specific Workflows.* Implement risk-related workflows where members of the formation act as individual risk sensors, contributing observations into a common interface connected to the common risk picture tool.

c. *Prioritize Acquisition of Sensors.* SOF Acquisitions, Technology, & Logistics should focus on acquiring a global array of sensors that relay risk-related information to the common risk picture.

d. *Commission Research.* The Joint Special Operations University should prioritize additional research into "black swan events,"

or extremely rare but high-impact events that could lead to strategic surprises.

e. *Expand Research Collaboration.* USSOCOM should make this approach to risk available across the joint force enterprise and the broader interagency community. Applying advanced computational mathematics, dimensional analysis, and simulations to this approach may be useful in expanding global risk awareness.[21]

By undertaking these initiatives, USSOCOM will be better positioned to maintain decision dominance, adapt to an evolving operational landscape, and achieve strategic advantages on the modern battlefield.

Conclusion

To enhance and maintain decision dominance on the modern battlefield, USSOCOM should develop and implement a novel risk framework and an AI-assisted common risk picture. This allows the SOF enterprise to leverage near real-time risk assessments to capitalize on opportunities rather than just focusing on negative outcome mitigation. The adoption of a dynamic risk framework, informed by best practices from the corporate sector, enables SOF leaders to "see" the organization as it is positioned against our adversaries across the operating environment and quickly adapt to the evolving global landscape. This approach enhances the speed and accuracy of decision-making, ensuring that USSOCOM remains ahead in the global observe, orient, decide, and act loop, securing a strategic advantage now and in the future.

About the Author

Lt. Col. Michael Tinker has over 20 years of combined civilian, military, and government experience. Tinker has a BA in physics from Clemson University, conducting research in astronomy, particle physics, and material science and was distinguished as a university ambassador for the College of Engineering and Science.

The author would like to acknowledge the significant contribution of numerous anonymous peer contributors and reviewers. Without your help, this paper would not have been possible.

Notes

1. Chairman of the Joint Chiefs of Staff. *Joint Risk Analysis Methodology,* CJCSM 3105.01B (Joint Chiefs of Staff, 2023), https://keystone.ndu.edu/Portals/86/CJCSM%203105_01B_Joint%20Risk%20Analysis%20Methodology_2023DEC22.pdf.

2. Mitchell Payne, "Assessing the Modern Fight," *Military Review*, Mar.–Apr. 2023, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/March-April-2023/Modern-Fight/.

3. Chairman of the Joint Chiefs of Staff, *Guidance for Developing and Implementing Joint Concepts,* CJCSI 3010.02E (Joint Chiefs of Staff, 2016), https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/cjcsi_3010_02e.pdf?ver=2018-08-01-134826-593.

4. President Donald J. Trump, *National Defense Strategy* (Washington, DC: White House, 2026): 21, https://media.defense.gov/2026/Jan/23/2003864773/-1/-1/0/2026-NATIONAL-DEFENSE-STRATEGY.PDF.

5. Mackenzie Eaglen, "'Economic Defense Unit': How the U.S. Military Wins in the 'Gray Zone,'" *American Enterprise Institute,* August 18, 2025, https://www.aei.org/op-eds/economic-defense-unit-how-the-u-s-military-wins-in-the-gray-zone/.

6. International Organization for Standardization, *Risk Management – Vocabulary,* ISO 21073 (2022), https://www.iso.org/obp/ui/en/#iso:std:iso:31073:ed-1:v1:en.

7. James Kallman and John Bugalla, "How to Map Your Risks," *CFO.com,* February 14, 2013, https://www.cfo.com/news/how-to-map-your-risks/666458/.

8. "What Is Enterprise Risk Management?" *Oracle*, n.d., https://www.oracle.com/erp/risk-management/what-is-enterprise-risk-management/.

9. Chairman of the Joint Chiefs of Staff, *Joint Risk Assessment Methodology.*

10. Arthur F. Lykke, "Defining Military Strategy," *Military Review* 69, no. 5 (1989): 183–186.

11. Lykke, "Defining Military Strategy," *Military Review* 69, no. 5 (1989): 183–186.

12. Lynette M. B. Arnhart and Marvin L. King, "Are We There Yet? Implementing Best Practices in Assessments," *Military Review*, May–June 2018, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2018/Are-We-There-Yet-Implementing-Best-Practices-in-Assessments/.

13. "Title 10 Authorities," United States Special Operations Command, n.d., https://www.socom.mil/about/title-10-authorities.

14. Lykke, "Defining Military Strategy," *Military Review* 69, no. 5 (1989): 183–186.

15. Harrison Morgan, "Dropping DIMEs: Leveraging All Elements of National Power on the Multi-Domain Battlefield," *Modern Warfare Institute*, September 18, 2019, https://mwi.westpoint.edu/dropping-dimes-leveraging-elements-national-power-multi-domain-battlefield/.

16. Lykke, "Defining Military Strategy," *Military Review* 69, no. 5 (1989): 183–186.

17. Aosheng Pusztaszeri and Emily Harding, "Technological Evolution on The Battlefield," *Center for Strategic and International Studies*, September 16,

2025, https://www.csis.org/analysis/chapter-9-technological-evolution-battlefield.

18. Breaking Defense, "The Connected Warrior Will Have a Common Operating Picture Even When Contested," *Breaking Defense*, October 18, 2024, https://breakingdefense.com/2024/10/the-connected-warrior-will-have-a-common-operating-picture-even-when-contested/.

19. Theresa Maher, "Pentagon Surges Palantir Maven Smart System Contract Spending More than $1B," *Inside Defense*, May 22, 2025, https://insidedefense.com/insider/pentagon-surges-palantir-maven-smart-system-contract-spending-more-1b.

20. Yakov Ben-Haim, *Info-Gap Decision Theory: Decisions Under Severe Uncertainty, Second Edition* (Academic Press, 2006), https://www.sciencedirect.com/book/monograph/9780123735522/info-gap-decision-theory.

21. Fernando Hernandez, "Using Monte Carlo Simulation for Three-Dimensional Risk Assessment," (blog) *LinkedIn,* April 13, 2023, https://www.linkedin.com/pulse/using-monte-carlo-simulation-three-dimensional-risk-hernandez.

Bibliography

Arnhart, Lynette M. B. and Marvin L. King. "Are We There Yet? Implementing Best Practices in Assessments." *Military Review*, May–June 2018, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2018/Are-We-There-Yet-Implementing-Best-Practices-in-Assessments/.

Ben-Haim, Yakov. *Info-Gap Decision Theory: Decisions Under Severe Uncertainty, Second Edition.* Academic Press, 2006. https://www.sciencedirect.com/book/monograph/9780123735522/info-gap-decision-theory.

Chairman of the Joint Chiefs of Staff. *Guidance for Developing and Implementing Joint Concepts. CJCSI 3010.02E 17.* Chairman of the Joint Chiefs of Staff, 2016. https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/cjcsi_3010_02e.pdf?ver=2018-08-01-134826-593.

Chairman of the Joint Chiefs of Staff. *Joint Risk Assessment Methodology.* CJCSM 3105.01. Chairman of the Joint Chiefs of Staff, 2023. https://www.jcs.mil/Portals/36/Documents/Library/Manuals/CJCSM%203105.01B.pdf.

Clausewitz, Carl von. *On War.* Knopf, 1993.

Combe III, Peter C., Benjamin Jensen, and Adrian Bogart. "Rethinking Risk in Great Power Competition." *Center for Strategic and International Studies*, February 17, 2023. https://www.csis.org/analysis/rethinking-risk-great-power-competition.

Eaglen, Mackenzie. "'Economic Defense Unit': How the U.S. Military Wins in the 'Gray Zone.'" American Enterprise Institute, August 18, 2025, https://www.aei.org/op-eds/economic-defense-unit-how-the-u-s-military-wins-in-the-gray-zone/.

Groves, Bryan, Jerad M. Rich, and Kaley Scholl. "Risky Business: Using the Joint Force's Framework for Managing Risk." *Joint Force Quarterly* 111 (2023). https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3571046/risky-business-using-the-joint-forces-framework-for-managing-risk/.

Herman, Mark. "Entropy-Based Warfare: Modeling the Revolution in Military Affairs." *Joint Force Quarterly* (Autumn/Winter 1998–1999). https://bip.imsi.athenarc.gr/site/details?id=10.21236%2Fada426666.

Hernandez, Fernando. "Using Monte Carlo Simulation for Three-Dimensional Risk." (Blog) LinkedIn, April 13, 2023. https://www.linkedin.com/pulse/using-monte-carlo-simulation-three-dimensional-risk-hernandez.

Hoffman, Frank. "Risk: A Weak Element in U.S. Strategy Formulation." *Joint Force Quarterly* 116 (2025), 4–18. https://digitalcommons.ndu.edu/joint-force-quarterly/vol116/iss4/3.

International Organization for Standardization. *Risk Management – Vocabulary.* ISO 21073 (2022). https://www.iso.org/obp/ui/en/#iso:std:iso:31073:ed-1:v1:en.

Kallman, James, and John Bugalla. "How to Map Your Risks." *CFO.com,* February 14, 2013. https://www.cfo.com/news/how-to-map-your-risks/666458/.

Lykke, Arthur F. "Defining Military Strategy." *Military Review*, 69, no. 5 (1989): 183–186.

Maher, Theresa. "Pentagon Surges Palantir Maven Smart System Contract Spending More than $1B." *Inside Defense*, May 22, 2025. https://insidedefense.com/insider/pentagon-surges-palantir-maven-smart-system-contract-spending-more-1b.

Morgan, Harrison. "Dropping DIMEs: Leveraging All Elements of National Power on the Multi-Domain Battlefield." *Modern Warfare Institute*, September 18, 2019. https://mwi.westpoint.edu/dropping-dimes-leveraging-elements-national-power-multi-domain-battlefield/.

Mushen, Emily and Jonathan Schroden. *Are We Winning? A Brief History of Military Operations Assessment*. DOP-2014-U-008512-1rev. CAN, 2014. https://www.cna.org/analyses/2014/are-we-winning.

Oracle. "What Is Enterprise Risk Management?" n.d., https://www.oracle.com/erp/risk-management/what-is-enterprise-risk-management/.

Payne, Mitchell. "Assessing the Modern Fight." *Military Review*, Mar.–Apr. 2023. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/March-April-2023/Modern-Fight/.

President Donald J. Trump. *National Defense Strategy.* Washington, DC: White House, 2026. https://media.defense.gov/2026/Jan/23/2003864773/-1/-1/0/2026-NATIONAL-DEFENSE-STRATEGY.PDF.

Pusztaszeri, Aosheng and Emily Harding. "Technological Evolution on The Battlefield." *Center for Strategic and International Studies*, September 16, 2025. https://www.csis.org/analysis/chapter-9-technological-evolution-battlefield.

Rosenberg, Adrian. "Army Struggles with Enabling Joint Situational Awareness at Project Convergence 21." *Potomac Officers Club*, November 18, 2021. https://www.potomacofficersclub.com/army-struggles-with-enabling-joint-situational-awareness-at-project-convergence/.

Sun Tzu. *The Art of War.* https://classics.mit.edu/Tzu/artwar.html

Breaking Defense "The Connected Warrior Will Have a Common Operating Picture Even When Contested." *Breaking Defense*, October 18, 2024. https://breakingdefense.com/2024/10/the-connected-warrior-will-have-a-common-operating-picture-even-when-contested/.

Ulansky V. and A. Raza. "Generalization of Minimax and Maximin Criteria in a Game Against Nature for the Case of a Partial a Priori Uncertainty." *Heylion: A Cell Press Journal* 7, no. 7 (2021). https://doi.org/10.1016/j.heliyon.2021.e07498.

United States Special Operations Command. "Title 10 Authorities." n.d. https://www.socom.mil/about/title-10-authorities.

Accessing Denied Digital Terrain: SOF-Enabled Access for Cyber Operations

By 2nd Lt. Carson Tucker

Introduction

As cyber defenses become more capable and more widely applied across military and civilian networks, remote access to adversary systems may become harder to achieve, slower to exploit, or less reliable in contested environments. At the same time, the physical infrastructure that enables those systems remains present within the operational environment (OE). Special operations forces (SOF) already operate in denied areas where such infrastructure may be found, yet current doctrine does not clearly explain how SOF access and placement can enable cyberspace initial access, exploitation, and follow-on effects. Treating that relationship as a deliberate planning and force design consideration would give SOF leaders, planners, and supported commanders additional options for intelligence collection, battlespace understanding, and follow-on effects.

Modern military operations depend on cyberspace systems that support command and control, intelligence, logistics, and decision-making. Those systems are enabled by physical infrastructure in the OE, including communications nodes, servers, storage devices, and the facilities that house them. In denied areas, SOF may already operate near or directly against that infrastructure as part of broader missions. Publicly available U.S. Army examples indicate that expeditionary cyber-related capability is already being pushed closer to supported tactical formations.[1]

The gap addressed here is narrower. Current doctrine and planning do not clearly frame cyber-relevant infrastructure encountered at or near the objective as a possible pathway to cyberspace initial access. As a result, commanders and planners may recognize the physical significance of an objective without fully respecting its potential value for intelligence collection, exploitation, or follow-on cyber effects.

Cyber-relevant infrastructure encountered in denied terrain may provide a pathway to cyberspace access, but that opportunity may be missed if it is not recognized and acted on in time.

Cyber-relevant infrastructure encountered in denied terrain may provide a pathway to cyberspace access, but that opportunity may be missed if it is not recognized and acted on in time. The central argument here is that SOF access and placement in denied terrain may create conditions for cyberspace initial access when cyber-relevant infrastructure is physically present at or near the objective. This does not imply that SOF should conduct technical cyber exploitation itself. Rather, physical access to digital infrastructure can create opportunities for specialized cyberspace operators that would otherwise remain difficult or impossible to achieve through remote means alone. The proposed solution is to improve mission analysis, pilot modular expeditionary cyberspace operations elements for SOF missions, develop a practical decision framework for cyber-relevant infrastructure encountered during operations, and refine doctrine through exercises and experimentation.

Doctrine

Joint Publication (JP) 3-12, *Cyberspace Operations,* explains how the joint force employs cyberspace capabilities to achieve objectives in or through cyberspace.[2] JP 3-05, *Special Operations,* explains how SOF provide commanders with discrete, precise, and scalable options through access, placement, and action in denied, hostile, or politically sensitive environments.[3] Within that framework, SOF access and placement allows small teams to infiltrate denied areas, establish local control at or near an objective, and create

conditions for follow-on actions by other joint capabilities. Missions such as special reconnaissance and direct action may therefore involve locating, observing, securing, exploiting, recovering, or acting against targets, infrastructure, and information of operational significance. JP 5-0, *Joint Planning,* provides the keystone doctrine for how commanders translate strategic guidance into joint plans by understanding the OE, defining problems, identifying opportunities and risk, and developing operational approaches.[4]

What doctrine does not clearly do, however, is connect those ideas in a way that matters for this problem. JP 3-12 explains cyberspace operations, JP 3-05 explains SOF access and core activities, and JP 5-0 explains how planners should understand and incorporate conditions in the OE, yet none clearly state that SOF access and placement in denied terrain may enable cyberspace initial access when cyber-relevant infrastructure is physically present. That omission matters because it affects mission analysis. A planner may recognize a communications node, server, computer workstation, or data storage location as a physical objective of operational significance without also recognizing it as a potential access opportunity into a larger digital system. The gap is not only doctrinal, but it is also planning-related. While doctrine gives planners the framework to define problems and identify opportunities across domains, it does not explicitly prompt them to treat SOF proximity to cyber-relevant infrastructure as a possible pathway to cyberspace access and follow-on effects.

Access in Cyberspace

To help planners understand how operations occur within this environment, doctrine describes cyberspace as consisting of three interrelated layers: the physical network layer, the logical network layer, and the cyber-persona layer, as shown in Figure 1.[5] The physical layer includes the hardware and digital infrastructure that support

digital activity, such as communications nodes, network servers, data storage systems, and the facilities that house them. The logical layer includes the software, protocols, and data structures that allow information to move across networks. The cyber-persona layer represents the identities of users and organizations operating within cyberspace systems. The most important point is that cyberspace is not purely virtual. It is supported by physical systems in real locations, and access to those systems may sometimes be influenced by local presence, proximity, or direct control of infrastructure.

A key challenge for cyberspace operations is gaining reliable access to target systems before information can be collected or operational effects can be created. Networks may be segmented,

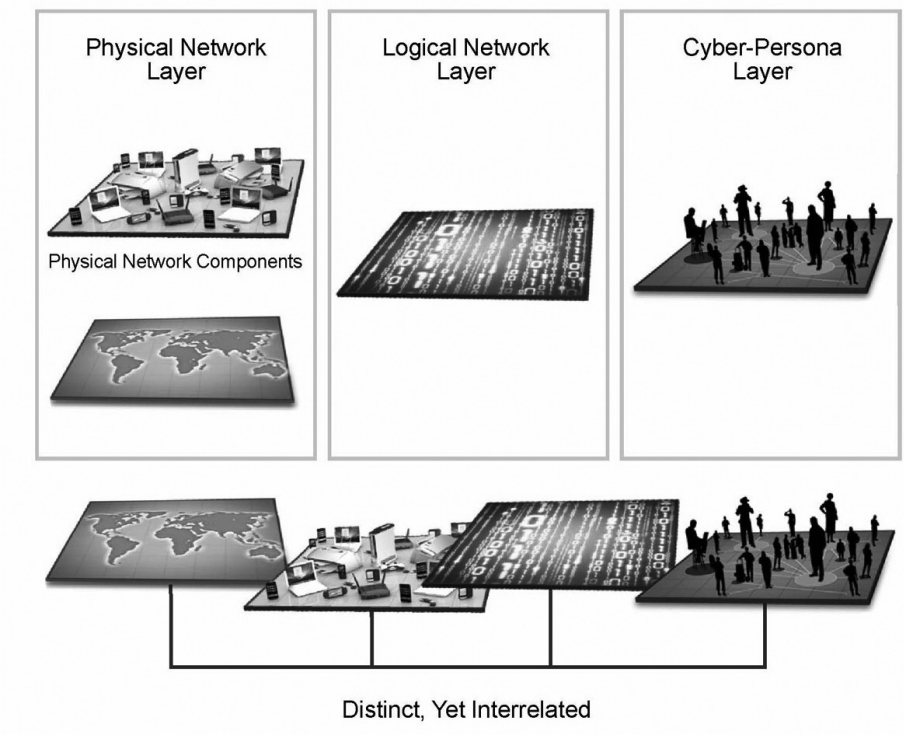


Figure 1. The three interrelated layers of cyberspace. Source: *Joint Cyberspace Operations*

isolated from external connectivity, protected by authentication controls, or physically separated from the internet. These measures are designed to prevent unauthorized entry into cyberspace systems and can reduce the speed, reliability, or feasibility of remote access. The MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework helps illustrate this problem by identifying initial access as the tactic through which an operator first gains entry into a target environment.[6] As shown in Figure 2, this access can take different forms across cyberspace layers, including identity-based access through users, remote access through the logical network layer, local or proximity-based access through signals and adjacent wireless pathways, and direct system access through the physical layer. For planners, the value of this framework is straightforward: Cyberspace effects depend on an access pathway. When remote pathways are denied, degraded, or unavailable, physical access to infrastructure in the OE may create conditions for that initial access.

Initial Access Across Cyberspace Layers

Representative access pathways adapted from JP 3-12 and MITRE ATT&CK

Cyberspace Layer	*Access Vector*	*Representative Method*	*ATT&CK Techniques*
Cyber Persona Layer	Identity / Human Access	User Targeting Credential Use Relationship Abuse	• Phishing • Valid Accounts • Trusted Relationship
Logical Network Layer	Remote Cyber Access	Public-Facing Exploits Remote Service Entry Web-Based Compromise	• Exploit Public-Facing Application • Drive-By Compromise • Content Injection
Signals / Proximity Layer	Local / RF Access	Adjacent Wireless Access Radio-Frequency Hijacking Signal Capture and Replay	• Wi-Fi Networks • Wireless Compromise
Physical Layer	Direct System Access	Removable Media Hardware Insertion Supply Chain Compromise	• Hardware Additions • Removable Media • Supply Chain Compromise

Figure 2. Initial access across cyberspace layers. Source: Author

Cyberspace systems also exist in physical form. Communications nodes, network servers, data storage systems, and other enabling infrastructure occupy real locations within the OE. This infrastructure is part of the physical expression of digital terrain, creating points where cyberspace systems intersect with the OE. If remote access is restricted or unavailable, the physical infrastructure supporting a system may represent the most practical point of interaction. If planners see digital infrastructure only as equipment on an objective, they may miss its value as a possible access point into a larger system.

This is not theoretical. A contested facility that contains a relay room, local server stack, data archive, or mission workstation may matter more than its immediate tactical value. It may represent a foothold into a broader adversary network, an intelligence opportunity, or a means of enabling follow-on cyberspace effects. If planners recognize that possibility early, they can make better decisions about whether to preserve, isolate, exploit, transfer, deny, or destroy the infrastructure they encounter.

SOF as an Access Partner

Cyber activities such as network exploitation, digital forensics, and cyberspace operations require specialized technical expertise—functions that SOF are not intended to perform. Their value in this context is their ability to operate in contested, denied, or politically sensitive environments where cyber-relevant infrastructure may be physically located. In those environments, SOF may help create the conditions that allow cyberspace operators to access systems that would otherwise be difficult or impossible to reach through remote means alone.

This enabling role is consistent with how SOF supports other joint capabilities. JP 3-05 describes SOF as providing “discrete,

precise, and scalable options" through access, placement, and action in locations that are difficult for other forces to reach. Special reconnaissance and direct-action missions may involve locating, securing, exploiting, recovering, or acting against targets and infrastructure of operational significance.[7] A similar supporting relationship can exist between SOF and cyber forces when communications nodes, routers, servers, relay sites, or data storage systems are located within the same environments where SOF already operate.

In this relationship, the roles remain distinct but complementary. SOF provide physical access to the objective, local presence, and control of the site, while cyberspace operators provide the technical exploitation. A SOF element may gain access to a facility, secure key infrastructure, or preserve a system that would otherwise remain inaccessible or be destroyed before it can be assessed. Cyberspace operators can then analyze the system, collect technical data, or establish digital access points that support intelligence gain and follow-on cyberspace effects. The contribution of SOF is not the cyber action itself. It is the access and placement that can make that action possible.

This does not mean every cyber-relevant objective should be preserved or exploited. Mission priority, time on target, threat conditions, available authorities, communications, technical support, and force protection may still drive decisions to isolate, deny, or destroy a system. The operational value of the concept is not that it removes those tradeoffs, but that it gives commanders and planners a better way to recognize them before the opportunity is lost.

Recommendations

To address the gap between physical access to digital infrastructure and the employment of cyberspace effects, the

SOF may help create the conditions that allow cyberspace operators to access systems that would otherwise be difficult or impossible to reach through remote means alone.

joint force should improve mission analysis, pilot expeditionary cyberspace operations capabilities for SOF missions, develop practical decision tools, and validate the concept through exercises. The central issue is not that SOF should perform technical cyber exploitation itself. It is that SOF access and placement may create conditions from which cyberspace operators can gain initial access to otherwise unreachable systems. These recommendations are intended to help planners, commanders, and capability developers recognize that opportunity, act on it, and refine it into a credible joint capability.

Improving Mission Planning

The first step is to improve how planners analyze objectives. If an objective contains communications nodes, routers, servers, storage devices, or other digital infrastructure, that infrastructure should not be viewed only as physical equipment on the objective—it should also be evaluated for its possible cyberspace value. Figure 3 provides a notional planning aid for assessing that value by comparing different device categories against access value, intelligence value, network leverage, denial impact, and access impact. In some cases, the unrealized value of a target is the access it can provide to local systems, networks, or stored data.

This step should begin during mission analysis. Planners should identify whether an objective contains infrastructure that may provide access to adversary communications, local networks, or

Cyberspace Value Assessment, Notional Planning Aid

Device \ Category	Access Value	Intel Value	Network Leverage	Denial Impact	Reachback Impact
Routers	High	Low	High	High	Low
Servers	High	High	High	High	High
Data Storage Systems	Low	High	Moderate	Moderate	Low
Admin Workstations	Moderate	Moderate	High	Low	High
SATCOM Gateways	High	Low	Moderate	High	High

*Devices, categories, and values to be determined by cyber-physical offensive cyberspace operations subject matter experts

Figure 3. Cyberspace device value assessment, notional planning aid.
Source: Author

technical intelligence. That should then inform whether a system should be preserved, isolated, exploited, transferred, or destroyed during the operation. This gives commanders a more complete understanding of what access to a location may actually provide.

This matters because the opportunity can be lost before cyberspace operators are ever involved. If planners do not recognize the significance of cyber-relevant infrastructure in advance, a force may bypass, damage, or destroy systems that could have supported intelligence collection, network mapping, or follow-on cyber operations. Integrating this into mission planning does not require SOF to become a cyber force. It requires planners to understand that physical access may create options for the broader joint force that goes beyond the immediate ground objective.

Forward Cyber Operations

Once this opportunity is recognized, the joint force needs personnel who can act on it. Cyber Mission Force personnel are trained to conduct exploitation and attack, but they are generally organized to operate from secure and remote locations. Expeditionary communications personnel are deployable into

SOF access and placement may create conditions from which cyberspace operators can gain initial access to otherwise unreachable systems.

austere environments, but they are not structured for technical cyber exploitation.

The joint force should pilot expeditionary cyber operations support elements that can operate alongside SOF or directly support SOF missions involving cyber-relevant objectives. These teams should be able to identify relevant systems, access local infrastructure, preserve technical opportunities, collect or deliver data, and establish secure reachback to offensive cyberspace operations (OCO) elements that can provide deeper exploitation and analysis. Their purpose would not be to independently conduct the full range of offensive cyberspace operations, but to bridge the gap between physical access and follow-on cyber action.

The concept proposed here is not without precedent. The U.S. Army Cyber Command's 11th Cyber Battalion publicly describes expeditionary cyber and electromagnetic activities teams that deploy to close gaps at the tactical edge and provide offensive cyber, information advantage, and electromagnetic warfare capabilities to supported formations.[8] In functional terms, that is very close to what the model here proposes. Both concepts push cyber-relevant capability forward so that physical access, local infrastructure, and tactical opportunity can be turned into operational advantage. The difference is not the basic logic, but the supported mission set. For SOF missions in denied terrain, cyber-relevant infrastructure may be at or near the objective, which may

> ***The joint force should pilot expeditionary cyber operations support elements that can operate alongside SOF or directly support SOF missions involving cyber-relevant objectives.***

provide an opportunity for initial access, technical exploitation, or follow-on cyberspace effects. See Figure 4.

Within the Air Force, for example, this capability could draw from existing 17S cyberspace effects operations officers and 1B4 cyber warfare operators, with additional training focused on expeditionary operations, integration with SOF, and support to denied-environment objectives. The value is in creating a layered model where SOF gains access and secures the site, forward cyberspace operators enable technical interaction at the objective, and reachback cyber forces expand that foothold into intelligence gain and follow-on effects.

Tactical Decision Framework

Not every system encountered during a mission should be treated the same way. Some systems may need to be preserved because they contain intelligence value or provide a pathway for further access. Others may need to be exploited quickly and handed off to supporting cyber elements. Some may need to be denied or disrupted to prevent enemy use, while others may still need to be destroyed based on mission demands or force protection concerns. Without a clear framework, these decisions could be made too quickly or without understanding their broader operational impact.

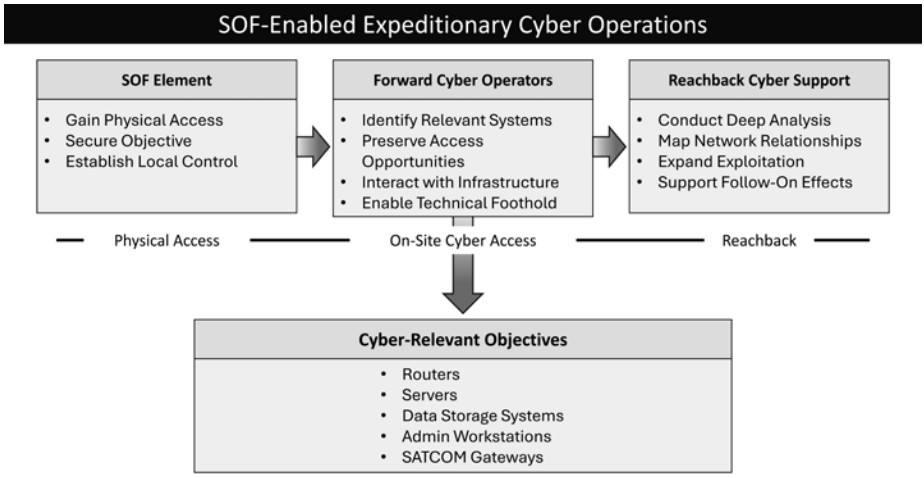


Figure 4. SOF-enabled expeditionary cyber operations sequence. Source: Author

The joint force should develop a practical decision framework for cyber-relevant infrastructure encountered during SOF missions. This framework should help commanders and operators make decisions based on mission priority, available time, threat conditions, communications, technical support, and the intelligence or access value of the system. It should also help define what minimum information should be captured when full exploitation is not possible, and how systems or data should be handed off when the mission moves faster than the technical exploitation process. One example is the Preserve, Isolate, Transfer, Exploit, Destroy, or Deny decision framework, shown in Figure 5.

This concept does not mean every cyber-relevant objective should be preserved or exploited. Mission priority, time on target, threat conditions, available authorities, communications, technical support, and force protection may still drive decisions to isolate, deny, or destroy a system. The value of the concept is not that it removes these tradeoffs, but that it gives commanders

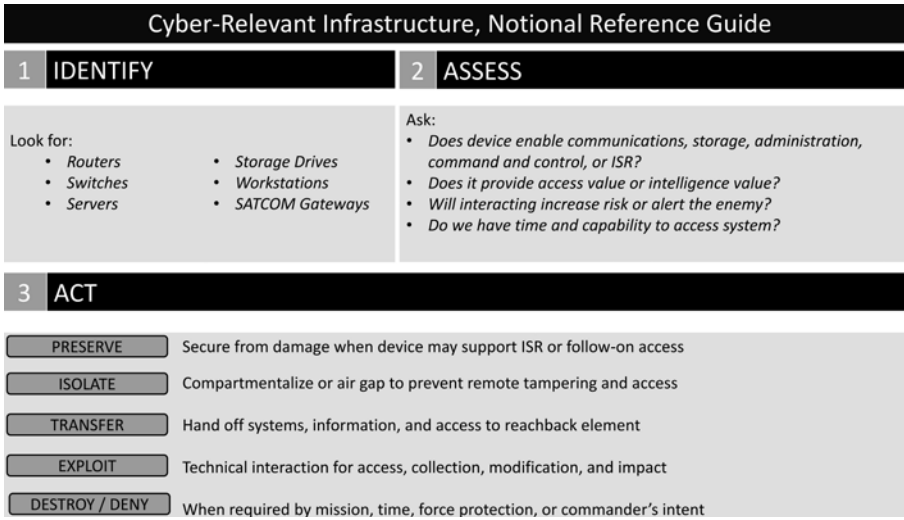


Figure 5. Cyber-relevant infrastructure decision concept chart. Source: Author

and planners a better way to recognize them before the opportunity is lost.

If SOF access can create conditions for cyber initial access, then operators and commanders need a clear way to decide what to do with the infrastructure they encounter. A decision framework helps realize this concept into a practical mission planning and execution tool.

Operational Validation and Refinement

These recommendations should be evaluated through exercises and pilot efforts before the concept is adopted more broadly. A paper can explain the idea, but only practical testing can show where it works, where it creates friction, and what support is required to make it useful. Small-scale scenarios involving denied-environment objectives with communications infrastructure, local networks, and stored digital systems would help clarify requirements for authorities, communications, equipment, training, and support

relationships between SOF, expeditionary cyber operations elements, and reachback cyber forces. Once those lessons are identified, doctrine and planning guidance should be updated to reflect them. JP 3-05 should more clearly explain how SOF access and placement can create opportunities for cyberspace initial access when cyber-relevant infrastructure is present at or near an objective. JP 3-12 should also acknowledge that physical control of terrain containing digital infrastructure may create access pathways when remote connectivity is insufficient.

Conclusion

The joint force increasingly depends on cyberspace capabilities for intelligence, command and control, and effects, but those capabilities still rely on physical infrastructure that exists in real terrain. As adversary networks become more segmented, more protected, and less accessible from outside, the assumption that cyber access can be gained remotely becomes less reliable in some environments. In denied terrain, that matters. Communications nodes, servers, storage systems, workstations, and other digital infrastructure may not only support the enemy's operations but may also present opportunities for intelligence collection, exploitation, and follow-on cyberspace effects if they are recognized and handled correctly.

SOF already operate in the kinds of contested, denied, and politically sensitive environments where cyber-relevant infrastructure may be physically present. The value SOF provide is not technical cyber exploitation itself. The value is physical access to the objective, local control of the site, and the ability to create conditions in which cyberspace operators can gain access to systems that might otherwise remain unreachable. If planners fail to recognize that relationship early, they may bypass, damage, or destroy

> ***The value SOF provide is not technical cyber exploitation itself. The value is physical access to the objective, local control of the site, and the ability to create conditions in which cyberspace operators can gain access to systems that might otherwise remain unreachable.***

infrastructure that could have produced intelligence gain, access opportunities, or broader joint effects.

The gap is not only doctrinal but also planning-related. Current doctrine explains cyberspace operations, special operations, and joint planning, but it does not clearly direct planners to view SOF proximity to cyber-relevant infrastructure as a possible pathway to cyberspace access. Closing that gap does not require turning SOF into a cyber force. It requires planners, commanders, and capability developers to better recognize the operational value of digital infrastructure in denied terrain, test practical ways to exploit that value, and refine doctrine based on what works in exercises and real-world conditions.

Treating physical access as a pathway to initial access in cyberspace would give SOF and the joint force an additional means to generate intelligence, create follow-on options, and produce effects in denied environments, an advantage that may become increasingly important as remote access grows more contested and cyber-relevant infrastructure on the objective becomes more operationally significant.

About the Author

2nd Lt. Carson Tucker is a U.S. Air Force cyberspace operations officer and graduate of the Cyber Effects Operations Course at the 333rd Training Squadron. Prior to commissioning, he served in emergency medical services, fire, and rescue roles with advanced life support responsibilities and is an International Board of Specialty Certification-Certified Tactical Responder. Tucker earned a Bachelor of Science in Cyber Intelligence and Security from Embry-Riddle Aeronautical University. His professional experience includes software development supporting contingency response operations, network and systems engineering in the aerospace and defense sectors, and large-scale data engineering and analysis supporting critical railroad infrastructure.

Notes

1. Joshua Good, "Meet 11th Cyber Battalion: Army Cyber's Workhorse for the Triad," *Special Warfare Journal* 37, no. 2 (July 1, 2024): 10–11, https://www.swcs.mil/Portals/111/SWJ_SUMMER-FALL%2024_vol%2037%20issue%202_TRIAD_INTERACTIVE.pdf.
2. Joint Chiefs of Staff, *Joint Cyberspace Operations*, JP 3-12 (Joint Chiefs of Staff, 2022), vii-ix; I-1; I-9.
3. Joint Chiefs of Staff, *Special Operations*, JP 3-05 (Joint Chiefs of Staff, 2020), ix–x; I-2; II-4 to II-5; GL-10.
4. Joint Chiefs of Staff, *Joint Planning*, JP 5-0 (Joint Chiefs of Staff, 2020), xii–xiii, xxi–xxii.
5. Joint Chiefs of Staff, JP 3-12, I-3.
6. MITRE ATT&CK, "Initial Access," accessed March 26, 2026, https://attack.mitre.org/tactics/TA0001.
7. Joint Chiefs of Staff, JP 3-05. ix; xii; xx; I-1; II-4; GL-2; GL-10.
8. Good, "Meet 11th Cyber Battalion," 10–11.

Chapter 3

The Space-Cyber-SOF-Strategic Command Nexus: How To Build Capabilities Greater Than the Sum of Its Individual Parts

As strategic competition expands into increasingly interconnected domains, SOF are uniquely positioned to bridge the gap between tactical operations and strategic effects. The convergence of space, cyber, and SOF capabilities offers new opportunities to shape the strategic environment, deter adversaries, manage crises, and prevail in conflict.

The papers in this chapter examine how USSOCOM can accelerate the development and employment of a strategic space-SOF-cyber nexus, both independently and alongside allies and partners. Topics include the potential for weaponizing the nexus to generate strategic effects, enabling operations in communications-degraded environments without reachback support, aligning SOF activities with strategic-level assets and objectives, and leveraging adaptive communication networks to conduct influence operations. Together, these studies offer insights into how SOF can enhance the joint force's ability to compete, deter, and, when necessary, fight and win.

Joint Special Operations Task Force 2030:
Weaponizing the Nexus

By Lt. Col. Michael Hagan

AI disclaimer: *This paper was prepared using Grammarly in basic mode for spelling and grammar. ChatGPT (free version) aided in the formatting of citations.*

Introduction

The contours of the 21st century are becoming clear, revealing an epoch defined by pervasive conflict. This eruption of conflicts, in turn, answers years of speculation about the impact of advances such as AI, nanotechnology, and robotics on the character of war. The U.S. Army's multi-domain operations (MDO) concept, reflected at the joint level in the joint warfighting concept, seemingly anticipated these developments and prescribed workable solutions. Among these solutions, the imperative to integrate domains ("convergence," in MDO parlance) is not new at operational echelons but is revolutionary at the tactical echelon.[1] The U.S. Special Operations Command (USSOCOM) desire to synergize effects from space, cyber, nuclear, and special operations forces (SOF) is therefore the logical progression of this broader MDO trend. Weaponizing this "nexus" is possible, but to do so, USSOCOM must evolve the joint special operations task force (JSOTF) into an MDO-capable formation, with all that this entails, to prevail in the hyper-contested and lethal battlefield that will typify peer conflict.[2]

To understand why JSOTF 2030 must be *the* enterprise priority for USSOCOM, this discussion will first examine the character of future conflict using the revealing lens of the Russia–Ukraine war. The experience of combined JSOTF-10 (CJSOTF-10) in that war highlights the need for a SOF headquarters that can survive and thrive in a battlespace defined by ubiquitous surveillance; pervasive robotics; the presence of chemical, biological, and nuclear threats; and effects from and through space and cyberspace. Returning to the enduring truth that war is a human endeavor brings the SOF value proposition to the foreground. Understanding what SOF brings to the nexus explains why the JSOTF echelon, rather than some other echelon, should be the focus of USSOCOM modernization.

The Character of War

While the above evolutions in the character of war have been extensively discussed by both academics and practitioners, the experience of CJSOTF-10 at the outset of the ongoing Russia–Ukraine War demonstrates their real-world consequences when melded with war's enduring violent and uncertain nature. CJSOTF-10, an O-6 command under Special Operations Command Europe (SOCEUR), was established to respond to Russia's invasion of Ukraine with a broad campaigning approach along NATO's eastern flank. CJSOTF-10 complemented the work that U.S. European Command (USEUCOM) and Security Assistance Group-Ukraine (SAG-U) had begun from the onset of the invasion, providing SOF expertise to enhance the unprecedented conventional security force assistance mission led by SAG-U.[3]

The first MDO challenge that CJSOTF-10 had to contend with was "ubiquitous surveillance": a consequence of the growth in all-domain intelligence, surveillance, and reconnaissance (ISR), which essentially means there is "nowhere to hide." Russian forces at the outset of the Russia–Ukraine War, for example, were equipped to detect adversaries using electronic direction-finding, open-source data (e.g., social media monitoring), small unmanned aircraft systems (sUAS), and traditional ISR platforms (e.g., the Beriev A-50 "Mainstay"). This constrained the ability for CJSOTF-10 to send advisors forward into Ukraine since, unlike in earlier conflicts, SOF placed with a partner force faced a high likelihood of detection in a context that carried severe escalation risks. CJSOTF-10 adapted through methods such as advising in sanctuary and leveraging its partner network.[4] Future peer conflict with adversaries such as the People's Republic of China is certain to replicate this environment of ubiquitous surveillance, along with similar escalation potentials and policy constraints, making it imperative for JSOTF 2030 to build on CJSOTF-10's success in adapting to this trend.

CJSOTF-10 also bore witness to, and had to contend with, a growth of robotics and nascent AI on the battlefield. The proliferation of unmanned systems (UxS) in the Russian–Ukraine war has been dramatic, with estimates of as high of 75 percent of casualties on both sides being caused by UxS. In some Ukrainian assaults, up to 60 percent of assets deployed now consist of UxS. The apex predator emerging from the interactive process of battlefield evolution has been the fiber-optically guided, first-person view, one-way attack UxS, but spectacular attacks such as the 2025 Operation Spiderweb also hint at the autonomous potential offered by AI.[5] While the CJSOTF can take little credit for this dramatic growth in UxS, scaled on both sides through crowdfunding and crowdsourcing, its coordination and partner network were key in detecting innovation and adapting the training of Ukrainian SOF as battlefield lessons emerged.[6] In short, JSOTF 2030 will require warfighting competencies beyond "door kicking" to successfully anticipate, understand, and communicate innovation to a partner force in this era of rapid technological change.

Most ominously, the Russia–Ukraine War resurrected the specter of chemical, biological, and nuclear use. Russia holds the largest and most diverse nuclear weapons arsenal in the world, and likely maintains chemical, biological, and radiological programs, with a demonstrated track record using these to attack dissidents abroad.[7] According to journalist Bob Woodward, Russian president Vladimir Putin seriously considered using tactical nuclear weapons in Ukraine, with the U.S. intelligence community putting the odds as high as 50 percent at some critical moments (e.g., when Russian troops were at risk of encirclement in Kherson).[8] CJSOTF-10 operated in this environment of severe escalation risk and corresponding policy constraints, and would probably have played a role in confirming a nuclear detonation through its network of partners. Russia's use of riot-control agents, maneuver through the Chornobyl area, and

seizure of the Zaporizhzhia Nuclear Power Plant all give further hints of the complications of operating on a contaminated battlefield. These developments show that JSOTF 2030 will need to operate in a decentralized manner, incorporate adequate training and personal protective equipment, and be proficient at both counter weapons of mass destruction activities and nuclear targeting to be adapted for the weapons of mass destruction (WMD) potentials of peer conflict.

Finally, while effects from and through space and cyberspace played a less outsized role in the conflict than many experts expected, the Russia–Ukraine War has been a harbinger of the transformative potentials of these domains. From the indispensability of the Starlink satellite network, to denial-of-service attacks on Ukrainian government and banking websites, to Ukrainian retaliation with cyberattacks on websites of Russian proxy forces, ample evidence shows that space and cyberspace are contested.[9] Trends in the "democratization of technology" mean that many capabilities, like those needed to conduct offensive cyberspace operations, once seen as strategic and held within combatant commands or Tier 1 units, can now be widely fielded at affordable cost within SOF. This again shows the need for a high level of technical savviness within JSOTF 2030, to either create effects through space and cyberspace or to advise and assist partner forces to do so.

The SOF Value Proposition Endures

The common thread in this discussion of CJSOTF-10's contribution to the Russia–Ukraine War is the enduring significance of the human dimension and, correspondingly, SOF expertise in building and leveraging human networks. Just as CJSOTF-10 synergized the disparate efforts of allies, industry, and the interagency, while communicating information from and to the Ukrainian battlefield, SOF habitually engage in core activities that

> ***Just as CJSOTF-10 synergized the disparate efforts of allies, industry, and the interagency, while communicating information from and to the Ukrainian battlefield, SOF habitually engage in core activities that empower human networks.***

empower human networks. Paradoxically, technologically driven battlefield conditions like ubiquitous surveillance, pervasive UxS, the specter of WMD threats, and effects from and through space and cyberspace only amplified the importance of the human dimension. This is yet another affirmation of SOF Truth #1, that "humans are more important than hardware."

CJSOTF-10's success was premised on decades of relationship-building in Europe as SOCEUR campaigned in the gray zone. The SOCEUR effort that bore fruit most directly was the training of Ukrainian SOF Teams at the Joint Multinational Training Group-Ukraine (JMTG-U), beginning in 2016.[10] However, SOCEUR's and 10th Special Forces Group (Airborne)'s persistent presence in Europe for over 70 years was even more consequential. In varying forms, both organizations have remained in Europe since the 1950s.[11] This yielded a regional orientation and local knowledge that proved invaluable for leveraging human networks in conflict. As USSOCOM proceeds with modernization, it is critical to stay oriented on this critical enduring advantage.

The Joint Special Operations Task Force as SOF's Unit of Action

The significance of the theater special operations command (TSOC) setting the theater might suggest that the theater-strategic

level is the decisive level for the nexus, but this is not the case. As has been seen, the TSOC's actions in campaigning are certainly critical for preparing the JSOTF to converge effects from space, cyber, nuclear, and SOF in conflict. However, in conflict, the TSOC continues setting the theater for future contingencies (e.g., branches and sequels) and can be expected to assume a new and significant theater-strategic role as the Joint Force Special Operations Component Command: essentially, an extension of the joint force commander's (JFC) staff. These significant theater-strategic demands on the TSOC dictate that any of its operational-level work, including the convergence of joint effects, must devolve to a lower-level headquarters in conflict.

Similarly, the special operations joint task force (SOJTF) is a general officer-led organization established in conflict to release the TSOC to its normal mission. It is an extension of the JFC staff, solving theater-strategic problems such as advising the JFC on recommended command relationships for SOF, preparing requests for forces, tailoring SOF into mission packages as they arrive in theater, and establishing reachback arrangements with the wider USSOCOM enterprise.[12] So, while a SOJTF can greatly assist the TSOC in establishing human and physical architecture to converge effects from space, cyber, nuclear, and SOF, it is not best placed to actually converge joint effects.

The lack of survivability of a single TSOC or SOJTF in an MDO environment, where ubiquitous surveillance combines with hyper-lethality, provides a final rationale to adopt a decentralized approach to nexus convergence. Imagining a mirror image of the current U.S./Israel–Iran War shows the risks of infiltration and targeting faced by a lone, exquisite headquarters in peer conflict. Higher-level headquarters were quickly eliminated by airstrikes, while the 31 decentralized Iranian Revolutionary Guards Corps provincial commands have continued to generate SOF, UxS, and missile strikes

well into the conflict.[13] Similarly, a series of decentralized JSOTFs—operating via burst transmissions that reduce their targetable signature—are both survivable and redundant. MDO battlefield requirements, therefore, align with SOF's decentralized mission command approach, where commanders operate on the basis of understanding, intent, and trust.[14]

Placing nexus capabilities of space, cyber, nuclear, and SOF at the JSOTF level pushes those effects down to the highest level that is survivable, and the lowest level with joint capability to converge joint effects. The U.S. Army sees convergence taking place at the Corps level, so placing responsibility for convergence on an O6-level command might be surprising to conventional forces.[15] However, as another example of the democratization of technology, advancements in AI-enabled command and control (C2) hold the potential for a smaller JSOTF staff to converge joint effects that previously required extensive and tedious coordination. In some portions of the joint operations area (JOA), where a JSOTF supports a larger joint or allied force, the JSOTF might merely "plug in" to a multi-domain task force architecture to request effects. In other portions of the JOA (e.g., peripheral zones), where the JSOTF is the exclusive battlespace owner, it might be responsible for converging joint effects unilaterally or on behalf of a partner force.

Making Joint Special Operations Task Force 2030 a Reality

In the near term, two urgent tasks lie ahead for USSOCOM to build the JSOTF into an MDO-capable formation. First is to reform the current ad-hoc model that JSOTFs are fielded under. This reform would both vastly increase JSOTFs' readiness for peer conflict and create a secondary benefit in advancing MDO leader development. Second is to accelerate the fielding of technological solutions that

allow for both the modernized C2 and the joint effects needed for a JSOTF in conflict.

JSOTFs are not currently standing organizations and are instead created when a crisis occurs. Typically, the core of a JSOTF is formed from a U.S. Army Special Forces Group, a U.S. Air Force Special Operations Wing, or a U.S. Navy Special Warfare Group. It is worth noting that the day-to-day missions of these organizations are often "generating force" in nature: These O-6 commands are focused on fielding team-level units for campaigning globally and must drastically reorient themselves when called upon for warfighting. After identifying the core staff, joint enablers are added from across the USSOCOM enterprise to give the JSOTF its "jointness," with subordinate SOTF's fielded from—ideally—the parent SOF O-6 command.

Obviously, fielding JSOTFs that are not "pickup teams" and that focus entirely on MDO warfighting would be ideal for readiness. Less obvious is the impact of this advancement on leader development, as standing JSOTFs can become the crucible where SOF leaders become multi-domain experts. The experience of the officers and NCOs of the former U.S. Army Asymmetric Warfare Group (AWG)—the closest real-world analog to a standing multi-domain O6-level SOF organization—provides an example of this. As a standing organization, AWG would conduct leader professional development (LPD) sessions on topics ranging from satellite transmission bands to battlefield medicine advancements. These LPDs paid dividends when, for example, AWG operational advisors imported sUAS lessons learned from AWG's Mosul Study Group to partner forces in the U.S. Pacific Command. Following their AWG tours, personnel went to follow-on assignments where they raised the MDO understanding of the entire joint force.[16] Likewise, JSOTFs can serve as a leadership factory, raising the MDO capability of SOF at all echelons as personnel rotate in and out of a premier MDO formation.

> ***Fielding joint special operations task forces that are not "pickup teams" and that focus entirely on multi-domain organization warfighting would be ideal for readiness.***

As previously described, some technological hurdles still remain to allow JSOTF 2030 to converge effects from space, cyber, nuclear, and SOF. Most significant is the need for AI-enabled C2, which ties disparate systems together, allows for rapid decision-making, and reduces the cognitive burden on staff. So-called joint all domain command and control (JADC2) is a classic wicked problem, requiring cooperation from all the services, solving technical challenges, and navigating the Department of War (DoW)'s procurement system.[17] The AI component will be critical for a JSOTF to stay lean: not grow to the size of a U.S. Army Corps Staff, yet perform many of the same functions. For example, in a peer conflict with theater nuclear exchange, one JSOTF staff officer may need to nominate targets to U.S. Strategic Command and rapidly perform preclusion analysis, while another oversees a partner-enabled close-access cyberspace operation to disable the enemy's missile launchers, and a third re-tasks a swarm of UxS to a new named area of interest. Operations across such a wide domain scope at these speeds would remain beyond both the practical experience of current JSOTFs and the capabilities of existing C2 systems.

Less critical but still significant is the development of additional joint effects, organic to SOF or to a SOF partner force. As previously highlighted, UxS, cyberspace capabilities at lower echelons, and battlefield awareness tools have all grown rapidly. However, the U.S. has not necessarily been the leader in any of these areas, as evidenced by senior leader frustration and a series of canceled programs.[18] Recent decisions to place USSOCOM at the center of much of this modernization are both a much-needed corrective

and an opportunity to ensure the resulting joint solutions are also suitable for SOF. Time is of the essence, however, as adversaries are also trying to accelerate their progress.

Conclusion: SOF Underpins the Nexus

In the past, effects from traditional domains and from space, cyberspace, nuclear forces, and SOF fell under the purview of distinct services or combatant commands. The technological advancements of the information age have rendered that construct obsolete. As CJSOTF-10's experience operating on the periphery of the Russia–Ukraine War shows, the battlefield has become transparent; swarmed by robotics; and hazarded by chemical, biological, radiological, and nuclear weapons as well as effects from and through space and cyberspace.

To survive and thrive in this MDO environment, JSOTF 2030 must be able to converge nexus capabilities from space, cyberspace, nuclear forces, and SOF. Far from being beyond the capability of an O6-headquarters, convergence is a critical competency for this SOF unit of action, which is both large enough to be joint and small enough to evade the hyper-lethal effects of peer adversaries. However, significant reforms are needed to get there: JSOTFs must transform into standing units and be enabled with still-nascent technologies, such as AI-augmented JADC2, which USSOCOM must accelerate.

Joint special operations task force 2030 must be able to converge nexus capabilities from space, cyberspace, nuclear forces, and SOF.

When President John F. Kennedy reflected on the advent of the "nuclear age," he concluded that the label was misleading. Rather

than transforming war into a contest of massive retaliation, growth in nuclear weapons had seemed to spark both a continuation of land warfare and a rash of insurgencies; Kennedy turned to SOF for a solution.[19] Now, in the information age, technological advances have, once again, paradoxically only increased the importance of the human element in war. As the forces best able to harness human networks, it's fitting for SOF to step forward again to tie together the nexus's power. The wars of the future may be fought with effects from space, cyberspace, and—in extreme cases—nuclear forces, but they will be won by human effort.

About the Author

Lt. Col. Michael Hagan is a U.S. Army Reserve officer who has served in the Army Strategist functional area since 2015. He holds a bachelor of science degree in engineering management from the Illinois Institute of Technology, a master's of business administration degree from DePaul University, and is a graduate of the U.S. Army Command and General Staff College and Basic Strategic Art Program.

Notes

1. Note that as early as 1946, Dwight Eisenhower could confidently declare that "separate ground, sea and air warfare is gone forever." Dwight D. Eisenhower, "Special Message to the Congress on Reorganization of the Defense Establishment," June 1946.

2. Note that the term "nexus" in this paper draws from the U.S. Army Special Operations Command (USASOC)-originated idea formerly known as "triad," which converges effects across space, cyber, and SOF; effects from U.S. Strategic Command (STRATCOM)—nuclear effects—were later added, so the "triad" term is now odd (four components, not three) and risks conflation with the "nuclear triad" (missiles, aircraft, submarines). USSOCOM and U.S. Space Command (SPACECOM) have been engaged in a separate "nexus" initiative aimed at fostering greater cooperation among functional combatant commands. As of March 2026, the Joint Special Operations University refers to the totality of both efforts as "nexus."

3. The Joint Staff, "Memorandum for Commander, Army Human Resources Command, ATTN: AHRC-PDP-PA. Subject: Joint Meritorious Unit Award." Permanent Order Number J-1 SO-0033-25. March 21, 2025. Awarded to Headquarters, Combined Joint Special Operations Task Force-10 for service from October 17, 2022, to April 30, 2024.

4. The Joint Staff, "Joint Meritorious Unit Award for CJSOTF-10," and Bob Woodward. *War* (Simon & Schuster, 2024),114-116.

5. Tsiporah Fried, "The Impact of Drones on the Battlefield: Lessons of the Russia–Ukraine War from a French Perspective," *Hudson Institute*, November 13, 2025, 3–7, https://www.hudson.org/missile-defense/impact-drones-battlefield-lessons-russian-ukraine-war-french-perspective-tsiporah-fried.

6. The Joint Staff, "Joint Meritorious Unit Award for CJSOTF-10."

7. U.S. Department of Defense, *2022 Nuclear Posture Review* (Department of Defense, 2022), 4, https://fas.org/wp-content/uploads/2023/07/2022-Nuclear-Posture-Review.pdf; Woodward, *War*, 25; Patty Housman, "Could Putin Use Chemical or Biological Weapons in Ukraine?," *American University*, March 14, 2022, https://www.american.edu/cas/news/could-putin-use-chemical-or-biological-weapons-in-ukraine.cfm.

8. Woodward, *War*, 151–159.

9. "How Elon Musk's Satellites Have Saved Ukraine and Changed Warfare," *Economist*, January 5, 2023, https://www.economist.com/briefing/2023/01/05/how-elon-musks-satellites-have-saved-ukraine-and-changed-warfare and Lauren Feiner, "Cyberattack Hits Ukrainian Banks and Government Websites," *CNBC*, February 23, 2022, https://www.cnbc.com/2022/02/23/cyberattack-hits-ukrainian-banks-and-government-websites.html.

10. "Towards New Armed Forces of Ukraine: Overview of Defense Reforms in Ukraine 2016," Ministry of Defense of Ukraine, Reforms Project Office, accessed July 21, 2026, https://andyreiter.com/wp-content/uploads/military-justice/ua/Government%20Documents/Ukraine%20-%202016%20-%20Ministry%20of%20Defense%20-%20Review%20of%20Reforms.pdf:5.

11. U.S. Special Operations Command Europe, "History," *U.S. Special Operations Command Europe*, accessed March 25, 2026, https://www.socom.mil/soceur/

history and U.S. Army, "10th Special Forces Group (Airborne) History," *Fort Carson*, accessed March 25, 2026, https://home.army.mil/carson/units-tenants/tenants/10sfg/10sfg-history.

12. Joint Chiefs of Staff, *Special Operations*, JP 3-05, (Joint Chiefs of Staff, 2014), A-2 thru A-6, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_05.pdf.

13. Andrew Fox, "The IRGC's Way of War," *Engelsberg Ideas*, November 10, 2023, https://engelsbergideas.com/notebook/the-irgcs-way-of-war/.

14. For a description of SOF Mission Command, see: Joint Chiefs of Staff, JP 3-05, A-2 through A-6.

15. U.S. Army Training and Doctrine Command, *TRADOC Pamphlet 525-3-1: The U.S. Army in Multi-Domain Operations 2028* (TRADOC, 2018), C-6, https://adminpubs.tradoc.army.mil/pamphlets/TP525-3-1.pdf.

16. Based on the author's own experience serving in the Asymmetric Warfare Group.

17. John R. Hoehn, "Joint All-Domain Command and Control (JADC2)," *Congressional Research Service In Focus* IF11493, July 1, 2021, https://www.congress.gov/crs-product/IF11493.

18. Mark Pomerleau, "Hegseth Orders Sweeping Changes to Army Structure," *DefenseScoop*, May 1, 2025, https://defensescoop.com/2025/05/01/hegseth-orders-sweeping-changes-army-structure-transformation/.

19. "'Another Type of Warfare': JFK's Address to the West Point Class of 1962," *Veritas: Journal of U.S. Army Special Operations History*, accessed March 25, 2026, https://arsof-history.org/articles/v19n1_jfk_address_to_west_point_page_1.html.

There's No One to Take Your Call at This Time: Operating Without Reachback—Decision Continuity at the Space–Cyber–SOF–STRATCOM Nexus

By Ryan K. Kaono-Wedemeyer

Integration Fails when Authority and Data Collapse Together

Future conflict will begin with disruption. Space and cyber systems central to the space–cyber–special operations forces (SOF)–U.S. Strategic Command (STRATCOM) nexus will be challenged early, sometimes deliberately and sometimes opportunistically. Near-peer competitors are widely assessed as having the ability to contest space-enabled and cyber-dependent systems in ways that undermine confidence and continuity without requiring immediate, total denial.[1]

The operational challenge is no longer whether these systems will be stressed. It is how the joint force, and particularly SOF, will continue to operate when access to space- and cyber-enabled capabilities degrades unevenly across time, systems, and echelons. In this environment, the promise of integration is tested not by performance under ideal conditions, but by resilience under disruption.

Modern integration across space, cyber, and SOF is built on speed.[2] It assumes that information moves quickly, that connectivity is available when needed, and that friction can be resolved through coordination and reachback. Under routine conditions, that model works well enough. Under disruption, it does not fail cleanly.

Some systems remain available. Others lag. Some updates continue to flow. Others stall. The result is not total loss but an uneven operating picture in which access and awareness degrade at different rates. This unevenness is more destabilizing than complete denial because it sustains the illusion of control long after authoritative context has begun to erode.

When space and cyber access degrade, the first failure is rarely the technology itself. It is the loss of authoritative context

that technology is expected to carry. Mission parameters, rules of engagement, delegated authorities, and priority guidance are increasingly delivered through the same pathways that provide situational awareness and coordination. When those pathways falter, access to authoritative guidance collapses alongside access to data.

This creates an enterprise-level problem that is structural rather than situational. Authority is often treated as external to the systems that deliver information, assumed to be retrievable through clarification or coordination when needed. That assumption holds only as long as connectivity holds.

When information degrades, authority blurs, and decisions that should be routine become questions.

When information degrades, authority blurs, and decisions that should be routine become questions. That vagueness works on paper; it rarely works in real time. In practice, standing plans are often pulled from the shelf, dusted off, and adjusted, yet still fail to keep pace with evolving conditions. Commanders and their staffs are then forced to sort it out and issue new orders on the fly.

The space-cyber-SOF-STRATCOM relationship sits at the center of this challenge. Each element brings critical capability. Space enables global access, timing, and awareness. Cyber provides transport and access. SOF deliver tailored effects forward, often with strategic consequence. STRATCOM integrates global operations and manages risk across domains and time horizons.

The value of this relationship is determined by whether authority, intent, and execution remain aligned when access cannot be assumed. When those elements separate, integration becomes brittle. When they remain aligned, integration becomes a force multiplier even under disruption.

These dynamics are visible at the enterprise level, but their consequences are felt most sharply at the point of execution. It is there, under degraded connectivity and incomplete information, that the burden of integration shifts onto operators. Understanding how this burden manifests at the tactical level is essential to identifying what capabilities are missing today.

The Problem as Experienced at the Point of Execution

For operators on the ground, disruption is experienced as friction rather than strategy. Maps stop updating, positions lag, messages queue instead of flowing, and reachback becomes slow, then unreliable, then gone. None of this happens all at once, and none of it is immediately decisive.

What makes this friction dangerous is not its severity but its ambiguity. Nothing has clearly failed. Systems still display information. Icons still populate. Messages still appear, just late. Operators are left to determine whether the delay reflects a technical issue, a routing problem, or a change in the operational environment itself. Each possibility implies a different response, but none can be confirmed quickly.

Time continues to pass. The team continues to move. Security is maintained, but attention shifts inward as operators begin to question the reliability of what they are seeing. The cost is measured in seconds and minutes, not hours. In a special operations context, that is often enough to alter outcomes.

Positioning, navigation, and timing do not need to disappear to create problems.[3] They only need to become inconsistent.

Communications don't need to be completely severed. They only need to be unreliable. When systems behave this way,

Operators may delay engagement, adjust positioning, or defer action entirely while attempting to reconstruct guidance.

operators hesitate not because they lack initiative, but because they lack certainty. They pause to confirm and validate. Inconsistent systems create a cognitive trap. Operators are trained to trust their equipment until it clearly fails.

When updates arrive sporadically, that trust degrades unevenly. Some team members act on information they believe is current. Others hold back, waiting for confirmation.

Coordination slows as internal alignment breaks down, even though the team remains physically together.

But the mission does not stop. The objective remains in front of them. They are forced to decide not only what to do, but whether they are still authorized to do it. They retain the ability to act, but is it still legal to do so?

This question is not academic. It shapes behavior in real time. Operators may delay engagement, adjust positioning, or defer action entirely while attempting to reconstruct guidance. Even when the tactical situation is clear, uncertainty about legal or policy constraints introduces hesitation. That hesitation is often invisible from higher headquarters, but its effects accumulate quickly at the point of execution.

The tools operators rely on inadvertently erode procedural muscle memory. Many modern mission systems are built around continuous connectivity. They pull maps, overlays, target data, and guidance from remote sources.

Over time, reliance on continuously connected systems changes how operators prepare. Fewer decisions are rehearsed in advance because clarification is expected to be available when needed. Authority is assumed to be reachable. When that assumption fails, training does not always fill the gap. Operators are left to improvise within boundaries they have not recently practiced enforcing without external confirmation.

In these moments, operators are not asking for more data. They are asking a simpler question: *What still applies right now?* Without a reliable answer, they are forced to reconstruct authority from memory, briefing notes, and judgment. That reconstruction happens under stress, in motion, and often in contact. What may have been authoritative when they infiltrated may have changed in the last 20 minutes.

This is where the gap in current integration approaches becomes operationally visible.

Where Current Technology and Training Fall Short

The gap is the product of how modern systems are designed and how forces are trained to rely on them. Technology has advanced faster than the assumptions embedded in its use, and training has not kept pace with how those systems actually fail.

Most modern mission systems are built around persistent connectivity. Maps, overlays, tasking updates, rules of engagement, and legal guidance are increasingly cloud-based and continuously refreshed.[4] As long as networks are available, this model works and information is current.

Guidance is clear. Authority feels present even when leadership is physically distant.

This is not a hardware problem. It is a design problem. Current systems prioritize access and synchronization over continuity.

Training reinforces these design assumptions. Exercises are typically conducted with full connectivity or with short, scripted outages. Loss of communications is treated as an inject, not a sustained condition.[5] When networks come back, play resumes. Rarely are teams required to operate for extended periods with partial data, outdated guidance, and no reachback.

This training approach builds technical proficiency but weakens confidence under disruption.

At the enterprise level, this gap is compounded by how authority is treated in system design. Rules of engagement, delegated authorities, and commander intent are often managed as documents rather than as data. They are briefed, referenced, and updated externally, but rarely embedded into the systems operators use during execution.

The combined effect is predictable. This gap does not exist because the force lacks capability. It exists because current approaches treat connectivity as a prerequisite for authority rather than as a transport mechanism for it. Until technology and training are designed to preserve authoritative context under disruption, integration will continue to produce friction at the moments it is supposed to provide advantage.

The Missing Capability: Decision Continuity Under Degraded Access

The missing capability is not more data. It is decision continuity under degraded access.

Today's systems are built to deliver information, not to preserve authority. Rules of engagement, commander intent, delegated authorities, and mission constraints are treated as external references rather than as operational data. As a result, authority and data remain tightly coupled to access.

What is missing is decision continuity, not decision automation or autonomous action. Decision continuity is the ability to preserve authoritative guidance at the point of execution as systems degrade, allowing operators to continue acting within approved boundaries even when reachback is unavailable.

This capability does not require new sensors or networks. It requires a shift in how authority is treated within existing systems. Authoritative mission context must be managed as data, versioned and updated alongside operational information, rather than stored in documents or briefings that vanish when access is lost.[6]

What is missing is decision continuity, not decision automation or autonomous action.

In practical terms, this means that mission parameters, rules of engagement, delegated authorities, priority tasks, and abort criteria must remain accessible at the edge even when live connectivity does not. The loss of access should not force operators to fall back to memory or static pre-mission briefs. It should trigger a transition to the most current authoritative guidance available at the moment connectivity is lost.

Without this capability, integration remains fragile. Space, cyber, and special operations capabilities may still function independently, but they no longer reinforce one another when access degrades. With decision continuity, integration becomes resilient, authority

remains aligned with available data, operators retain confidence, and tempo is preserved.

The absence of this capability explains why current integration efforts struggle under disruption. Its presence would allow the space–cyber–SOF–STRATCOM nexus to function as intended, not only when networks are available, but when they are not.

Designing for Decision Continuity at the Tactical Edge

Decision continuity does not require a new platform or a standalone system. It requires rethinking how existing mission systems handle authoritative information. The core design principle is simple: Authority must persist independently of connectivity. If access to space- and cyber-enabled systems degrades, the guidance that governs action should not degrade with it.

In practice, this means treating rules of engagement, delegated authorities, mission priorities, and abort criteria as operational data rather than static references. While connectivity is available, this data should update continuously through existing space- and cyber-enabled pathways, just as maps, positions, and tasking updates do today. The system should not wait for a mission start point to load guidance. It should carry the most current authorized context forward, continuously refreshed up to the moment access degrades.

When connectivity becomes unreliable or unavailable, the system should transition automatically. No user actions. No menu selection. No judgment call under stress. The loss of access itself becomes the trigger. At that point, the system preserves the most current authoritative guidance available and makes it readily accessible at the point of execution. This is not simply cached data—it is

Decision continuity is not about automation or autonomy. It is about preventing authority from becoming ambiguous at the moment judgment is required.

a deliberate handoff from live authority to preserved authority, designed into the system rather than improvised by the operator.

This preserved guidance does not replace judgment. It provides the boundaries within which judgment is exercised. Operators still decide how to act, but they do so with confidence in what authorities remain in effect. The system does not tell them what to do. It tells them what still applies. That distinction matters. Decision continuity is not about automation or autonomy. It is about preventing authority from becoming ambiguous at the moment judgment is required.

Integration with existing Blue Force Tracking systems, which provide a shared display of friendly force locations, is essential. Operators already rely on these interfaces under stress. Adding a parallel tool would increase cognitive load rather than reduce it. Decision continuity must live where operators already look, alongside position data, terrain, and mission overlays. When access degrades, operators should not have to change tools or workflows. The system should change behavior around them.

The design should prioritize clarity over completeness.[7] Operators do not need full legal text or extensive policy detail in the moment. What they need are concise, authoritative boundaries, such as what actions are authorized; what actions are restricted; and what conditions trigger abort, escalation, or transition. This information

should be presented in a format that is immediately understandable under pressure and does not require interpretation or reconstruction.

This approach also supports uneven degradation. As partial connectivity returns, authoritative updates can resume incrementally. The system does not require full restoration to be useful. It adapts as access improves or worsens, preserving continuity across fluctuating conditions rather than treating loss and restoration as binary states.

Importantly, this capability does not undermine command authority. It reinforces it. Commanders retain full control over what guidance is issued, updated, and delegated. The system simply ensures that their intent and constraints remain present when reachback is unavailable. Rather than forcing operators to improvise governance under stress, it preserves the commander's last authoritative guidance at the moment it matters most.

Designed this way, decision continuity becomes a force multiplier. It reduces hesitation without encouraging recklessness. It preserves tempo without eroding control. It limits unnecessary escalation while maintaining accountability. Most importantly, it aligns authority with available data at the moment decisions must be made, allowing integration across space, cyber, and SOF to remain effective even when access is degraded.

Implications for the Space–Cyber–SOF–STRATCOM Nexus

Decision continuity is not a tactical convenience. It is an enterprise requirement that sits squarely at the intersection of space, cyber, SOF, and STRATCOM responsibilities. The conditions that create the problem are generated at the strategic level, even though the consequences are felt at the tactical edge. No single component can solve this in isolation because the failure modes emerge

from how the enterprise is integrated, not from how individual elements perform.

Space-enabled services provide timing, navigation, and global reach. Cyber infrastructure carries mission data, updates, and authoritative guidance. SOF execute forward with limited margin for error and limited opportunity for correction once committed. STRATCOM integrates global operations, manages escalation risk, and balances effects across domains and time horizons. When access degrades in one domain, the effects cascade across all four, often in ways that are difficult to predict in advance.

In this environment, uneven degradation is the norm rather than the exception. Space effects may be localized, intermittent, or delayed. Cyber access may be throttled, burdened, or selectively unavailable. Strategic command and control may remain intact even as tactical reachback becomes unreliable or unreachable. These conditions are particularly likely early in a conflict or crisis, when adversaries seek to create uncertainty without crossing clear thresholds.

This capability also addresses a persistent challenge in joint and coalition operations. Authorities are often delegated differently across components, partners, and operational phases. Under full connectivity, these differences can be clarified through coordination and reachback. Under degraded conditions, they become friction points that slow tempo and increase risk. Preserving authoritative context at the edge reduces the need for real-time coordination and limits the likelihood that ambiguity produces unintended escalation, mission failure, or political consequence.

For STRATCOM, decision continuity directly supports strategic risk management.[8] It reduces the probability that tactical actions taken under uncertainty create effects that commanders did not intend or anticipate. By preserving intent, constraints, and delegated

> ***The conditions that create the problem are generated at the strategic level, even though the consequences are felt at the tactical edge.***

authority forward, STRATCOM maintains influence over execution even when direct communication is disrupted. This is particularly important in scenarios where tactical actions may have strategic signaling or escalation implications beyond their immediate operational effect.

For space and cyber forces, this approach reframes their role within the enterprise. Rather than being viewed solely as providers of access and connectivity, they become custodians of authoritative context. Their contribution is not only to move data but also to ensure that what matters most to decision-making survives when movement becomes unreliable. This shifts emphasis from availability alone to continuity under stress.

For SOF, decision continuity restores confidence without reducing flexibility. Operators retain initiative while operating within clearly defined boundaries. They are empowered to act decisively without waiting for confirmation that may never arrive, while remaining aligned with commander intent and strategic constraints.

Taken together, this capability allows the space–cyber–SOF–STRATCOM nexus to function as intended. Each element contributes independently, but the combined effect is greater than the sum of its parts. Authority, data, and execution remain aligned even under disruption. Integration becomes resilient rather than brittle, and the enterprise retains decision advantage when access is contested or unreliable.

Why This Capability Has Not Emerged

The absence of decision continuity is not the result of neglect or ignorance. The problem has persisted because responsibility for authority, data, and delivery is distributed across systems, organizations, and processes that are rarely aligned by design.

Authoritative guidance is still treated primarily as policy, not as operational data. Rules of engagement, delegated authorities, and mission constraints are developed through deliberate processes that are approved at senior levels and distributed through briefings, documents, and message traffic. Once issued, they are assumed to be retrievable through reachback when clarification is required. That assumption holds only when access holds.

At the system level, mission tools are optimized for access and synchronization rather than continuity. Cloud-based architectures, dynamic updates, and real-time collaboration are valued because they increase speed and precision under normal conditions. Little incentive exists to design for prolonged degradation, especially when outages are treated as exceptional rather than expected.

Training reinforces these assumptions. Exercises are built to validate processes, not to stress them over time. Connectivity loss is introduced as a temporary inject, often resolved quickly to keep scenarios moving. Rarely are teams required to operate for days or weeks with partial data and no reachback, relying on preserved guidance rather than fresh updates. As a result, the force becomes proficient at operating with systems, but not at operating when systems only partially function.

There are also cultural barriers. Preserving authoritative guidance forward is sometimes viewed as risky. Concerns about outdated instructions, legal exposure, or loss of control lead organizations to prefer live clarification over pre-positioned authority. The unintended

consequence is that authority becomes brittle, disappearing precisely when it is needed most.

Finally, no single organization owns the problem. Space and cyber forces focus on access and resilience. SOF focus on execution and adaptability. STRATCOM elements focus on escalation management and global integration. Decision continuity sits between these seams. It is everyone's interest, but no one's explicit responsibility.

These factors explain why the decision continuity has not emerged organically. The gap persists not because it is unsolvable, but because it has not been framed as a technological and data problem with operational consequences. Once framed that way, it becomes addressable.

Building the Capability Through Training, Experimentation, and Use

Decision continuity will not emerge from doctrine alone, nor will it appear through policy refinement. It must be built, tested, and refined through how forces train and how systems are used in realistic conditions.[9] The most effective path forward does not begin with a program of record. It begins with deliberate experimentation at the operational and tactical level.

Exercises are the natural starting point. Most current training environments treat space and cyber effects as temporary disruptions. Communications go down briefly. Systems flicker. Play resumes once connectivity returns. This approach validates processes, but it does not build confidence when degradation is prolonged and uncertainty compounds. To develop decision continuity, exercises must impose longer periods of unreliable

To develop decision continuity, exercises must impose longer periods of unreliable access and require forces to operate through them without immediate restoration.

access and require forces to operate through them without immediate restoration.

This means forcing teams to rely on preserved guidance rather than reachback. Rules of engagement, delegated authorities, mission priorities, and abort criteria should be issued, updated, and then deliberately frozen at points during execution. Operators should be required to continue operating based on what remains available, not on what they hope to clarify later. The objective is not to induce failure, but to normalize decision-making when authoritative information is incomplete, outdated, or unreachable.

Technology experimentation should occur alongside training. Existing Blue Force systems provide a viable testbed. Rather than introducing new tools, the focus should be on how authoritative guidance is packaged, updated, and retained within those systems. Simple mechanisms that preserve the most current approved guidance at the moment access degrades can be tested, refined, and evaluated without significant infrastructure changes.

Critically, these experiments should be conducted with commanders involved. Decision continuity is not about delegating more authority by default. It is about making delegation explicit and survivable. Commanders must be able to see how preserved guidance is used, where it helps, and where it creates friction. Their feedback is essential to shaping how authority is expressed in a form that works under stress.

Joint and coalition exercises offer additional value. Differences in authorities, rules, and decision thresholds are often manageable when connectivity is strong. Under degraded conditions, those differences become fault lines. Training with preserved authoritative context allows partners to understand where boundaries lie and reduces the likelihood of hesitation or unintended escalation when access is limited. Simple mechanisms that preserve the most current approved guidance when access degrades, such as locking the last authorized version or retaining an approved snapshot, can be tested and refined without major infrastructure changes.

Over time, these training and experimentation efforts can inform requirements more effectively than abstract analysis. Patterns will emerge. Certain types of guidance will prove essential to preserve. Others will prove unnecessary. The goal is not to preserve everything, but to preserve what matters most at the moment of decision.

Building this capability will not eliminate uncertainty. It will not guarantee perfect decisions. What it will do is reduce hesitation, preserve tempo, and align authority with available data when systems degrade. That alignment is what allows the space–cyber–SOF–STRATCOM nexus to function as a true force multiplier rather than a fragile construct.

By treating authoritative mission context as operational data and ensuring it persists independently of access, the enterprise can preserve alignment between intent, authority, and execution even under disruption.

Conclusion

The space–cyber–SOF–STRATCOM nexus is designed to work, and, under normal conditions, it does. Each element brings formidable capability. Space enables global awareness and timing. Cyber delivers access and transport. SOF execute with precision forward. STRATCOM integrates these elements and manages strategic risk. The problem is not performance in ideal conditions, but fragility under degradation.

Modern operations assume persistent access. When that access becomes unreliable, mission data and decision context often disappear together. Operators retain the ability to act but lose confidence in what still applies. Decisions slow. Risk shifts upward. Tempo suffers. This outcome is not the result of poor judgment or insufficient training—it is the predictable consequence of systems and processes that were never designed to preserve authoritative context when connectivity degrades.

Building capability greater than the sum of its parts requires addressing this gap directly. Decision continuity provides a path forward. By treating authoritative mission context as operational data and ensuring it persists independently of access, the enterprise can preserve alignment between intent, authority, and execution even under disruption. This is not automation. It is not autonomy. It is a means of carrying command guidance forward when reachback is unavailable.

This capability cannot be delivered through doctrine alone. It must be tested where friction is real. Exercises must move beyond brief outages and scripted injects. Technology experiments must focus on preserving what matters most at the moment of decision, not on adding new layers of complexity. Commanders must be involved, not as approvers after the fact, but as participants shaping how authority is expressed and retained under stress.

> ***If the space–cyber–SOF–STRATCOM nexus is going to matter in the fight, it has to work when the network does not.***

Near-peer competitors understand that disruption does not need to be total to be effective. Inconsistent access, delayed updates, and uneven degradation are sufficient to create hesitation and friction. A force that depends on uninterrupted connectivity will struggle in that environment. A force that preserves decision continuity will not.

If the space–cyber–SOF–STRATCOM nexus is going to matter in the fight, it has to work when the network does not. The win condition is not better bandwidth. It is systems that keep the mission context current, then lock the last approved version when access degrades and put it in front of the team on the move. That is how integration stops being fragile and starts being an advantage.

About the Author

Ryan K. Kaono-Wedemeyer spent 30 years in the Department of Defense, serving as an Air Force Chief Master Sergeant and senior civilian with a career built around real-world operations. He worked alongside joint and coalition forces in Bosnia, Kosovo, and Iraq, supporting missions in military working dog operations and logistics where outcomes depended on speed, precision, and trust. His leadership experience includes assignments at intermediate headquarters, the Air Staff, and the F-35 Joint Program Office, giving him a ground-truth view of how decisions made at the top translate into effects on the line.

He is now the Chief Executive Officer of Romeo Kilo Defense Systems LLC, a defense technology firm focused on AI-enabled software built to support operators, preserve human judgment, and meet governance requirements inside zero-trust environments.

NOTES

1. Center for Strategic and International Studies (CSIS), *Competing Without Fighting: China's Gray Zone Strategy* (CSIS, 2020).
2. Joint Chiefs of Staff, *Cross-Domain Synergy in Joint Operations Planner's Guide* (Joint Staff, 2017), 1–3.
3. Government Accountability Office, *Defense Space Systems: Actions Needed to Improve Resilience of Positioning, Navigation, and Timing Capabilities* (GAO, 2022).
4. Department of Defense Chief Information Officer, *DoD Cloud Strategy* (DoD, February 2019).
5. Software Engineering Institute, Carnegie Mellon University, *A Framework for Designing Realistic Cyber Warfare* Exercises (SEI, 2017).
6. Department of Defense, *DoD Data Strategy* (DoD, 2020).
7. Department of Defense, *DoD Directive 5000.01, The Defense Acquisition System* (DoD, 2020), 2–4.
8. U.S. Strategic Command, *Congressional Posture Statement* (2025).
9. Department of Defense, *DoD Experimentation Guidebook v2.0* (2021).

Layered Global Presence and Twin Peaks: Aligning Special Operations Forces and Strategic Assets in Campaigns

By Lt. Col. Jaewook “Jay” Lee

Abstract

In an era of strategic competition, U.S. Special Operations Command (USSOCOM) must integrate its persistent U.S. special operations forces (SOF) global presence with high-end strategic assets, such as bombers, carrier strike groups, and submarines within combatant command campaign plans.

Analysis of the Korean Peninsula, Eastern Europe, and Indo-Pacific reveals that while both SOF and strategic peaks recur, they are rarely framed explicitly as synchronized elements of geographic combatant command (GCC) -led regional campaigns. Instead, they often appear in parallel narratives, SOF partnership-building versus strategic deterrence, missing opportunities for mutual reinforcement.

The three key findings derived from the analysis are:

1) Layered presence—combining persistent SOF, episodic twin peaks, and narrative layer—delivers more sustained and flexible effects than post-chase operations reliant on a single layer.

2) SOF-centric surges and strategy-centric deployments are most effective when operating as twin peaks within combatant command campaign plans (CCPs).

3) Due to differences between theaters and global constraints, common principles must be applied regionally and contextually.

Practical design principles, including co-posture nodes and integrated planning steps, would treat SOF and strategic assets as complementary campaign peaks rather than isolated efforts.

By aligning CCPs with USSOCOM and United States Strategic Command (USSTRATCOM) -led functional campaign plans through this twin-peaks logic, the joint force can achieve greater deterrence

Analysis of the Korean Peninsula, Eastern Europe, and Indo-Pacific reveals that while both SOF and strategic peaks recur, they are rarely framed explicitly as synchronized elements of geographic combatant command-led regional campaigns.

credibility, partner confidence, and global posture resilience without new authorities or resources.

Introduction

USSOCOM was created to provide globally responsive SOF that can operate persistently in competition as well as in conflict. In today's era of longterm strategic competition, SOF presence can no longer be viewed in isolation from the joint force. Presence must be understood as part of a layered, campaign-driven architecture in which SOF, strategic assets, and non-physical tools are combined to shape regional environments and support global objectives.[1]

Recent U.S. concepts emphasize integrated deterrence and campaigning, calling for the coordinated use of all instruments of national power, including military capabilities below the threshold of armed conflict.[2] GCCs are responsible to CCPs that blend conventional forces, SOF, and strategic capabilities in support of theater objectives. Meanwhile, functional combatant commands such as USSOCOM and USSTRATCOM lead functional campaign plans (FCPs) in their respective domains: global SOF operations on one hand and global deterrence and strike on the other.[3] Within these overlapping efforts, SOF typically provide a human and networked layer of presence; strategic assets such as bombers, carrier strike groups (CSGs), and submarines provide high-end presence; and narrative tools link these actions into a coherent story over time.[4]

The layered and twin-peaks perspective on global presence helps make sense of this complexity. The layered aspect distinguishes among persistent SOF engagement, episodic physical concentrations of capability, and a narrative layer that gives those actions meaning across audiences.[5] The twin-peaks aspect highlights that episodic presence is not solely about strategic asset deployments; it often takes the form of paired peaks within a CCP: SOF-centric surges such as major combined special operations exercises or cooperation milestones and strategy-centric peaks, such as bomber task force (BTF) and CSG or submarine visits. When these two types of peaks are deliberately designed to occur within the same GCC-led CCP timeline and are supported by a coherent narrative, they can generate effects greater than either could achieve alone.[6]

Answering the *Special Operations Research Topics 2026* topic 43 "SOF Global Presence," the purpose of this study is to explore how USSOCOM can better integrate its persistent presence and SOF-centric peaks with strategy-centric peaks and narrative tools inside GCC-led CCPs, and how those regional CCPs can in turn support FCPs led by USSOCOM and USSTRATCOM.[7] The structure of the campaign plans, which follows the sequence JSCP-GCP-FCP-CCP, is cited from *CJCSI 3100.01F Joint Strategic Planning System* (2024).[8] Using three archetypal theaters, the Korean Peninsula, Eastern Europe, and Indo-Pacific, illustrates how different threat environments, alliance structures, and geographies shape the design of layered presence.

Recent U.S. concepts emphasize integrated deterrence and campaigning, calling for the coordinated use of all instruments of national power, including military capabilities below the threshold of armed conflict.

Three questions guide the analysis. First, how do persistent SOF, episodic twin peaks, and the narrative layer interact within CCPs? Second, how can SOF-centric and strategy-centric peaks be more deliberately designed as twin peaks rather than separate planning streams? Third, how can CCPs and FCPs be better aligned so that theater posture contributes coherently to global messaging?

Conceptual Foundations: Layered Presence, Twin Peaks, and Command Roles

U.S. Special Operations Command's Global Presence Mandate

Global presence has always been central to USSOCOM, but what "presence" means has evolved. In the post-9/11 era, presence was often equated with where SOF units were deployed and how many operations they were conducting. In today's strategic competition, presence is better understood as how SOF contribute to a joint and combined posture that can shape, deter, and, if necessary, fight across multiple theaters over long periods.[9]

Within this context, USSOCOM's mandate is to provide globally integrated, ready, and networked SOF that operate forward, persistently, and with partners in support of GCCs and the joint force. SOF are expected to compete below armed conflict, expand decision space for senior leaders, and prepare the environment so that other elements of U.S. power can be applied more effectively.[10] This requires distributed, often low-visibility engagement such as unconventional warfare, foreign internal defense, civil affairs, and military information support operations that builds relationships and understanding over time. For planners, the key questions are where such persistent SOF presence is most needed and how it should adapt as the environment changes.[11]

Crucially, USSOCOM does not operate in a vacuum. Its global presence must fit within GCC-led CCPs and functional constructs overseen by other combatant commands, including USSTRATCOM.[12] While USSOCOM can sustain a unique form of persistent engagement, its activities are most effective when aligned with conventional forces and strategic capabilities such as strategic bombers or submarines that lie outside its chain of command.[13] Understanding how SOF presence interacts with these other elements is therefore essential to thinking clearly about "global presence."

Three Layers of Presence: Persistent, Episodic, and Narrative

To see how SOF and strategic assets can be combined within campaigns, it is useful to distinguish three layers of presence: persistent, episodic, and narrative. These layers are different ways the U.S. makes itself present in a region and in audience perceptions. Thinking in layers helps planners combine SOF, strategic assets, and narrative mechanisms into a coherent architecture instead of managing them as separate efforts.[14]

Persistent presence refers to forces and activities that are in or engaged with a theater continuously or nearly so. For SOF, this includes forwardbased units, long-term liaison elements, recurring advisory, and training that builds enduring relationships. Persistent presence is valuable for understanding local dynamics, shaping partner capabilities, and building trust that cannot be generated quickly in a crisis.[15] Furthermore, the forward presence not only enhances deterrence by improving the ability to act rapidly but also demonstrates the political will and resolve of the U.S., thereby maximizing the credibility of the 'costs' it can impose on adversaries.[16] However, its limitations lie in scale and visibility: SOF elements are typically small and discreet and not designed

In today's strategic competition, presence is better understood as how SOF contribute to a joint and combined posture that can shape, deter, and, if necessary, fight across multiple theaters over long periods.

to provide the large-scale strategic signaling that high-end forces can deliver.[17]

Episodic presence encompasses deployments and activities that occur at intervals for signaling or concentrated operational effect. These include strategic deployments, BTF, CSG patrols, and submarine visits, as well as major combined exercises and other time-bound surges by SOF. Episodic presence offers high visibility and can send powerful deterrence signals under realistic conditions. It is also resource intensive and can appear disjointed if not connected to a larger campaign.[18]

The narrative layer consists of the virtual tools and communication mechanisms that connect physical actions into a coherent story. They frame how allies, adversaries, and domestic audiences interpret persistent engagement and episodic events: explaining why a particular exercise or deployment matters, how it relates to previous efforts, and what it signals about future intent.[19] In this sense, narrative layer is less about being everywhere online and more about providing the connective tissue and storyline that turns individual actions into recognizable chapters in a campaign.

When combined, these three layers suggest simple planning logic (see Fig. 1). Persistent SOF presence builds human networks that make episodic actions more meaningful and less risky; episodic actions provide visible demonstrations and stress tests that validate the foundations built over time; and the narrative layer ties them

together, ensuring that they are understood as parts of the same CCPs and FCPs rather than as isolated reactions.

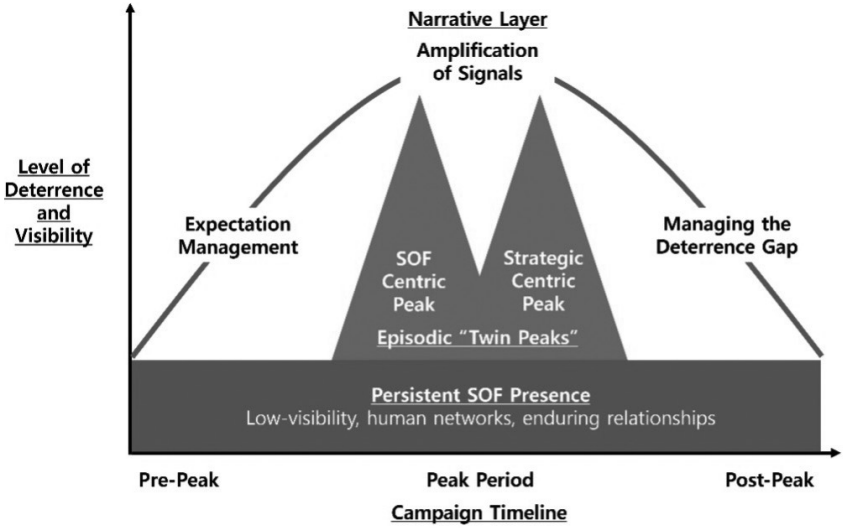


Figure 1. The Layered Presence and Twin Peaks Model.
Source: Developed by the author

Strategic Asset Deployments and Special Operations Forces Surges as Episodic Twin Peaks

Within the episodic layer, presence manifests through two distinct but complementary "peaks": strategy-centric peaks, generated by the deployment of high-end assets like bombers, CSG, and submarines; and SOF-centric peaks, characterized by surges in special operations activity such as major combined exercises or partner capability milestones.[20] While these events often occur within the same theater, they are frequently managed as separate planning streams.

However, the relationship is best understood as a complementary symbiosis rather than a functional hierarchy. Strategic assets deliver high-intensity deterrence signals and visibility but are not designed

for deep regional context or long-term trust building.[21] Conversely, SOF specialize in persistent human networks and situational understanding but lack the overwhelming visual impact of strategic assets such as CSGs.[22]

By treating these as twin peaks within a single campaign timeline, planners can sequence them to maximize synergy. For instance, a SOF-centric surge can build the necessary access and interoperability. A subsequent strategic deployment then validates and dramatizes this progress under realistic conditions.[23]

The narrative layer is what turns these twin peaks into a campaign. On their own, a large SOF exercise or a BTF can be perceived as a one-off event. Narrative tools such as coordinated messaging become most important when they explain how a SOF surge set conditions for a strategic deployment, or how a strategic deployment is linked to the quieter work of building local capacity. By framing twin peaks as connected chapters (before, during, and after they occur), the narrative layer gives them meaning in the perceptions of all audiences, allies, and adversaries.[24]

For USSOCOM and its partners, the implication is that episodic presence should be conceptualized not only in terms of what is deployed but also in terms of how SOF-centric and strategy-centric peaks are paired.[25] Strategic deployments remain primarily under USSTRATCOM and the services; SOF surges are shaped by USSOCOM. Recognizing them as twin peaks within CCPs by GCCs and using the narrative layer to bind them into a single story sets the stage for a more integrated approach to campaign design and global posture.[26]

By treating these as twin peaks within a single campaign timeline, planners can sequence them to maximize synergy.

Roles of U.S. Special Operations Command, U.S. Strategic Command, and Geographical Combatant Commands in Layered Presence

Global presence is the product of multiple commands exercising overlapping authorities. USSTRATCOM is responsible for strategic deterrence and global strikes, and it plans, commands, and controls the strategic assets that form the backbone of deterrence. GCCs are responsible for specific theaters, integrating conventional, special operations, and strategic activities into CCPs that support national objectives. USSOCOM provides globally integrated SOF capabilities, synchronizes special operations across theaters, and leads global SOF campaigning in support of national objectives.[27]

At the regional or theater level, campaigns are GCC-led CCPs. Within these CCPs, SOF provide the human and networked layer of presence; strategic assets provide a high-end layer; and the narrative layer ties these actions together for regional audiences. SOF-centric surges and strategy-centric deployments can thus be seen as twin peaks within the same CCPs, rather than as separate efforts. The GCC's role is to design and sequence these peaks so they support coherent theater objectives, taking into account political constraints, partner sensitivities, and the broader joint posture.[28]

At the global level, USSOCOM and USSTRATCOM can each lead FCPs that cut across theaters. USSOCOM leads a global SOF campaign focused on competition and network development while USSTRATCOM leads a global deterrence and strike campaign centered on strategic forces and associated signaling. GCCs then implement and adapt these global campaign plans and FCPs in their theaters, aligning regional posture with global and functional guidance. In this construct, presence and campaigning are multilayered: CCPs host SOF and strategic peaks and employ the narrative layer locally while USSOCOM-led and USSTRATCOM-led

Treating layered presence, persistent SOF, episodic twin peaks, and the narrative layer, as a shared design problem at both regional and global levels provides a common logic for aligning SOF, strategic assets, and messaging.

global efforts provide overarching direction for how those peaks and narratives should be used.[29]

This means USSOCOM does not "own" strategic assets, and USSTRATCOM does not manage SOF—but both have a stake in how their tools are integrated into the contributing global posture of CCPs and FCPs. If strategic deployments are planned without reference to ongoing SOF contributions and without a narrative that links them, opportunities to reinforce partnerships and amplify influence may be missed. Conversely, SOF posture and campaigning that ignore the potential of strategic deployments risk underutilizing some of the most powerful instruments available to the joint force. Treating layered presence, persistent SOF, episodic twin peaks, and the narrative layer, as a shared design problem at both regional and global levels provides a common logic for aligning SOF, strategic assets, and messaging.[30]

Regional Applications: Layered Presence and Implicit Twin Peaks

Having outlined a layered and twin-peaks approach to global presence and clarified the respective roles of USSOCOM, USSTRATCOM, and the GCCs, it is useful to see how this framework manifests in theaters. This section applies the persistent–episodic–narrative lens, and the notion of SOF-centric and strategy-centric peaks, to three regions frequently highlighted in U.S. strategy: the Korean Peninsula, Eastern Europe, and the broader Indo-Pacific.

The Korean Peninsula: Dense Posture and High-Intensity Signaling

The Korean Peninsula is a prime theater where high-density forward deployment and heightened crisis potential coexist. A combined defense structure between the U.S. and Republic of Korea (ROK) is established in Korean Peninsula, within the range of short-range missiles while confronting North Korea, which possesses nuclear and missile capabilities.[31] This necessitates a very robust deterrence and defense posture combining permanent forward deployment, a combined defense structure, and high-frequency combined training.[32]

Persistent SOF presence is realized through close cooperation with ROK SOFs, joint planning, and combined training. These activities are integrated within the frameworks of U.S. Forces Korea (USFK), U.S. Special Operations Command Korea (SOCKOR), and the broader ROK–U.S. combined defense structure. This provides a foundation of detailed understanding of the terrain, targets, and social environment, as well as trust and interoperability for rapid combined operations during crisis.[33]

Episodic peaks are particularly evident in the deployment of strategic assets. Deployments of B-52/B-1B bombers, CSG, and submarines are repeatedly conducted in conjunction with North Korean provocations or major summit meetings/declarations, forming strategy-centric peaks that enhance the visibility of extended deterrence.[34] Simultaneously, during large-scale combined exercises like Exercise Freedom Shield, SOF-centric surges occur where ROK-U.S. SOF train direct actions, special reconnaissance, countering weapons of mass destruction, time-sensitive target seizure, etc., creating peaks in readiness and interoperability in non-visible domains.[35]

The narrative layer should serve to weave these peaks into a single alliance story. Joint press releases and messages directed

at North Korea and domestic audiences frame the deployment of strategic assets and SOF training not as "separate events" but as interconnected scenes within the same deterrence and assurance campaign.[36] However, at the public level, the strategic asset peak tends to be described primarily in terms of extended deterrence, while the SOF peak is often framed around special operations readiness (see Fig. 2). As a result, explicit framing of the intended twin peaks remains limited.[37]



Figure 2. Examples of applications for episodic twin peaks in the Korean Peninsula. (From left): U.S. and Republic of Korea special operations forces conduct routine air assault training at Baengnyeong-Do. Source: DVIDS, photo by Staff Sgt. Daniel Lee; U.S. Air Force Global Strike Commands. Source: U.S. Air Force; South Korean navy sailors welcome the Los Angeles-class submarine USS Annapolis to Jeju Naval Base. Source: *Stars and Stripes*, photo courtesy of South Korean Ministry of National Defense

Eastern Europe: Multinational Deterrence and Rotational Presence

Eastern Europe is a theater combining a multilateral alliance structure, potential for ground warfare, and a deterrence posture centered on rotational deployments. Following Russia's invasion of Ukraine and its coercion of neighboring countries, NATO has expanded forces, equipment, and training to strengthen its eastern front. Rotational deployments and continuous training are key, rather than permanent stationing, and all activities require coordination among numerous allies.[38]

Persistent SOF presence manifests through cross-border networking via training, advising, joint exercises, and liaison activities with various allied SOF. These low-visibility, multinational SOF

activities form a background layer enhancing resilience against gray-zone threats and hybrid warfare while strengthening interoperability with NATO forces in contingencies.[39]

Episodic peaks occur on both axes. Large-scale NATO exercises like Steadfast Noon and Astral Knight, along with some BTFs, represent strategy-centric peaks. They demonstrate rapid reinforcement capabilities and nuclear capabilities, performing deterrence and assurance.[40] SOF-centric peaks are formed through multinational special operations training and exercises, focusing on enhancing partners' special operations capabilities and developing common tactics and doctrine.[41]

The narrative layer should position these peaks as part of the Alliance's deterrence and defense campaign through NATO statements, public affairs activities, and information-sharing. Nevertheless, public explanations tend to treat strategic assets and large-scale exercises primarily within the context of conventional/strategic deterrence, while addressing SOF activities separately within the context of special operations and partnership enhancement (see Fig. 3). Language consistently weaving the SOF surge and strategic asset deployment as twin peaks on a CCPs timeline, prominently featuring the concept, is still in its formative stages.



Figure 3. Examples of applications for episodic twin peaks in the Eastern Europe. (From left): NATO special operations forces secure the Baltic. Source: DVIDS, photo by Petty Officer 1st Class Trey Hutcheson; NATO Secretary General Mark Rutte standing in front of a Dutch F-35 fighter jet at Volkel Air Base, the Netherlands. Source: NATO; USAF Global Strike Command. Source: U.S. Air Force

The Indo-Pacific: Distribution, Distance, and Maritime Focus

The Indo-Pacific is characterized by vast distances, a maritime-centric operational environment, and allies and partners with varying threat perceptions and capabilities. Due to anti-access/area denial, gray-zone maritime coercion, and the need for wide-area dispersed operations, the U.S. and its allies are pursuing a more dispersed and resilient presence.[42]

Persistent SOF presence is realized through small teams dispersed across island and coastal nations, working alongside partner SOF to enhance maritime special operations capabilities and counter-coercion resilience. This builds trust and situational awareness for crisis response, but the sheer geographic expanse makes the very location of permanent SOF presence a strategic choice.[43]

The strategy-centric axis of episodic peaks is handled by the deployment of CSG, submarine, and BTF, and large-scale joint/combined exercises. These are high-visibility peaks demonstrating the ability to project power across broad areas and operate within contested zones.[44] SOF-centric peaks manifest through SOF exercises, special operations-linked maritime interdiction training, and establishing new forward operating bases, intensively building the human and infrastructure foundation for dispersed deterrence and operations.[45]

The narrative layer positions these peaks within the long-term story of a "free and open Indo-Pacific" through strategic documents, joint statements, and public affairs/strategic communications with allies and partners.[46] However, in public materials, the deployment of naval and air forces and strategic assets is often presented as one narrative thread, while SOF cooperation form another, meaning the twin peaks concept is not explicitly articulated (see Fig. 4). In

this theater where distributed and multi-domain operations are emphasized, designing and articulating SOF-centric and strategy-centric peaks as twin summits on the same campaign timeline appears to be the area where the greatest additional effect can be achieved.



Figure 4. Examples of applications for episodic twin peaks in the Indo-Pacific. (From left) U.S. Air Force Special Tactics operators with the 23rd Special Tactics Squadron. Source: U.S. Army; Bomber Task Force operations in the Indo-Pacific area of responsibility. Source: DVIDS, U.S. Air Force photo by Senior Airman Samantha White; U.S. Indo-Pacific Command joint force conducts dual carrier operations in South China Sea. Source: U.S. Navy Press Office

CrossCase Findings on Layered Presence and Implicit Twin Peaks

Comparing the three theaters, the fundamental logic of layered presence is common. Persistent SOF presence provides the foundation for networks and understanding; SOF-centric and strategy-centric episodic peaks concentrate effects at specific points in time; and the narrative layer weaves all these activities into the story of a single CCP or FCP.[47] The better the alignment between these layers, the greater the reliability and flexibility of deterrence and assurance.

The global force projection capability which formed by combining SOF and strategic assets into episodic peaks is a critical tool for the joint force commander. It enhances the capacity to influence an adversary's decision-making through three primary ways: imposing costs, denying benefits, and encouraging restraint.[48]

Simultaneously, each theater demands different equilibrium points. The Korean Peninsula, due to its forward deployment and high crisis potential, sees frequent and sensitive strategy-centric peaks, while SOF-centric peaks focus on preparing for high-intensity combined operations. Eastern Europe emphasizes coordination and alliance cohesion within multilateral structures, rotational deployments, and hybrid threat environments, where SOF acts as the glue binding diverse partners. The Indo-Pacific, due to vast distances, a maritime focus, and the need for dispersed operations, demands a highly distributed SOF presence coupled with the wide-area power projection of strategic assets.

While SOF-centric and strategy-centric peaks exist across all three theaters, publicly available materials rarely consistently design or describe them as intended twin peaks within a CCP. Although numerous doctrines and strategic concepts advocate for the integration of narratives,[49] the actual phenomenon at the public level across all three theater cases appears to be quite the opposite. Deployment of strategic assets and SOF surges are typically explained within separate, compartmentalized narratives: strategic deterrence versus special operations. This gap is precisely where the twin-peaks framework can contribute. By introducing language that views the SOF-centric and strategy-centric peaks as twin summits connected by time, space, and message within the same CCPs and FCPs, USSOCOM, USSTRATCOM, and GCCs could secure additional synergies in deterrence, assurance, and influence simply by realigning existing activities.

While SOF-centric and strategy-centric peaks exist across all three theaters, publicly available materials rarely consistently design or describe them as intended twin peaks within a command campaign plan.

Integrating Twin Peaks Into Campaign Plans

The challenge for USSOCOM is not controlling strategic assets but rather becoming more actively involved in designing when, where, and within what narrative the SOF-centric peak and strategy-centric peak should appear together.

Practically, when planning strategic asset deployments, an approach is needed that first asks, "At what point in the current theater campaign and SOF activities will this deployment create a twin peak?" Conversely, when planning surges, training, or capability rollouts above a certain level, SOF must consider whether a strategy-centric peak can be added at this point, or at least how to connect it narratively. The more USSOCOM articulates its requirements in this campaign language, the more likely USSTRATCOM and GCC recognize SOF postures as critical design variables on par with strategic asset operations.

Posture Design Principles and Co-Posture Nodes

To intentionally create twin peaks, several fundamental principles must be incorporated into the post-deployment design.

First, treat all SOF-centric and strategy-centric major events as "campaign peaks." Rather than isolated training or deployments, this approach involves first determining which point on the theater campaign timeline serves as the apex, then designing what form of peak SOF and strategic assets each creates.50 For example, create an SOF-centric peak first, then layer strategic asset deployment onto that point to demonstrate "how the capabilities prepared thus far actually provide support."[51]

Second, designate and develop co-posture nodes where SOF and strategic assets can operate together. Intentionally select locations where both the permanent presence of SOF[52]

and episodic deployment of strategic assets are feasible, then enhance their facilities, protective posture, and C2 capabilities.[53] Regularly conducting SOF training and strategic asset deployments together or consecutively at these nodes not only facilitates implementing twin peaks but also validates the infrastructure and procedures needed during actual crisis. The designation of co-posture nodes is not merely a logistical convenience; it is a strategic requirement for deterrence platforms in contested environments.

Third, adjust the weighting of layer composition to reflect theater-specific conditions and global demand. Not every theater can frequently receive strategic assets, nor can every partner sustain high SOF density. Therefore, strategic choices are required. Some theaters should prioritize a persistent SOF presence. Others might combine an SOF-enabled network with relatively infrequent strategy-centric peaks to create major deterrence events.[54] Crucially, SOF and strategic asset postures must be integrated and coordinated at the GCC level to avoid separate logics.[55]

Fourth, incorporate the information and narrative dimensions into the twin peaks design from the outset. Strategic asset deployment automatically generates narratives through photos, videos, and press releases/announcements. SOF activities are intentionally low visibility but can be selectively revealed when necessary. It is crucial to preemptively frame messages and develop explanatory strategies for partners and domestic audiences so both peaks are perceived as part of the same story. This role falls to the narrative layer which must approach the task not as simple publicity but closer to campaign storytelling.[56]

Toward an Integrated Presence and Campaign-Planning Framework

To incorporate these elements into operational planning, a simple framework can be proposed for use by GCCs, USSTRATCOM, and USSOCOM. The purpose of this framework is not to create a new command structure but to align thinking to view the layers, peaks, and narrative simultaneously.

At the CCP level, it can be summarized in four steps:

1) Identify problems, partners, and key points.
GCC and SOF jointly identify highly contested points within the theater, critical partners, and strategic chokepoints.[57]

2) Design the persistent layer.
Determine where to place which SOF and other forces on a persistent or semi-persistent basis, and which partner capabilities to develop and in what sequence.[58]

3) Design twin peaks.
Determine when and where to create SOF-centric and strategy-centric peaks on the timeline of the CCPs and how to pair them within feasible constraints. Coordinate with USSTRATCOM, find strategic asset availability and risks at this stage.[59]

4) Design narrative layer.
Plan how to communicate the actions determined in the above three steps—what story to tell, to which audience, and in what sequence. This includes pre-peak, peak-period messaging, and post-peak follow-up narratives.[60]

The same logic can be applied to USSOCOM and USSTRATCOM FCPs. USSOCOM FCPs with SOF identify which theaters require which types of SOF-centric peaks and what persistent postures are essential, while USSTRATCOM FCPs for global deterrence and strike

campaigns prioritize the theaters, timing, and form of strategy-centric peaks. In this alignment process, theater special operations commands (TSOCs) act as the critical connective tissue.[61] TSOCs, such as SOCKOR, SOCEUR, SOCPAC, serve as critical regional hubs. They physically and conceptually link the global objectives of USSOCOM's FCPs with the regional execution of the GCC's CCP twin peaks. GCCs can adapt this to their own CCPs, enhancing the realism of FCPs by providing USSOCOM and USSTRATCOM with feedback on actual twin peaks and narrative design experiences.[62]

The value of this framework lies not in introducing new concepts but in making existing elements visible at a glance. When GCC, USSOCOM, and USSTRATCOM begin treating persistent SOF, episodic twin peaks, and narrative layers as a single campaign design problem, rather than optimizing them separately, they can achieve more consistent deterrence, assurance, and competitive effects with the same resources.

Conclusion: Implications and Recommendations

Global presence in the era of strategic competition is not the deployment of a single tool but rather a structure composed of layers and campaigns. Persistent SOF provide the human and network foundation, episodic twin peaks deliver concentrated effects, and the narrative layer connects and explains these two. Analysis of three theaters, the Korean Peninsula, Eastern Europe, and the Indo-Pacific, reveals these layers are already partially utilized. However, the design of SOF-centric and strategy-centric peaks as intended twin summits within GCC-led CCPs, and their systematic linkage to global SOF and strategic FCPs, remains implicit.

From the USSOCOM perspective, SOF and strategic assets are independent functions contributing to a joint campaign. Persistent SOF provide the foundation-enabling peaks; strategic assets deliver

visible, high-intensity signals; and the narrative layer weaves all these actions into a continuous story conveyed to allies, adversaries, and domestic audiences. The key challenge is to view these layers and peaks not as separate efforts but as integrated design elements within regional and global campaigns.

Three key findings derived are as follows:

1) Layered presence, such as combining persistent SOF, episodic twin peaks, and narrative layer delivers more sustained and flexible effects than post-chase operations reliant on a single layer. A pattern emerges where reliability in deterrence and assurance increases when physical activities and narrative connections align well across all three layers.

2) SOF-centric surges and strategy-centric deployments are most effective when operating as twin peaks within a CCP. Each peak holds independent significance, but synergy is maximized when time, space, and message converge.

3) Due to differences between theaters and global constraints, common principles must be applied regionally and contextually. Simultaneously, bidirectional coordination is necessary: USSOCOM and USSTRATCOM's FCPs provide functional direction for CCPs, while GCC's regional experience informs global priorities. TSOCs can act as a hub in these processes.

USSOCOM and joint forces can take specific actions to apply this finding to operational practice.

1) Incorporate the layered presence and twin peaks perspective into theater posture reviews and campaign design. Require CCPs to explicitly describe how persistent SOF, SOF-centric/strategy-centric peaks, and the narrative layer are integrated. This allows

USSOCOM to present SOF contributions as core elements of CCP design rather than as separate requirements.

2) Plan SOF-centric and strategy-centric peaks not as independent but as complementary events. Establish regular planning forums between USSOCOM, USSTRATCOM, and TSOCs to coordinate how SOF surges and strategic asset deployments interlock within the campaign timeline.

3) Designate and develop co-posture nodes where SOF and strategic assets can operate together. Select locations capable of supporting both routine SOF operations and episodic strategic asset deployments. Enhance facilities, protection, and C2 at these nodes. Conduct regular SOF training and strategic asset deployments at these nodes in a continuous or parallel manner to test twin peaks.

These measures do not require new authority or structural reorganization. USSOCOM simply needs to share a common language—layered presence, twin peaks, narrative—with USSTRATCOM, and GCCs with TSOCs, and add a question about layers, peaks, and narrative to existing planning processes. This approach enables more consistent deterrence, assurance, and competitive effects with the same resources, allowing for more effective design and operation of global presence in the era of strategic competition.

About the Author

Lt. Col. Jaewook "Jay" Lee is a Republic of Korea (ROK) Army functional area officer specialized in strategy and a special forces-qualified officer. He brings a unique blend of tactical execution and strategic planning to his work. Following his voluntary participation in Operation ENDURING FREEDOM in 2011, he commanded ROK special forces and special mission units at various levels. Transitioning to strategic roles, he served in the C5 Strategy Division of the ROK-U.S. Combined Forces Command and the J5 Strategy and Plans Division, Countering Weapons of Mass Destruction Directorate of the ROK Joint Chiefs of Staff. His research focuses on the intersection of special operations, extended deterrence, and conventional-nuclear integration within the context of the U.S.-ROK alliance and broader Indo-Pacific security.

Notes

1. *2018 United States Special Operations Command Posture Statement, Before the House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities*, 115th Congress (2018) (Statement Of General Raymond A. Thomas, III, U.S. Army Commander United States Special Operations Command), 3–4, https://www.socom.mil/Documents/Posture%20Statements/2018%20USSOCOM%20Posture%20Statement_HASC%20Final.pdf.; United States Special Operations Command, SOF Renaissance: People, Win, Transform (United States Special Operations Command, 2025), 14–15, https://www.socom.mil/Documents/2025-SOF_Renaissance(25FEB)Web.pdf; James E. Cartwright et al., *Operationalizing Integrated Deterrence: Applying Joint Force Targeting across the Competition Continuum*, Atlantic Council, June 8, 2023, 4–5, https://www.atlanticcouncil.org/in-depth-research-reports/report/operationalizing-integrated-deterrence-evolving-the-joint-forces-application-of-targeting-across-the-competition/.

2. Jonathan Schroden, "Competition Campaigning: What It Looks Like and Implications for US Special Operations Command," *Modern War Institute at West Point*, January 20, 2023, https://mwi.westpoint.edu/competition-campaigning-what-it-looks-like-and-implications-for-us-special-operations-command/.

3. Joint Chiefs of Staff, CJCSI 3100.01F: Joint Strategic Planning (Joint Chiefs of Staff, January 29, 2024), D-2–D-4, https://www.jcs.mil/Portals/36/Documents/Library/Instructions/CJCSI%203100.01F.pdf.

4. Thomas, testimony on *2018 United States Special Operations Command Posture Statement, 19; Before the Subcommittee on Strategic Forces, Senate Armed Services Committee*, 119th Congress, 1st session (2025) (Statement of Anthony J. Cotton, Commander, United States Strategic Command), 18–19, https://www.armed-services.senate.gov/imo/media/doc/testimony_of_general_anthony_jcotton1.pdf.

5. United States Special Operations Command, *SOF Renaissance*, 10; *Joint Chiefs of Staff, Joint Publication 3-13.2: Military Information Support Operations* (December 20, 2011), I–2. https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1C1_JP_3-13-2.pdf.

6. Cartwright et al., *Operationalizing Integrated Deterrence*, 4.; Chad Pillai, "Developing a Combatant Command Campaign Plan: Lessons Learned at US Central Command," Modern War Institute at West Point, June 16, 2021, https://mwi.westpoint.edu/developing-a-combatant-command-campaign-plan-lessons-learned-at-us-central-command/.

7. United States Special Operations Command, *SOF Renaissance*, 14–15; Cotton, testimony *Before the Subcommittee on Strategic Forces, Senate Armed Services Committee*, 21.

8. Joint Chiefs of Staff, *CJCSI 3100.01F: Joint Strategic Planning System*, D-2–D-4.

9. Clementine G. Starling and Alyxandra Marine, *Stealth, Speed, and Adaptability: The Role of Special Operations Forces in Strategic Competition*, Atlantic Council, March 7, 2024, 5, 10–12, https://www.atlanticcouncil.org/in-depth-research-reports/report/starling-marine-special-operations-forces-in-strategic-competition/; United States Special Operations Command, *SOF Renaissance*, 4–5.

10. United States Special Operations Command, *2025 Fact Book* (United States Special Operations Command, 2025), 8. https://www.socom.mil/FactBook/2025%20Fact%20Book.pdf.; Starling and Marine, *Stealth, Speed, and Adaptability*, 16–17.; *Statement for the Record, Before the Senate Armed Services Committee*, 119th Congress (2025)(Statement of Deputy Assistant Secretary of Defense Colby Jenkins and General Bryan P. Fenton, Commander, United States Special Operations Command), 1, 6, https://www.armed-services.senate.gov/imo/media/doc/general_fulton_joint_opening_statement_with_mrcolbyjenkins.pdf.

11. Starling and Marine, *Stealth, Speed, and Adaptability*, 6–7, 12; Lauren Hickok and Larson Miller, "Strategy for a New Era: USSOCOM Takes on Strategic Competition," *Inter Populum: The Journal of Irregular Warfare and Special Operations* 2, no.1 (2024): 30, 32–33, https://interpopulum.org/strategy-for-a-new-era-ussocom-takes-on-strategic-competition/.

12. Jenkins and Fenton, testimony *Statement for the Record, Before the Senate Armed Services Committee*, 13; Michael D. Tisdel, Ken D. Teske, and William C. Fleser, *Theater Special Operations Commands Realignment* (United States Special Operations Command, 2014), 4–6, https://ntrl.ntis.gov/NTRL/dashboard/searchResults/titleDetail/ADA607289.xhtml.

13. Starling and Marine, *Stealth, Speed, and Adaptability*, 18.

14. Cartwright et al., *Operationalizing Integrated Deterrence*, 4–5; Joint Chiefs of Staff, *Design and Planning* (Joint Chiefs of Staff J7, 2013), 2–3.

15. Maurice "Duc" DuClos, "Closing the GAP: Strategic Presence Through Embedded U.S. Military Advisors," *Strategy Central*, June 26, 2025, https://www.strategycentral.io/post/closing-the-gap-strategic-presence-through-embedded-u-s-military-advisors.

16. United States Department of Defense, *Deterrence Operations Joint Operating Concept* (Department of Defense, 2006), 33–34, https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joc_deterrence.pdf.

17. Starling and Marine, *Stealth, Speed, and Adaptability*, 5–6.

18. Pillai, "Developing a Combatant Command Campaign Plan."

19. United States Department of Defense, *Deterrence Operations Joint Operating Concept*, 42–43; Jeremiah "Lumpy" Lumbaca, "Imagining the Near-Future of American Irregular Warfare in the Indo-Pacific," *Small Wars Journal* (2025), https://smallwarsjournal.com/2025/06/18/imagining-iw-in-the-indo-pacific/.

20. Cotton, testimony *Before the Subcommittee on Strategic Forces, Senate Armed Services Committee*, 21; United States Special Operations Command, *2025 Fact Book*, 23–24; Lee Willett, "US Navy Carrier High North Deployment Points to NATO Deterrence Impact of CSG Presence," *Naval News*, September 24, 2025, https://www.navalnews.com/naval-news/2025/09/us-navy-carrier-high-north-deployment-points-to-nato-deterrence-impact-of-csg-presence/.

21. United States Department of Defense, *Deterrence Operations Joint Operating Concept*, 39–41.

22. DuClos, "Closing the GAP: Strategic Presence Through Embedded U.S. Military Advisors."

23. United States Special Operations Command, *SOF Renaissance*, 18–19; United States Army, *TRADOC Pamphlet 525-3-1: The U.S. Army in Multi-Domain Operations 2028* (U.S. Army Training and Doctrine Command, 2018), 20–21, https://www.army.mil/article/243754/the_u_s_army_in_multi_domain_operations_2028.

24. United States Department of Defense, *Deterrence Operations Joint Operating Concept*, 42–43; Joint Chiefs of Staff, JP 3-13.2: *Military Information Support Operations*, I-4–I-5.

25. Monte Erfourth, "SOF Competitive Campaigning in Great Power Competition," *Strategy Central*, January 24, 2025, https://www.strategycentral.io/post/sof-competitive-campaigning-in-great-power-competition; Cotton, testimony *Before the Subcommittee on Strategic Forces, Senate Armed Services Committee*, 18–19.

26. United States Department of Defense, *Department of Defense Directive 5132.03: Department of Defense Policy and Responsibilities Relating to Security Cooperation* (Department of Defense, 2016), 3, 13. https://open.defense.gov/portals/23/documents/foreignasst/dodd_513203_on_security_cooperation.pdf; United States Special Operations Command, *SOF Renaissance*, 14–15; Pillai, "Developing a Combatant Command Campaign Plan."

27. "About USSTRATCOM," United States Strategic Command, https://www.stratcom.mil/About/; Pillai, "Developing a Combatant Command Campaign Plan," United States Special Operations Command, *2025 Fact Book*, 8.

28. Joint Chiefs of Staff, *CJCSI 3100.01F: Joint Strategic Planning*, D-3–D-5; Erfourth, "SOF Competitive Campaigning in Great Power Competition."

29. United States Department of Defense, *DoD Directive 5132.03: DoD Policy and Responsibilities Relating to Security Cooperation*, 12–13; Joint Chiefs of Staff, *CJCSI 3100.01F: Joint Strategic Planning*, D-2-D-4; United States Special Operations Command, *SOF Renaissance*, 10, 14.

30. Jenkins and Fenton, testimony *Statement for the Record, Before the Senate Armed Services Committee*, 13, 15; Cartwright et al., *Operationalizing Integrated Deterrence*, 6–7; Joint Chiefs of Staff, Design and Planning, 2, 8–10.

31. "Tri-Command Lines of Effort: A Unified Approach to Security," United States Forces Korea, https://www.usfk.mil/What-We-Do/; *U.S. Indo-Pacific Command Posture Statement*, 119th Congress (2025) (statement of Admiral Samuel J. Paparo, Commander, United States Indo-Pacific Command), 3–4, https://armedservices.house.gov/uploadedfiles/indopacom_posture_statement_2025.pdf; Cotton, testimony *Before the Subcommittee on Strategic Forces, Senate Armed Services Committee*, 6; Madelyn Creedon et al., *America's Strategic Posture: The Final Report of the Congressional Commission on the Strategic Posture of the United States*, Institute for Defense Analyses, October 2023, 20–21, https://www.ida.org/research-and-publications/publications/all/a/am/americas-strategic-posture.

32. United States Special Operations Command, *2025 Fact Book*, 8–9, 24; Paparo, testimony U.S. *Indo-Pacific Command Posture Statement*, 11–12; "ROK-U.S. Combined Forces Command Hosts Republic of Korea Minister of National Defense," United States Indo-Pacific Command, January 7, 2026, https://www.pacom.mil/Media/News/News-Articles/Article/4372757/rok-us-combined-forces-command-hosts-republic-of-korea-minister-of-national-def/.

33. United States Special Operations Command, *2025 Fact Book*, 24; DuClos, "Closing the GAP: Strategic Presence Through Embedded U.S. Military Advisors."

34. Rachel Buitrago,"B-1s Train with US, ROKAF Fighter Aircraft," U.S. Air Force Global Strike Command, February 20, 2025, https://www.afgsc.af.mil/News/Article-Display/Article/4075735/b-1s-train-with-us-rokaf-fighter-aircraft/; David Choi, "Navy Discloses Submarine Visit to South Korea for First Time This Year," *Stars and Stripes*, September 24, 2024, https://www.stripes.com/theaters/asia_pacific/2024-09-24/submarine-visit-busan-south-korea-15282986.html.

35. Christopher Mesnard, "U.S. and ROK Special Operations Forces Conduct Routine Combined Training During Exercise Freedom Shield 2025," March 19, 2025, United States Forces Korea; Special Operations Command, Korea, https://www.usfk.mil/Media/Newsroom/News/Article/4127793/us-and-rok-special-operations-forces-conduct-routine-combined-training-during-e/.

36. United States Department of Defense, *Deterrence Operations Joint Operating Concept*, 42–43; Joint Chiefs of Staff, *JP 3-13.2: Military Information Support Operations*, I-4; Giulio Pugliese, "The 'Free and Open Indo-Pacific' as a Strategic Narrative," China US Focus, February 18, 2019, https://www.chinausfocus.com/foreign-policy/the-free-and-open-indo-pacific-as-a-strategic-narrative.

37. Cross-comparative citations of different framing of strategic assets press releases and SOF press releases. See *Stars and Stripes*, "Navy Discloses Submarine Visit to South Korea for First Time this Year," and United States Forces Korea "U.S. and ROK Special Operations Forces Conduct Routine Combined Training During Exercise Freedom Shield 2025."

38. Peter Rough, "Deterrence on NATO's Eastern Flank" (written testimony, Commission on Security and Cooperation in Europe [U.S. Helsinki Commission], November 17, 2025), Hudson Institute, 2–4, https://www.hudson.org/defense-strategy/deterrence-natos-eastern-flank-peter-rough.; Goddy U. Osimen, Oluwakemi Fulani, and Nesochi Mogbolu, "The Evolving Landscape of European Security: An Assessment of NATO's Posture and Deterrence Strategies in Response to the Russia-Ukraine War," *Journal of Strategic Security* 18, no. 4 (2025): 3–5; https://www.researchgate.net/publication/398390338_The_Evolving_Landscape_of_European_Security_An_Assessment_of_NATO's_Posture_and_Deterrence_Strategies_in_Response_to_the_Russia-Ukraine_War/link/693d263727359023a00c09aa/download?=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19.

39. Jenkins and Fenton, testimony *Statement for the Record, Before the Senate Armed Services Committee*, 7–8; Osimen, Fulani, and Mogbolu, "The Evolving Landscape of European Security," 7–10; Daniel Pullan and Joshua Young, "Going on the Offensive: Rethinking US SOF's Mission Set for the Age of Strategic Competition," *Small Wars Journal* (2026), https://smallwarsjournal.com/2026/02/26/going-on-the-offensive/.

40. NATO, "Exercise Steadfast Noon 25: NATO Allies Train for Nuclear Deterrence," NATO video, 7:15, October 30, 2025, https://www.nato.int/en/multimedia/multimedia/videos/2025/10/30/exercise-steadfast-noon-25-nato-allies-train-for-nuclear-deterrence; "Bomber Task Force Europe 26-1 Concludes, Demonstrating Global Reach and Allied Integration," United States Air Force

Global Strike Command, November 24, 2025, https://www.afgsc.af.mil/News/Article-Display/Article/4341565/bomber-task-force-europe-26-1-concludes-demonstrating-global-reach-and-allied-i/.

41. Jacob Murray, "US, NATO Forces Showcase Tactics, Integration During Exercise Astral Knight 2024," DVIDS, May 22, 2024, https://www.dvidshub.net/news/471836/us-nato-forces-showcase-tactics-integration-during-exercise-astral-knight-2024; United States Special Operations Command, *2025 Fact Book*, 23.

42. Paparo, testimony *U.S. Indo-Pacific Command Posture Statement,* 2–3, 16; U.S. Air Force, *Air Force Doctrine Note 1-21: Agile Combat Employment* (Department of the Air Force, December 2021), 3–4.

43. United States Special Operations Command, 2*025 Fact Book*, 26; Hickok and Miller, "Strategy for a New Era: USSOCOM Takes on Strategic Competition," 30–32, 36; Starling and Marine, *Stealth, Speed, and Adaptability*, 22–23; Brent Sadler, "American Samoa Is America's Strategic Hub in the South Pacific," *Irregular Warfare Initiative*, February 3, 2026, https://irregularwarfare.org/articles/american-samoa-is-americas-strategic-hub-in-the-south-pacific/.

44. Paparo, testimony *U.S. Indo-Pacific Command Posture Statement*, 6–7; Cotton, testimony *Before the Subcommittee on Strategic Forces, Senate Armed Services Committee*, 21–22; "BTF Operations in the Indo-Pacific AOR [Image 4 of 5]," DVIDS, September 10, 2024, https://www.dvidshub.net/image/8636715/btf-operations-indo-pacific-aor; "Abraham Lincoln Carrier Strike Group Arrives in Guam," United States Indo-Pacific Command, December 11, 2025, https://www.pacom.mil/Media/NEWS/News-Article-View/Article/4358108/abraham-lincoln-carrier-strike-group-arrives-in-guam/.

45. Adeola Adetimehin, "U.S. Naval Special Warfare, Philippines NAVSOU Conduct Joint Combined Training Exchange," United States Indo-Pacific Command, March 14, 2025, https://www.pacom.mil/Media/NEWS/News-Article-View/Article/4121327/us-naval-special-warfare-philippines-navsou-conduct-joint-combined-training-exc/.

46. Pugliese, "The 'Free and Open Indo-Pacific' as a Strategic Narrative"; Erfourth, "SOF Competitive Campaigning in Great Power Competition."

47. Cartwright et al., *Operationalizing Integrated Deterrence*, 4.

48. United States Department of Defense, *Deterrence Operations Joint Operating Concept*, 36–37.

49. United States Department of Defense, *Deterrence Operations Joint Operating Concept*, 42; Joint Chiefs of Staff, JP 3-13.2: *Military Information Support Operations*, I-4–I-6; Cartwright et al., *Operationalizing Integrated Deterrence*, 4.

50. Joint Chiefs of Staff, *CJCSI 3100.01F: Joint Strategic Planning*, A-3; Erfourth, "SOF Competitive Campaigning in Great Power Competition."

51. United States Army, TP 525-3-1: *The U.S. Army in Multi-Domain Operations 2028*, 20–21.

52. United States Special Operations Command, *SOF Renaissance*, 18.

53. United States Air Force, AFDN 1-21: *Agile Combat Employment*, 6–7.

54. Cartwright et al., *Operationalizing Integrated Deterrence*, 12–13; United States Special Operations Command, *SOF Renaissance*, 19.

55. United States Department of Defense, *Department of Defense Directive 5132.03*, 3-4, 12-13; Tisdel, Teske, and Fleser, *Theater Special Operations Commands Realignment*, 5–8.

56. Lumbaca, "Imagining the Near-Future of American Irregular Warfare in the Indo-Pacific"; Joint Chiefs of Staff, *JP 3-13.2: Military Information Support Operations*, II-7–II-8.; United States Department of Defense, *Deterrence Operations Joint Operating Concept*, 43.

57. Hickok and Miller, "Strategy for a New Era: USSOCOM Takes on Strategic Competition," 30.

58. Joint Chiefs of Staff, *Design and Planning*, 1–3.

59. Joint Chiefs of Staff, *CJCSI 3100.01F: Joint Strategic Planning*, D-2–D-4; Erfourth, "SOF Competitive Campaigning in Great Power Competition"; Pillai, "Developing a Combatant Command Campaign Plan."

60. Joint Chiefs of Staff, JP 3-13.2: *Military Information Support Operations*, I-5–I-6.

61. Tisdel, Teske, and Fleser, *Theater Special Operations Commands Realignment*, 5–6.

62. United States Department of Defense, *Department of Defense Directive 5132.03*, 11–12; Joint Chiefs of Staff, *CJCSI 3100.01F: Joint Strategic Planning*, D-3.

Advanced Resilience and Resistance in Digital Battlespaces: Countering Multiplatform Influence Operations Through Adaptive Communication Networks

By Troy C. Troublefield, PhD

Abstract

The contemporary digital information environment presents unprecedented challenges to U.S. Special Operations Command (USSOCOM) as adversary nations—particularly Russia and China—deploy sophisticated, multi-platform influence operations targeting Western democratic institutions and military operations. This paper examines the critical need for adaptive communication networks that can counter these threats through resilient strategic communication frameworks. Drawing from recent analysis of Russian and Chinese digital influence campaigns, this research proposes an integrated approach combining platform-specific communication strategies, real-time narrative intelligence, and adaptive network architectures to enhance special operations forces' (SOF) counternarrative capabilities. The analysis reveals that traditional communication approaches are insufficient against contemporary hybrid warfare tactics that exploit algorithmic amplification, cross-platform coordination, and psychological operations (PSYOP) targeting specific demographic segments. This paper presents a comprehensive framework for building resilient communication networks that can effectively resist and counter adversarial influence operations while maintaining operational security (OPSEC) and strategic effectiveness. Key findings indicate that successful counternarrative operations require an understanding of platform-specific affordances, audience engagement patterns, and the integration of technological solutions with human-centered communication strategies. The research concludes with

USSOCOM faces an urgent imperative to develop resilient strategic communication networks that can operate effectively in this contested digital environment.

actionable recommendations for USSOCOM to establish effective counternarrative capabilities leveraging emerging technologies while maintaining ethical standards and democratic values.

Introduction

The digital transformation of the global information environment has fundamentally altered the nature of warfare, creating new battlespaces where narratives compete alongside kinetic operations for strategic advantage. Russia and China have emerged as sophisticated actors in this domain, employing multiplatform influence operations that combine AI, social media manipulation, and coordinated inauthentic behavior to undermine Western interests and democratic institutions.[1] USSOCOM faces an urgent imperative to develop resilient strategic communication networks that can operate effectively in this contested digital environment.[2]

Contemporary assessments of U.S. information operations (IO) reveal significant gaps in capability and coordination, with experts assigning grades of "F" to national security community efforts in strategic communication.[3] This deficit becomes particularly concerning when considering that adversary nations significantly outspend the U.S. on information activities, creating an asymmetric disadvantage in the digital domain.[4] The challenge is compounded by the speed and scale at which digital influence operations can now be conducted, with Chinese operatives employing AI-generated content and coordinated campaigns that have led to a 60 percent increase in the dissemination of false information in 2025 alone.[5]

The unique operational requirements of SOF demand communication solutions that transcend traditional military communication paradigms. SOF operate in denied environments, where maintaining connectivity with conventional forces while conducting irregular warfare (IW) requires seamless integration

across multiple communication domains.[6] This operational context necessitates adaptive communication networks that can dynamically reconfigure to maintain effectiveness against sophisticated electronic warfare and IO targeting SOF activities.[7]

Research Problem and Objectives

This research addresses the critical gap between current USSOCOM communication capabilities and the evolving threat landscape by proposing a comprehensive framework for adaptive communication networks. The proposed approach integrates defensive resilience measures with offensive counternarrative capabilities, enabling SOF to maintain communication superiority while actively countering adversarial influence operations. The framework emphasizes platform-specific strategies that leverage unique affordances of different digital platforms while maintaining OPSEC and strategic coherence across multiple communication channels.

Literature Review

The scholarly literature reveals a significant evolution in state-sponsored digital influence operations over the past decade. Russian approaches to information warfare encompass the full spectrum of conflict and competition between states, including peacetime operations designed to shape the attitudes and policy preferences of adversaries.[8] This comprehensive approach differs markedly from traditional propaganda models, incorporating a sophisticated understanding of digital psychology and platform-specific engagement mechanisms.

Recent analysis indicates growing convergence between Russian and Chinese IO, with Chinese state media amplifying Russian narratives to create unified fronts that undermine Western policy

positions.[9] This coordination represents a significant escalation in the sophistication of multiplatform influence operations, requiring equally sophisticated defensive and offensive responses from the U.S Department of War (DoW) and other allied partners.[10]

Literature on strategic communication reveals ongoing challenges in adapting traditional communication doctrines to digital environments. An article published at the Joint Special Operations University identifies narrative intelligence as a critical tool for countering misinformation within IW constructs, emphasizing the role of cyberpsychology in shaping effective narrative strategies.[11] This interdisciplinary approach recognizes that effective counternarrative operations require an understanding of both technological and psychological dimensions of digital communication.[12]

Historical analysis of narrative space operations reveals the importance of synchronizing communication efforts with combat operations. However, research indicates that the U.S. approach has historically lagged behind those of its adversaries in terms of speed and agility.[13] This temporal disadvantage represents a critical vulnerability that adaptive communication networks must address through automated response capabilities and real-time narrative adjustment mechanisms.

The literature also emphasizes the importance of whole-of-government approaches to strategic communication. Effective counternarrative strategies require coordination across multiple departments and agencies, combining expertise from neuroscientists, sociologists, PSYOP specialists, and intelligence analysts.[14] This multidisciplinary requirement highlights the complexity of building effective and adaptive communication networks for SOF operations.

Emerging research on social media warfare reveals the critical importance of understanding platform-specific affordances and audience engagement patterns.[15] Contemporary hybrid warfare leverages social media platforms as potent tools for PSYOP, targeting civilian populations through rapid dissemination of tailored messages designed to exploit algorithmic amplification mechanisms.[16] Understanding these mechanisms is essential for developing effective counterstrategies.

Methods

Modern warfare increasingly depends on digital information dominance, where adversaries use sophisticated influence operations to shape narratives and undermine democratic institutions. SOF face unprecedented challenges countering these digital threats while maintaining operational effectiveness across multiple domains. This research develops adaptive communication frameworks enabling SOF units to effectively operate within and counter adversarial information ecosystems.

Research Design

This study employed an integrated research approach that combined a systematic literature review, case study analysis, expert consultation, and framework development methodology. The research design incorporated four distinct phases: (1) systematic review of existing literature on digital influence operations and military strategic communications, (2) detailed analysis of documented Russian and Chinese influence campaigns, (3) expert consultation with SOF personnel and IO specialists, and (4) development and validation of an adaptive communication networks framework through scenario-based testing.

Adversaries use sophisticated influence operations to shape narratives and undermine democratic institutions. SOF face unprecedented challenges countering these digital threats.

The methodological approach was designed to capture both the technological and human dimensions of digital influence operations while ensuring practical applicability to SOF operational requirements. This integrated research design enabled the triangulation of findings across multiple data sources, thereby enhancing the validity and reliability of the framework recommendations.

Data Collection

The rapid evolution of digital influence operations requires a comprehensive research approach to understand adversary capabilities and countermeasure requirements for special operations environments. This study's data collection methodology captures the full spectrum of digital influence phenomena through systematic analysis of documented operations, expert practitioner insights, and empirical validation of proposed solutions. This approach ensures findings are grounded in both theoretical understanding and operational reality, providing actionable intelligence for SOF communication requirements.

Systematic Literature Review Protocol

A comprehensive search was conducted across multiple academic and policy databases, including JSTOR, ProQuest Military Database, Defense Technical Information Center, and specialized

repositories from the Center for Strategic and International Studies, RAND Corporation, and Joint Special Operations University Press. The search covered publications from 2020 to 2025, focusing on peer-reviewed articles, government reports, and policy analyses.

Search terms included combinations of: "digital influence operations," "information warfare," "military strategic communications," "special operations forces," "counternarrative," "adaptive networks," "social media warfare," "hybrid warfare," and "narrative intelligence." Boolean operators and proximity searches ensured comprehensive coverage while maintaining relevance to research objectives.

Inclusion criteria required documents to address either: (1) state-sponsored digital influence operations by major powers, (2) strategic communication challenges in digital environments, (3) SOF communication requirements in contested environments, or (4) technological solutions for counternarrative operations. Exclusion criteria eliminated commercial marketing studies, purely technical communications research, and historical analysis predating the social media era.

Case Study Selection and Analysis

Three categories of influence operations were systematically analyzed based on documented evidence and operational significance: (1) Russian information campaigns targeting NATO unity and Western democratic institutions, (2) Chinese digital influence strategies during electoral periods and crises, and (3) documented instances of convergent Russia–China operations demonstrating coordinated messaging.

Cases were selected using purposive sampling to ensure representation across different operational contexts, target audiences, and technological approaches. Primary sources

included intelligence assessments, platform transparency reports, academic case studies, and journalistic investigations with verified documentation.

Analysis methodology employed structured case comparisons using standardized coding frameworks to identify patterns in adversary tactics, techniques, and procedures. The analyzed variables included platform selection, audience targeting, message coordination, technological tools, timeline analysis, and effectiveness indicators.

Expert Consultation Process

Semi-structured interviews were conducted with 15 subject matter experts representing diverse perspectives on digital influence operations and SOF communications. Participants included current and former SOF personnel with IO experience, academic researchers specializing in digital warfare, intelligence analysts focused on adversary influence operations, and technology specialists working on military communication systems.

Interview protocols addressed five key areas: (1) current SOF communication challenges in contested environments, (2) assessment of adversary influence operation capabilities, (3) gaps in existing counternarrative approaches, (4) technological requirements for adaptive communication networks, and (5) organizational and training implications for SOF units.

Participants were selected through snowball sampling, beginning with recognized experts in SOF operations and information warfare. Geographic distribution included representatives from U.S. military institutions, allied partner nations, and academic institutions with relevant research programs. All interviews were conducted under appropriate security protocols, with content reviewed for OPSEC compliance.

Framework Development and Validation

The adaptive communication networks framework was developed using systems engineering principles combined with human-centered design methodology. The development process included requirement analysis based on literature review and expert consultation findings, architectural design incorporating existing SOF communication systems, and integration planning for new technological capabilities.

Validation employed scenario-based testing using realistic operational vignettes developed in consultation with SOF planning personnel. Test scenarios included denied environment operations, crisis response communications, and extended counternarrative campaigns. Framework components were evaluated against effectiveness criteria, including responsiveness, security, interoperability, and scalability.

Data Analysis

Data analysis employed a systematic integrated approach combining qualitative content analysis of literature and case studies, grounded theory analysis of expert interviews, and multi-criteria evaluation of framework components. This methodology ensured a comprehensive examination of adversary capabilities, identification of SOF communication requirements, and a rigorous assessment of proposed solutions across technical, operational, and security dimensions.

Qualitative Content Analysis

Literature review findings and case study data were analyzed using a systematic qualitative content analysis methodology. Initial coding employed both deductive codes derived from existing theoretical frameworks and inductive codes emerging

from data analysis. Primary code categories included adversary tactics, capability gaps, technological requirements, and organizational factors.

Thematic analysis identified patterns across different data sources, with particular attention to convergent findings regarding adversary capabilities and defensive requirements. Inter-rater reliability was ensured through independent coding by multiple researchers with reconciliation of discrepancies through consensus discussion.

Expert Interview Analysis

Interview transcripts were analyzed using grounded theory methodology to derive framework requirements and implementation priorities. Open coding identified key concepts and relationships, followed by axial coding to develop category relationships and selective coding to identify core themes.

Analysis employed a constant comparative method to identify similarities and differences across expert perspectives. Theoretical saturation was achieved when additional interviews provided no new significant insights regarding framework requirements or implementation challenges.

Framework Evaluation Methodology

Framework effectiveness was evaluated using a multi-criteria decision analysis that incorporated expert judgment and scenario-based performance assessment. Evaluation criteria included technical feasibility, operational effectiveness, resource requirements, security considerations, and the complexity of integration.

Quantitative scoring employed structured decision matrices with weighted criteria reflecting SOF operational priorities. Qualitative assessment incorporated expert feedback on framework components and implementation recommendations.

Results

Contemporary digital influence operations reveal a rapidly evolving threat landscape with sophisticated state-sponsored campaigns that challenge traditional military communication paradigms. Russian and Chinese operations demonstrate unprecedented coordination, technological advancement, and strategic targeting that collectively represent a fundamental shift in information warfare capabilities. These findings expose critical vulnerabilities in current SOF communication approaches while identifying requirements for adaptive networks capable of operating in contested digital environments.

Contemporary Threat Assessment

Analysis of documented influence operations revealed three primary categories of adversary capabilities that pose significant challenges to SOF communications, with each demonstrating distinct operational characteristics and technological sophistication.

Russian Information Operations Capabilities

Intelligence assessments revealed that Russian IO have evolved to incorporate AI for generating and spreading misleading narratives, with documented campaigns targeting U.S. electoral processes and allied democratic institutions.[17] Russian operational approaches leverage multiple attack vectors simultaneously, including physical sabotage, cyber operations, and information warfare, creating complex challenges for defensive strategies.[18]

The geographic scope of Russian influence operations extends globally, with particular emphasis on undermining NATO unity and allied cooperation. Analysis of Russian information campaigns reveals coordinated efforts to exploit perceived divisions within Western alliances, using platform-specific messaging to amplify discord and undermine collective defense mechanisms.[19] This strategic approach requires counternarrative capabilities that can operate effectively across multiple linguistic and cultural contexts.

Russian operations demonstrate a sophisticated understanding of Western social media ecosystems and psychological vulnerabilities within target populations. Documented campaigns show integration of IO with kinetic activities, representing a fundamental shift in warfare that demands corresponding adaptations in SOF communication strategies.

Chinese Digital Influence Strategies

Chinese approaches to digital influence operations focus primarily on cyber espionage and influence campaigns targeting specific political figures and organizations, with documented attempts to hack devices associated with senior U.S. government officials.[20] These operations demonstrate sophisticated intelligence collection capabilities integrated with influence activities.

Chinese IO exhibit opportunistic characteristics, amplifying Russian narratives when they serve Chinese strategic interests while maintaining independent messaging capabilities.[21] This flexible approach enables Chinese operators to maximize influence while maintaining plausible deniability regarding coordination with other adversary nations.

Meta's analysis of Chinese influence operations reveals sophisticated audience-building strategies designed to establish credibility before deploying influence campaigns during critical periods such as major elections.[22] This long-term approach to influence operations requires sustained counternarrative efforts that can identify and neutralize influence networks before they achieve operational effectiveness.

Convergent Threats and Operational Implications

Growing evidence indicates increasing coordination between Beijing and Moscow in digital influence efforts, leading to convergence in tactics and strategic objectives that amplify the overall threat to Western interests. This convergence multiplies the challenges facing SOF communication operations, requiring adaptive networks capable of countering coordinated multi-adversary campaigns.

The technological sophistication of adversary influence operations continues to evolve rapidly. Emerging threats include AI-powered propaganda campaigns that can be precisely targeted to exploit societal divisions, sophisticated cyber warfare capabilities driven by AI algorithms, and potential deployment of autonomous weapons systems that could give small insurgent groups outsized military capabilities. These technological advances demand corresponding innovations in adaptive communication technologies and methodologies.

> ***The absence of unified command structures for information operations across government agencies compounds these challenges.***

USSOCOM Capability Gap Analysis

Systematic assessment of current U.S. IO capabilities revealed multiple categories of deficiencies that significantly impact SOF effectiveness in contested digital environments.

Coordination and Integration Deficiencies

Assessment revealed approximately 15 different definitions of information-related capabilities across military services, undermining effective integration of IO with kinetic activities and reducing overall operational effectiveness.[23] This conceptual fragmentation creates coordination challenges that adversaries can exploit through synchronized multi-platform campaigns.

Leadership assessments indicate that adversaries are outspending the U.S. on information activities, creating capability gaps that allow misinformation and false narratives to gain traction in critical operational areas.[24] This resource disparity requires force multiplication approaches that leverage technological innovation and strategic partnerships to maximize impact from available resources.

The absence of unified command structures for IO across government agencies compounds these challenges. Recent organizational changes, including the dismantling of the Global Engagement Center and reductions in traditional strategic communication capabilities, have created coordination gaps that adversaries can exploit.[25] Adaptive communication networks must account for these organizational limitations while providing SOF with autonomous capability to conduct effective counternarrative operations.

Technical and Operational Limitations

Current USSOCOM communication systems demonstrate limited adaptability to rapidly-changing threat environments. Existing networks lack automated threat detection and response capabilities necessary for operating in contested digital environments where adversary electronic warfare and cyberattacks can disrupt traditional communication channels.

Analysis revealed insufficient integration between communication systems and intelligence platforms, limiting real-time threat assessment and response coordination. SOF units require seamless integration of communication, intelligence, and operational capabilities to maintain effectiveness against sophisticated adversary influence operations.

Training and doctrine development lags behind technological advancement and adversary capability evolution. Current SOF personnel lack specialized training in counternarrative operations and platform-specific communication strategies necessary for effective operations in digital environments.

Platform-Specific Communication Analysis

Comprehensive analysis of social media platform dynamics revealed distinct characteristics that significantly influence information flow, audience engagement patterns, and operational effectiveness for counternarrative strategies.

Individual Platform Characteristics

Twitter/X analysis demonstrated real-time communication capabilities that make it particularly effective for rapid narrative deployment and crisis communication. The platform's algorithms favor trending topics and high engagement content, creating

opportunities for counternarrative operations but also vulnerabilities to adversary manipulation.

Facebook's algorithm-driven content distribution enables sophisticated targeting of specific demographic segments through detailed user profiling and behavioral analysis. The platform's community structure facilitates organic message amplification but requires authentic engagement strategies to avoid detection and removal.

Instagram's visual-centric approach provides opportunities for narrative reinforcement through imagery and short-form video content. The platform's younger user demographics require adapted messaging strategies that resonate with different generational communication preferences.

LinkedIn's professional networking focus enables targeting specific occupational and industrial segments relevant to SOF operations. The platform's emphasis on credible professional content provides opportunities for authoritative counternarrative deployment.

Cross-Platform Coordination Requirements

Effective social media strategies in military contexts require integration across multiple platforms to maximize reach and reinforce key messages through diverse communication channels. This multi-platform approach enables narrative reinforcement while reducing vulnerability to platform-specific disruption or censorship.

Digital diplomacy research demonstrates that multichannel orchestration strengthens reputation through cross-platform message consistency while enabling authentic emotional engagement with target audiences.[26] These principles apply directly

to SOF counternarrative operations, where credibility and emotional resonance determine operational effectiveness.

The challenge of maintaining message consistency across platforms while adapting to platform-specific characteristics requires sophisticated content management systems. Effective cross-platform strategies must account for different audience expectations and engagement patterns while maintaining core narrative coherence and strategic objectives.

Audience Engagement Pattern Analysis

Media influence on public perception operates through selective exposure mechanisms that allow individuals to engage with content aligning with pre-existing beliefs while excluding opposing perspectives. Understanding these psychological factors is crucial for designing counternarrative strategies that can penetrate adversary information bubbles and reach target audiences effectively.

Analysis of U.S. influence operations revealed that covert accounts typically achieve low engagement rates, with the vast majority of posts receiving minimal likes or retweets. This finding emphasizes the importance of authentic engagement strategies that build genuine credibility rather than relying on inauthentic amplification mechanisms.

Effective military audience engagement requires an understanding of geographic concentration patterns and lifestyle factors that influence communication preferences. SOF operations benefit from targeted approaches that leverage knowledge of military community characteristics while maintaining OPSEC requirements.

Adaptive Communication Networks Framework Development

The comprehensive framework developed through this research incorporates four interconnected components designed to address identified capability gaps while maintaining compatibility with existing SOF operational procedures and security requirements.

Network Architecture Specifications

Modern battle networks require dynamically reconfigurable mesh architectures capable of adapting to threats and disruptions while maintaining interoperability across multiple systems and security levels.[27] These architectural principles were adapted for counternarrative operations requiring similar resilience and adaptability characteristics.

Lessons from the Ukraine conflict demonstrate the importance of resilient communication architectures that integrate military, government, and commercial domains while maintaining adaptability to changing electromagnetic conditions.[28] SOF communication networks must incorporate these lessons while addressing unique OPSEC requirements.

The framework emphasizes redundancy and path diversity to ensure continuity of communication under adversarial pressure. Protected satellite communications and integrated space–terrestrial networks provide resilient channels that maintain effectiveness against sophisticated electronic warfare threats.[29] These capabilities enable SOF units to maintain connectivity while operating in contested environments.

AI-driven solutions can proactively identify and respond to emerging threats while optimizing communication strategies based on real-time audience engagement data.

Real-Time Adaptation Mechanisms

Contemporary military communication systems require real-time threat detection and automated response capabilities to maintain effectiveness against rapidly evolving cyber threats. Adaptive communication networks must incorporate similar capabilities for counternarrative operations, enabling automatic adjustment of messaging strategies based on adversary responses and audience feedback.

Future communication systems will feature automatic reconfiguration and self-healing capabilities that defend against all weapon systems potentially impacting network continuity and resilience. These technical capabilities provide foundation technologies for adaptive networks that can maintain operational effectiveness under sustained adversary pressure.

The integration of AI and machine learning capabilities enables predictive adaptation based on pattern recognition and threat assessment. AI-driven solutions can proactively identify and respond to emerging threats while optimizing communication strategies based on real-time audience engagement data.

Counternarrative Integration Capabilities

Narrative statecraft represents a proactive approach to shaping perceptions through stories that codify meaning to events and behaviors, requiring SOF personnel capable of analyzing cultural patterns and co-creating interventions with joint and interagency

partners.[30] This comprehensive approach recognizes that effective counternarratives must address both cognitive and emotional dimensions of audience engagement.

Effective counternarrative operations demand an in-depth understanding of adversary narratives and why they resonate with target audiences, as well as comprehensive strategic communication plans that directly support desired end states. Advanced analytical capabilities enable real-time assessment of narrative effectiveness and adversary response patterns. Social media analysis tools can provide near real-time event monitoring and population correlation to gauge the depth of network messaging penetration while capturing references to U.S. presence and activities.

Implementation Structure and Organization

Framework implementation requires the establishment of a dedicated counternarrative operations center that integrates personnel from IO, PSYOP, intelligence, and communications specialties. This organization should have the authority to coordinate counternarrative activities across SOF components while maintaining liaison with interagency partners and allied nations.

The counternarrative operations center should incorporate civilian expertise in social media analytics, cultural anthropology, and digital marketing to supplement military capabilities. Effective narrative statecraft requires personnel naturally predisposed to analyzing cultural patterns and social structures, though current numbers may be insufficient for anticipated requirements.[31]

Training programs should emphasize cross-cultural competency and platform-specific communication skills. Effective military social media engagement requires an understanding of target audience characteristics and communication preferences while maintaining OPSEC requirements.[32]

Discussion

The evolution of digital battlespaces presents both significant challenges and unprecedented opportunities for USSOCOM to enhance strategic communication capabilities and counter adversarial influence operations. The sophisticated multiplatform influence operations deployed by Russia and China require equally sophisticated responses that leverage technological innovation while maintaining ethical standards and democratic values.

Framework Effectiveness and Validation

The adaptive communication networks framework provides a comprehensive approach to building resilient counternarrative capabilities that can operate effectively across diverse platforms and cultural contexts. The network-of-networks approach enables dynamic reconfiguration to address emerging threats while maintaining interoperability across SOF components and allied partners.

Scenario-based testing revealed that framework effectiveness depends heavily on integration quality between technological capabilities and human expertise. Automated systems excel at pattern recognition and threat detection, but human judgment remains essential for cultural sensitivity and strategic decision-making in complex operational environments.

Validation exercises demonstrated that cross-platform coordination capabilities significantly enhance counternarrative effectiveness compared to single-platform approaches. However, maintaining message consistency while adapting to platform-specific requirements requires sophisticated content management and quality control procedures.

Critical Success Factors and Implementation Requirements

Analysis revealed that effectiveness depends on sustained investment in AI-powered analytical capabilities, development of cross-cultural competency among SOF personnel, and establishment of robust partnerships with technology companies and allied nations. Addressing current capability gaps requires sustained commitment to innovation and adaptation in the face of rapidly evolving adversary tactics. Leadership commitment emerged as the most critical factor for successful implementation. Without sustained organizational support and resource allocation, technological capabilities alone cannot overcome entrenched coordination challenges and institutional resistance to operational adaptation. Training and doctrine development must parallel technological advancement to ensure personnel can effectively employ new capabilities. Current SOF training programs require significant expansion to incorporate counternarrative operations and platform-specific communication strategies.

Integration with Kinetic Operations

The integration of counternarrative operations with kinetic activities represents a fundamental shift in SOF operational approaches that demands corresponding adaptations in training, equipment, and organizational structures. Success requires synchronization of actions and words to build credibility

> ***Automated systems excel at pattern recognition and threat detection, but human judgment remains essential for cultural sensitivity and strategic decision-making.***

while countering adversary attempts to undermine trust in democratic institutions.[33]

Military doctrine emphasizes that visible actions coordinated with credible words influence audiences more effectively than uncoordinated or contradictory actions and words. This principle requires adaptive networks capable of synchronizing narrative deployment with operational activities while maintaining OPSEC.[34]

Operational experience from ongoing conflicts demonstrates that IO integration with kinetic activities requires careful timing and coordination to maximize effectiveness while minimizing unintended consequences. SOF units must develop a sophisticated understanding of narrative timing and audience psychology to achieve strategic objectives.

Ethical Considerations and Democratic Values

Analysis of U.S. influence operations revealed that inauthentic tactics achieve limited effectiveness while potentially undermining Western credibility and supporting adversary objectives of attacking the objective truth. Effective counternarrative strategies must maintain ethical standards while achieving operational objectives. The framework emphasizes transparency and accountability in counternarrative operations. Democratic approaches to IO must balance security requirements with fundamental rights to freedom of speech and information access. This balance requires sophisticated

Success requires synchronization of actions and words to build credibility while countering adversary attempts to undermine trust in democratic institutions.

approaches that counter adversary narratives without replicating their unethical methods. Operational guidelines must address the potential for unintended consequences in counternarrative operations. Effective management of IO requires comprehensive approaches that balance security concerns with the protection of digital freedoms and democratic values.

Limitations and Constraints

Several significant limitations should be acknowledged when considering framework implementation. The rapidly evolving nature of digital technologies may outpace framework adaptation capabilities, requiring continuous updating and refinement of technological components and operational procedures. Resource requirements for full implementation may exceed current SOF budgetary allocations, particularly for advanced AI capabilities and specialized personnel training. Cost-benefit analysis suggests that phased implementation focusing on the highest-priority capabilities may be more realistic than comprehensive deployment.

Ethical constraints on democratic nations may limit counternarrative effectiveness compared to authoritarian approaches that employ deception and manipulation without legal or moral restrictions. This asymmetry requires innovative approaches that leverage democratic advantages while mitigating inherent disadvantages. Organizational resistance to change may impede implementation despite technological feasibility and operational necessity. Cultural transformation within SOF organizations requires sustained leadership commitment and demonstration of operational effectiveness to overcome institutional inertia.

Future Research Directions and Technological Development

Emerging areas requiring investigation include quantum communication technologies for secure counternarrative coordination, integration of augmented and virtual reality technologies into influence operations, and development of comprehensive metrics for assessing counternarrative effectiveness in contested information environments. Future research should examine the potential for quantum communication technologies to provide secure channels that cannot be intercepted for counternarrative coordination. Quantum communication development represents a significant advancement in providing impenetrable encryption for sensitive military communications.

The integration of augmented and virtual reality technologies into counternarrative operations represents an emerging area requiring investigation. Immersive technologies may transform how conflicts are perceived and experienced, creating new opportunities for narrative influence while requiring corresponding defensive capabilities. Research should examine the potential for blockchain technologies to provide tamper-resistant narrative verification systems that enable audiences to distinguish authentic information from adversary manipulation attempts.

Adversary capabilities continue to evolve rapidly … USSOCOM must act decisively to implement adaptive communication networks that can maintain effectiveness against these evolving threats.

Continued research into cross-cultural narrative effectiveness is essential for SOF operations in diverse global environments. Understanding cultural factors that influence narrative resonance enables more effective targeting while reducing unintended consequences. Investigation of generational differences in information consumption and processing patterns will inform long-term counternarrative strategy development. Different age cohorts exhibit distinct platform preferences and engagement patterns that require tailored approaches.

Research into the psychological effects of sustained information warfare exposure on both operators and target populations will inform operational guidelines and support requirements for SOF personnel conducting extended counternarrative operations. Development of comprehensive metrics for assessing counternarrative effectiveness remains a critical research requirement. Traditional communication metrics may be insufficient for evaluating operations in contested information environments where adversaries actively distort engagement signals.

Conclusion

The framework presented provides a comprehensive roadmap for building resilient, adaptive communication networks capable of supporting SOF operations in contested digital environments. Implementation success will require sustained leadership commitment, innovative partnerships, and continuous adaptation to emerging technologies and adversary tactics. The stakes extend beyond SOF operational effectiveness to encompass the broader defense of democratic values and institutions in an increasingly contested global information environment. Critical implementation recommendations include the establishment of a dedicated counternarrative operations center with integrated multi-disciplinary personnel, investment in AI-powered narrative analysis

tools and resilient communication infrastructure, and development of partnerships with technology companies and allied nations for capability sharing and interoperability.

The urgency of addressing these challenges cannot be overstated. Adversary capabilities continue to evolve rapidly, incorporating AI-powered propaganda campaigns and sophisticated cyber warfare capabilities that threaten to overwhelm defensive measures. USSOCOM must act decisively to implement adaptive communication networks that can maintain effectiveness against these evolving threats while supporting SOF missions across the spectrum of conflict. Future effectiveness will depend on USSOCOM's ability to balance technological innovation with human-centered communication strategies that resonate with diverse global audiences. Narrative statecraft requires an understanding of cultural patterns and social structures combined with the ability to co-create effective interventions with partner organizations.[35]

The integration of counternarrative operations with kinetic activities represents a fundamental evolution in warfare that demands corresponding adaptations in military doctrine, training, and organizational culture. Success requires recognition that information superiority may prove as decisive as technological superiority in future conflicts. The adaptive communication networks framework offers a pathway for transforming current capability gaps into strategic advantages through systematic integration of technological innovation with human expertise. However, implementation requires unprecedented coordination across organizational boundaries and sustained commitment to innovation in the face of rapidly evolving threats. The research demonstrates that effective counternarrative operations require a sophisticated understanding of adversary capabilities, platform-specific communication strategies, and cultural factors that influence narrative effectiveness. The framework provides structure for

Implementation requires unprecedented coordination across organizational boundaries and sustained commitment to innovation in the face of rapidly evolving threats.

developing these capabilities while maintaining ethical standards and democratic values that distinguish Western approaches from authoritarian alternatives.

The challenge facing USSOCOM extends beyond technical implementation to encompass fundamental questions about the role of IO in democratic societies. The framework addresses these concerns through emphasis on transparency, accountability, and respect for fundamental rights while providing effective capabilities for countering adversary influence operations. The path forward requires sustained commitment to innovation, adaptation, and coordination across multiple domains and organizations. The adaptive communication networks framework provides a foundation for this effort, but success ultimately depends on human judgment, cultural understanding, and strategic wisdom in applying technological capabilities to complex operational challenges.

About the Author

Dr. Troy C. Troublefield holds a DBA in international business management, a PhD in cyberpsychology, a PhD in information technology, a master of science degree in strategic intelligence, and MBAs in international business and management of information systems. He previously served as a master instructor at the Joint Special Operations University and an adjunct professor at the National Intelligence University. Currently, he is a doctoral research chair and adjunct professor at Capital Technology University. Professionally, Dr. Troublefield is a retired sergeant major and currently serves as program manager for the Department of War's U.S. European Command Web Operations program. His expertise encompasses cultural and social media analysis, internet-based psychological operations, and cyberpsychology applications in offensive and defensive cyber operations. He specializes in integrating intelligence, cyber, and influence capabilities in cyberspace and information operations, he also serves as a subject matter expert in multi-domain operations.

Notes

1. Joel Stradinger, "Narrative Intelligence: Detecting Chinese and Russian Information Operations to Disrupt NATO Unity," *Foreign Policy Research Institute,* 2024. https://www.fpri.org/article/2024/11/intelligence-china-russia-information-operations-against-nato/.
2. Paul Lieber, "Strategic Communication," *Joint Special Operations University Press,* March 1, 2020, https://jsou.edu/Press/PublicationDashboard/29.
3. Mark Pomerleau, "SOCOM Leader Warns of Information Operations 'Void,'" *DefenseScoop,* April 9, 2025, https://defensescoop.com/2025/04/09/socom-leader-warns-of-information-operations-void-gen-bryan-fenton/.
4. Li Zhang, Yufei Chen, and Ming Wang, "Forecasting Synergies in Chinese and Russian Digital Influence Operations," *The Asan Forum,* 2025. https://theasanforum.org/forecasting-synergies-in-chinese-and-russia-digital-influence-operations/.
5. Madalena de Almeida Veiga, "Combating Foreign Information Manipulation and Interference through EU-Restrictive Measures," in *The High Representative of the Union for Foreign Affairs and Security Policy as a Legal Actor* (Brill Nijhoff, 2025), 184–202, https://doi.org/10.1163/9789004700635_009.
6. Lauren Hickok and Larson Miller, " Strategy for a New Era: USSOCOM Takes on Strategic Competition," *Inter Populum: The Journal of Irregular Warfare and Special Operations* 2, no. 1 (2024): 30, https://interpopulum.org/wp-content/uploads/2024/12/InterPopulum_V2N1_Compliation_final.pdf#page=33.
7. Eddie Mobley, "Resilient Communications: Synchronizing the U.S. Army's Contested Logistics in INDOPACOM," *L3Harris,* September 28, 2023, https://www.l3harris.com/newsroom/editorial/2023/08/resilient-communications-synchronizing-us-armys-contested-logistics.
8. Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (Farrar, Straus, and Giroux, 2020), https://profilebooks.com/wp-content/uploads/wpallimport/files/PDFs/9781788160742_preview.pdf.
9. Stradinger, "Narrative intelligence."
10. Seth G. Jones, *Russia's Shadow War Against the West* (Center for Strategic and International Studies, 2025), https://www.jstor.org/stable/pdf/resrep68536.pdf?acceptTC=true&coverpage=false&addFooter=false.
11. Troy Troublefield, "Narrative Intelligence in Internet-Based Military Information Support Operations: A Cyberpsychology Perspective Under the Irregular Warfare Construct," *Joint Special Operations University Press,* December 30, 2024, https://jsou.edu/Press/PublicationDashboard/256.
12. Lieber, "Strategic Communication."
13. Charles Moore, Jr et al., "Maneuver and Engagement in the Narrative Space," *Strategic Multilayer Assessment Periodic Publication,* January 2016, https://nsiteam.com/social/wp-content/uploads/2015/12/Maneuver-in-the-Narrative-Space_Final_Jan2016.pdf.
14. Moore, "Maneuver and Engagement in the Narrative Space," 5.
15. Lauren Y. Hunter et al., "Artificial Intelligence and Information Warfare in Major Power States: How the U.S., China, and Russia Are Using Artificial Intelligence

in Their Information Warfare and Influence Operations," *Defense & Security Analysis* 40, no. 2 (2024): 112–134, https://doi.org/10.1080/14751798.2024.2321736.

16. Brett Van Niekerk et al., "Arab Spring: Analysing the Role of ICTs in the Tunisian and Egyptian Unrest from an Information Warfare Perspective," *International Journal of Communication* 5 (2011): 1406–1416, https://ijoc.org/index.php/ijoc/article/view/1168.
17. Alexander Martin, "Russian and Chinese Interference Networks Are 'Building Audiences' Ahead of 2024, Warns Meta," *The Record,* November 30, 2024, https://therecord.media/russia-china-interference-networks-building-audiences-elections.
18. Jones, Russia's Shadow War Against the West.
19. Stradinger, "Narrative Intelligence."
20. Moore et al., "Maneuver and Engagement in the Narrative Space."
21. Zhang et al., "Forecasting Synergies in Chinese and Russian Digital Influence Operations."
22. Moore et al., "Maneuver and Engagement in the Narrative Space."
23. Pomerleau, "SOCOM Leader Warns of Information Operations 'Void.'"
24. Pomerleau, "SOCOM Leader Warns of Information Operations 'Void,'" 3.
25. Pomerleau, "SOCOM Leader Warns of Information Operations 'Void,'" 4.
26. Smriti Singh Chauhan et al., "The Influence of Digital Diplomacy on Traditional Diplomatic Practices: Transforming Roles and Functions through Social Media." *South India Journal of Social Sciences* 23, no. 4 (2025): 53–57, https://doi.org/10.62656/SIJSS.v23i4.2185.
27. Todd Harrison, "Battle Networks and the Future Force," *Center for Strategic and International Studies* (2021), http://aerospace.csis.org/wp-content/uploads/2021/11/211103_Harrison_Battle_Networks_Part2-compressed.pdf.
28. David Betz and M. L. R. Smith, "Smart Weapons, Dumb Assumptions: Western Strategic Delusions Meet Industrial Reality in Ukraine," *Military Strategy Magazine,* June 26, 2025, https://www.militarystrategymagazine.com/exclusives/smart-weapons-dumb-assumptions-western-strategic-delusions-meet-industrial-reality-in-ukraine/.
29. Mobley, "Resilient Communications."
30. Kevin Maurer, "America's Special Operations Force Is Facing an Identity Crisis," *Task and Purpose,* November 15, 2021, https://taskandpurpose.com/news/americas-special-operations-force-is-facing-an-identity-crisis/.
31. Maurer, "America's Special Operations Force Is Facing an Identity Crisis," 2.
32. Lieber, "Strategic Communication."
33. U.S. Department of the Army, *Inform and Influence Activities,* FM 3-13 (Department of the Army, 2013).
34. U.S. Department of the Army, *Inform and Influence Activities,* 7.
35. Maurer, "America's Special Operations Force Is Facing an Identity Crisis."

Chapter 4

Digital Force Protection: Threats and Risks to SOF

In an era where digital footprints are persistent, data is weaponized, and influence can travel faster than military force, security challenges extend far beyond the battlefield. The papers in this chapter examine the growing intersection of technology, information, privacy, and national security, highlighting how individuals, organizations, and operational forces are increasingly exposed to threats across physical, cyber, and cognitive domains.

Contributors explore issues that shape both personal and professional security, from signature reduction and the risks posed by social media and open-source intelligence to the vulnerabilities of critical infrastructure and the demands of cyber resilience. The chapter also addresses the evolving role of counterintelligence in a hyperconnected world, as well as the strategic implications of economic messaging, marketing, and influence operations. Together, these studies provide insights into the challenges of protecting identities, safeguarding missions, and maintaining competitive advantage.

From Signature Reduction to Digital Force Protection: Operationalizing Counteroffensive Irregular Warfare in the Digital Domain

By Christopher Moede

Introduction

Congress, in the National Defense Authorization Act from Fiscal Year 2026, defined digital force protection as the "policies, tools, and practices used to protect military personnel, operations, and critical assets from adversarial exploitation of the commercial digital surveillance economy, associated commercial data, and digital footprints."[1] This definition was positioned not as an ancillary concern but rather a critical enabler of special operations forces (SOF) mission success.[2] Policymakers have rightly grasped the unmitigated risks to mission and force from the commercial digital surveillance economy and the digital footprints SOF leave behind—characterized by conditions of ubiquitous technical surveillance (UTS). This necessitates an adequate doctrinal response.[3] Digital force protection for SOF is not a defensive security discipline but rather the operational manifestation of signature reduction doctrine in the digital domain, enabling counteroffensive irregular warfare maneuver, survivability, and freedom of action for SOF in the UTS environment.

The Operational Condition: Ubiquitous Technical Surveillance

The commercial digital surveillance economy is now a direct and persistent threat to SOF, not just in theaters of conflict but across operational and personal aspects of mission preparation as well. AI-enabled targeting,[4] commercial surveillance ecosystems,[5] open-source intelligence,[6] and data brokers have dramatically reduced the barriers adversaries face when tracking previously undetected force movements. This allows them to conduct extensive digital surveillance and compromise operations before they ever depart home station.[7] This persistent and offensive problem extends across domains to wherever digital devices are in use, not just in theaters of conflict. Digital exhaust from units in forward operating

Where digital systems are used routinely, omnipresent information is produced, routinely collected, and exploited across time and space.

locations can be used for effects at home station, impacting service members' families in disturbing ways and vice versa. This generates difficult-to-measure effects and erodes operational effectiveness while increasing risk.[8] Where digital systems are used routinely, omnipresent information is produced, routinely collected, and exploited across time and space.

These conditions characterize a UTS environment in which observability itself becomes a form of vulnerability that can be weaponized by adversaries with the aid of other technologies.[9] This vulnerability extends across what is now known as gray zone warfare. In such an environment, force protection cannot be limited to a series of defensive security measures in forward operating locations alone, augmented by operational security (OPSEC) measures at home.[10] It must be grounded in an adequate counteroffensive doctrine that reclaims decision advantage and freedom under such prohibitive conditions before SOF depart to the operational area.

Signature Reduction as Counteroffensive Doctrine

Warfare has progressed into an unrestricted format in which irregularity and asymmetry dominate.[11] This gray zone warfare significantly challenges legacy systems and structures which struggle to adapt and keep pace as risk profiles increasingly span time and space with the help of digital technology, the phenomenon of UTS. This risk is both acute and generalized.[12]

Accordingly, maneuver suffers as the offensive technology-derived risks to mission and force growth. UTS poses such an existential threat because it collapses the boundaries of war and non-war, reaching from service members' personal devices to the closed-circuit television cameras which might physically place them in the operational area conducting sensitive activities.

This leads to the discovery of signature reduction—the doctrinal counteroffensive corollary to unrestricted warfare in the gray zone. Signature reduction offers a holistic and ordered logic that promotes freedom of action under conditions of UTS. Its value proposition is not necessarily anonymity or invisibility for SOF in digital spaces, but rather adequate obfuscation, deception, and denial of adversary visibility. Properly understood, signature reduction is maneuver under surveillance, and thus operational survivability for the post-digital age. Within this doctrinal foundation, digital force protection, the operational form in the digital domain, is discovered.

Digital Force Protection: Navigating the Digital Terrain

In gray zone warfare, digital terrain is not merely an OPSEC consideration prior to deployment but rather a critical battlespace that holds the key to positional and decision advantage in forward deployed locations. The conditions of UTS transform observability in digital terrain into vulnerability that spans time and space. Since digital technology makes SOF observable at home and during mission preparation, they now require digital safeguards in the operational area and prior to their arrival. We are vulnerable at home and in our daily lives simply by virtue of using digital devices and the commercial surveillance ecosystem which exploits them.[13] Simply not having a digital presence is neither practical nor helpful, as the absence of a digital signature also becomes its own signature. Yet,

> *We are vulnerable at home and in our daily lives simply by virtue of using digital devices and the commercial surveillance ecosystem which exploits them.*

by correlating digital device data using vehicles in the commercial surveillance economy, adversaries can target specific individuals at-scale.[14] This identity persistence amounts to risks to mission and force, especially for sensitive operational activity. Digital force protection, then, becomes maneuver in the digital terrain that mitigates or otherwise manages digital risk through policies, tools, and practices for SOF.

Digital force protection does not necessarily seek anonymity or invisibility in the digital terrain. Rather, it enables navigating this terrain through signature management or controlling visibility. Digital force protection is not merely "security through obscurity," but rather is a counteroffensive capability that holds power to shape digital observability, and thus, actively minimizes vulnerability and risk under conditions of UTS. The objective is to intentionally shape what an adversary may be able to observe. Adversary targeting depends not solely on collection but on attributing observability to an identity in time and space for some desired effect. Digital force protection disrupts this logic by degrading the adversary's ability to correlate and attribute with certainty. It is, in some sense, "hiding in the noise." Through digital force protection, freedom for action is preserved and survivability is extended—not because there is no digital footprint or signature, but because the digital footprint has been intentionally and systematically managed to control visibility according to desired operational outcomes.

As the digital terrain continues to grow, digital force protection is necessary to shape the battlespace and retain freedom for action often before physical movement occurs. This is to say, agility and decisiveness for SOF in digital terrain is shaped prior to their deployment. The commercial digital surveillance economy extends from the operational area to home station. Digital force protection reduces risk before SOF physically enter the operational area. These are not mere defensive force protection measures, or cybersecurity best practices, but functions of maneuver that shape operations.

Mapping Digital Force Protection to Ubiquitous Technical Surveillance Threat Vectors

UTS poses a multi-vector threat to freedom for action, seeking to correlate and attribute identity across time and space persistently. UTS operates across online, electronic, financial, visual–physical, and travel vectors to disrupt SOF activities.[15] Digital force protection is not specific to any of these vectors but functions across them and offers proactive multi-domain signature management that shapes identity correlation and reduces attribution risk. It directly enables operational flexibility under conditions of persistent observability. Understanding these vectors is not merely academic; it informs the operational steps that shape SOF digital signatures before deployment.

Through digital force protection, freedom for action is preserved and survivability is extended.

Operationalizing digital force protection begins with individuals and their devices as the locus where key digital terrain is won or lost. When the battlefield is everywhere, everyone must respond to efforts to collect, correlate, and disrupt their activity; this

should begin in the personal setting and continue to apply in an operational one. This requires coordinated planning, decision-making, and risk shaping from individuals to organizations before SOF deploy forward. Digital force protection is an operational effort that proactively shapes the digital terrain and denies the adversary observability. This begins in the pre-deployment environment where understanding and shaping activities are being conducted. Understanding adversary collection and correlation capabilities across UTS vectors is critical, and recognizing where SOF are exposed across UTS vectors uncovers hidden attribution risk for force movements. Implementing training and education programs to address this risk shapes the digital terrain prior to physical arrival.[16] Coordinating team device usage to reduce attribution risk while forward deployed becomes standard operating procedure. By shaping individual digital signatures prior to deployment, digital force protection preserves operational initiative, reduces adversary targeting certainty, and extends SOF survivability under UTS.

Toward Counteroffensive Freedom for Action

Digital force protection is the operational form of a counteroffensive signature reduction doctrine. It proactively reduces attribution risk in the UTS environment and extends survivability and optionality in gray zone warfare, where digital terrain demands shrewd navigation. It begins with individuals and their devices and has operational impacts well before reaching the physical battlespace. Digital force protection does not seek invisibility but a managed signature, or reduced adversary observability and correlation of SOF prior to operational activity. A controlled digital footprint in the digital terrain is the key to navigating gray zone warfare, providing a doctrinal lens for planning, training, and decision-making in UTS environments.

Digital force protection does not seek invisibility but a managed signature.

By integrating digital force protection into planning, training, and pre-deployment preparation, SOF translate signature reduction doctrine into real operational advantage, anticipating adversary collection and disrupting correlation attempts. This shapes their digital footprints in advance, creating freedom for action before deployment. This freedom for action translates to operational maneuver in the physical battlespace. Digital force protection thus degrades adversary targeting and attribution, transforming observability from a vulnerability into an opportunity for decisive action.

About the Author

Christopher Moede is the director of the Institute for Signature Reduction, an independent 501(c)(3) nonprofit charitable organization dedicated to advancing the disciplines of signature reduction, digital force protection, and cyber privacy in support of national defense and public institutions. Moede develops instruction for SOF units on emerging technology-based threat vectors and the operational risks of digital exposure, and explores how signature reduction can serve as a doctrinal foundation for modern irregular warfare. He also previously served as a mission commander in a selectively manned unit.

Notes

1. U.S. Congress, House, Committee on Armed Services, *Streamlining Procurement for Effective Execution and Delivery and National Defense Authorization Act for Fiscal Year 2026*, 119th Cong., 1st sess., H. Rep.119-231, H.R. 3838, sec. 1083, https://www.congress.gov/bill/119th-congress/house-bill/3838?s=1&r=5.

2. U.S. Congress, Streamlining Procurement for Effective Execution and Delivery and National Defense Authorization Act for Fiscal Year 2026, 1033.

3. Christopher Moede, "Counteroffensive Irregular Warfare: A Doctrine of Signature Reduction for Strategic Competition," *Small Wars Journal*, December 22, 2025, https://smallwarsjournal.com/2025/12/22/counteroffensive-irregular-warfare/.

4. Harry Davies and Yuval Abraham, "Revealed: Israeli Military Creating ChatGPT-Like Tool Using Vast Collection of Palestinian Surveillance Data," *The Guardian*, March 6, 2025, https://www.theguardian.com/world/2025/mar/06/israel-military-ai-surveillance.

5. U.S. Congress, Streamlining Procurement for Effective Execution and Delivery and National Defense Authorization Act for Fiscal Year 2026, 1037.

6. "Iran Monitor | Real-Time Open-Source Intelligence Dashboard for Iran," Iran Monitor, accessed March 2026, https://www.iranmonitor.org/.

7. U.S. Congress, Streamlining Procurement for Effective Execution and Delivery and National Defense Authorization Act for Fiscal Year 2026, 1035.

8. An uncorroborated operational vignette came to us from Ukraine, where a U.S. SOF member was discovered by foreign intelligence and security services to be using a particular location-based mobile application for various personal purposes during their deployment. While the individual was still deployed, a pair of ethnic representatives posing as salespersons arrived at their home address in the U.S. and asked the service member's spouse if they could speak with him. In a moment of surprise, the spouse let slip that their husband was unavailable as he was currently deployed. The salespersons' chilling response reportedly was: "We know." While clearly an attempt at intimidation and harassment, this vignette highlights the collapse between war and non-war, where omnipresent information—in this case made available to hostile security services through mobile application data—became a personalized instance of actualized risk. The emotional, psychological, and otherwise personal effects now compound even if the apparent operational effects seem limited.

9. *2024 Annual Threat Assessment: Testimony Before the Armed Services Subcommittee on Intelligence and Special Operations*, U.S. Congress, House (April 11, 2024) (statement of U.S. Air Force Lieutenant General Jeffrey Kruse, Director of Defense Intelligence Agency), https://docs.house.gov/meetings/AS/AS26/20240411/117088/HHRG-118-AS26-Wstate-KruseJ-20240411.pdf.

10. Joe Littell, Maggie Smith, and Nick Starck, "The Devil Is in the Data: Publicly Available Information and the Risks to Force Protection and Readiness," *Modern War Institute*, September 20, 2022, https://mwi.westpoint.edu/the-devil-is-in-the-data-publicly-available-information-and-the-risks-to-force-protection-and-readiness/.

11. Christopher Moede, "Ubiquitous Technical Surveillance and the Renewal of Irregular Warfare," *Small Wars Journal*, February 13, 2026, https://smallwarsjournal.com/2026/02/13/ubiquitous-technical-surveillance/.

12. 2024 *Annual Threat Assessment*, 33.

13. Alexander Master et al., *Tracking the Trackers: Commercial Surveillance Occurring on U.S. Army Networks*, Army Cyber Institute Technical Report (The Army Cyber Institute at Westpoint Military Academy, 2025), February 12, 2026, https://arxiv.org/pdf/2602.12388.pdf.

14. U.S. Government Accountability Office, Information Environment: DoD Faces Risks with Publicly Available Data, GAO-26-108771 (Government Accountability Office, 2025), https://files.gao.gov/reports/GAO-26-108771/index.html.

15. Ma'Ceo Bell, "Data Security Concerns Rise as Surveillance Becomes Ubiquitous," *U.S. Army*, August 12, 2025, https://www.army.mil/article/287760/data_security_concerns_rise_as_surveillance_becomes_ubiquitous.

16. Moede, "Counteroffensive Irregular Warfare."

Digital Force Protection in the Age of Social Media Intelligence and Open-Source Intelligence: Threats and Risks to SOF—and a Blueprint to Counter Them

By Claire Moravec

Abstract

The proliferation of social media intelligence and open-source intelligence (OSINT) has transformed the operational environment for special operations forces (SOF). While these tools offer opportunities for situational awareness, they simultaneously expose SOF personnel, families, and missions to unprecedented vulnerabilities. Adversaries—including near-peer competitors, terrorist networks, and non-state actors—leverage digital footprints to enable targeting, disinformation campaigns, and psychological warfare. Digital force protection (DFP) must be elevated from an individual responsibility to an institutionalized core competency within SOF. Drawing on recent case studies—including Strava's exposure of U.S. bases, ISIS's online radicalization tactics, China's state-directed OSINT infrastructure, and Hamas's use of encrypted messaging apps—analysis identifies five primary threat vectors: targeted violence, counter-SOF intelligence collection, influence operations, identity exploitation, and reputational risk. A blueprint for DFP grounded in education, technical safeguards, counterintelligence integration, whole-of-nation partnerships, and proactive influence capabilities is proposed. Ethical and legal considerations are also addressed. Ultimately, SOF can only preserve its operational advantage in irregular warfare by embedding resilience, foresight, and moral clarity into its digital practices.

Introduction

In the modern information environment, every digital action leaves a trace. The battlefield has expanded beyond the physical and kinetic to include the digital and cognitive. For special operations forces (SOF), whose success often depends on discretion, surprise, and trust, the rise of social media intelligence (SOCMINT) and open-source intelligence (OSINT) represents both a tool and a threat.

SOCMINT and OSINT exploit the openness of the digital ecosystem. Data once accessible only through classified collection is now available to anyone with a smartphone and an internet connection. Near-peer adversaries such as China and Russia, as well as non-state actors like ISIS and Hamas, increasingly exploit these digital footprints to track movements, intimidate families, manipulate narratives, and erode public trust.

Examining how adversaries exploit SOCMINT and OSINT against SOF identifies key gaps in current approaches to force protection and outlines a blueprint for institutionalized digital force protection (DFP). By reframing DFP as a mission-essential competency, SOF can safeguard its people, preserve operational advantage, and strengthen resilience in the 21st century.

> ***In the modern information environment, every digital action leaves a trace.***

The Digital Attack Surface

Social Media Intelligence and the Commodification of Identity

Social media platforms serve as real-time repositories of personal identity and behavior. SOCMINT enables adversaries to extract patterns from public and semi-public posts, geotags on Instagram, interactions on X (formerly Twitter), or fitness routes recorded on Strava. The 2018 Strava heat map incident, which exposed U.S. base perimeters in Syria and Afghanistan, demonstrated how user-generated data could inadvertently reveal operational vulnerabilities.[1] What was intended as a benign fitness-sharing feature became an intelligence goldmine for adversaries.

Open-Source Intelligence as an Aggregator of the Mundane

OSINT encompasses a broader array of data, from property records and commercial satellite imagery to LinkedIn profiles and academic publications. While each data point may seem innocuous, aggregation creates sensitive intelligence. Investigative groups such as Bellingcat have repeatedly shown how OSINT can geolocate troops, identify units, and verify strikes.[2] For SOF, this capacity in the hands of adversaries creates persistent exposure.

Families and Civilian Partners as Targets

The attack surface extends beyond operators. Spouses, children, and contractors often lack training in operational security (OPSEC) but still leave exploitable digital traces. Russian information operations in Ukraine included harassment of soldiers' families, spreading fear and eroding morale.[3] Similar tactics could destabilize SOF family networks, eroding trust between the home front and the operational environment.

China has institutionalized open-source intelligence as a state capability.

Case Studies in Adversary Exploitation

ISIS and the Weaponization of Social Media

ISIS pioneered the use of social media as both a propaganda tool and a tactical intelligence platform. Researchers at George Washington University's Program on Extremism found that ISIS recruiters actively mined Twitter and Telegram not only to radicalize but also to identify potential Western fighters.[4] For SOF, the lesson is clear: Adversaries can turn open platforms into recruitment pipelines and real-time intelligence sensors.

China's Open-Source Intelligence Infrastructure

China has institutionalized OSINT as a state capability. The People's Liberation Army and Ministry of State Security run extensive OSINT operations, often disguised as commercial or academic research centers.[5] Through "civil-military fusion," China integrates commercial big data firms and universities into intelligence collection, harvesting everything from Western military research papers to social media posts of military families stationed abroad. This blurs the line between civilian and military domains, making SOF personnel permanent subjects of surveillance.

Hamas, Telegram, and Hybrid Information Warfare

During the 2023 Israel–Hamas conflict, Hamas leveraged Telegram channels to broadcast propaganda, crowdsource intelligence from sympathizers, and manipulate the narrative of battlefield events.[6] The immediacy of Telegram, coupled with its encrypted infrastructure, allowed Hamas to bypass traditional media filters and shape global perceptions in real time. This model demonstrates how non-state actors weaponize digital ecosystems to contest the influence advantage of SOF.

Deepfakes and the Future of Disinformation

Emerging technologies further complicate DFP. In 2022, a deepfake of Ukrainian President Volodymyr Zelensky appeared online, falsely urging soldiers to surrender.[7] While quickly debunked, the incident illustrates the near-term risk of fabricated videos targeting SOF leadership or missions. Such tactics could erode trust within units, confuse allies, or delegitimize operations.

Threat Vectors to SOF

The convergence of SOCMINT and OSINT manifests in five primary threat vectors. Each vector highlights that digital exposure is not ancillary—it is central to adversaries' hybrid strategies.

1. **Targeted violence and terrorism**: Digital footprints enable physical targeting of SOF and families.

2. **Counter-SOF intelligence collection**: Adversaries aggregate data to map networks, deployments, and tactics, techniques, and procedures.

3. **Psychological and influence operations**: Manipulation of narratives undermines morale and legitimacy.

4. **Identity and credential exploitation**: OSINT fuels phishing, credential theft, and cyber intrusions.

5. **Reputational and institutional risk**: Viral disinformation, scandals, or deepfakes can erode public trust.

Current Gaps in Digital Force Protection

Individual burden versus institutional responsibility. Current OPSEC models overemphasize personal responsibility, failing to address systemic vulnerabilities. RAND's assessment of Russian propaganda models stresses that structural features of the information environment, not just user behavior, drive exploitation.[8]

Reactive posture. SOF responses to digital threats are typically reactive. After Strava, guidance was updated; after deepfakes, workshops were initiated. But adversaries evolve faster than doctrine, leaving SOF perpetually behind the curve.

Fragmented authorities. Cyber, counterintellligence (CI), family support, and psychological operations all touch DFP, yet

Just as physical fitness and weapons proficiency are non-negotiable elements of SOF identity, digital resilience must be considered foundational.

remain siloed. This fragmentation undermines coherence and speed of response.

A Blueprint for Digital Force Protection

Addressing the vulnerabilities created by SOCMINT and OSINT requires a shift in mindset: DFP must move from a series of ad hoc initiatives toward a fully integrated mission competency. The following blueprint outlines a holistic approach that spans education, technology, CI, partnerships, and influence. Rather than a checklist of isolated actions, it should be understood as an interconnected system that redefines how SOF conceives of readiness in the information age.

The first step is cultural. Just as physical fitness and weapons proficiency are non-negotiable elements of SOF identity, digital resilience must be considered foundational. Operators must understand that every digital action—whether a family member's photo on Instagram, a personal LinkedIn update, or a fitness tracker route—carries operational implications. This cannot be achieved by one-off briefings; it requires embedding digital literacy and adversary exploitation scenarios throughout professional military education, unit training cycles, and even family support programming. Scenario-based exercises, in which adversary analysts demonstrate how quickly a digital footprint can be assembled into actionable intelligence, can make the threat tangible. Families must

SOF counterintelligence programs must therefore incorporate red teaming of digital vulnerabilities, mirroring adversary collection techniques to identify gaps.

be brought into the fold—not as passive bystanders, but as active participants in the culture of digital resilience.

Technical safeguards form the second layer. The SOF enterprise should adopt privacy-enhancing tools at scale, from metadata scrubbers and virtual private networks to encrypted communication platforms designed for secure personal use. Automated monitoring systems can flag when operators' personal data surfaces in risky contexts—such as breached databases or hostile online forums—providing timely alerts before adversaries exploit it. Equally critical is the ability to remove harmful content quickly. Building formal partnerships with social media companies, including escalation channels for rapid takedown of doxxing or manipulated media, can prevent adversary exploitation from metastasizing. These safeguards must be enterprise-wide to avoid the current inequities where protection is uneven across units and families.

CI must also evolve. Historically, CI focused on detecting insider threats and hostile intelligence services. In the SOCMINT/OSINT era, digital exposure is itself an intelligence vector. SOF CI programs must therefore incorporate red teaming of digital vulnerabilities, mirroring adversary collection techniques to identify gaps. Lessons learned should not remain siloed but be disseminated across commands to anticipate emerging tactics. Moreover, CI support should extend to families and contractors, ensuring that the most vulnerable members of the SOF ecosystem are not left unprotected.

No single organization can manage this challenge alone. A fourth dimension of DFP is the cultivation of whole-of-nation partnerships. Civilian technology companies own the platforms where SOCMINT is harvested; universities and non-governmental organizations are at the forefront of OSINT research; allied militaries face the same adversaries and can share best practices. SOF must formalize partnerships with these actors, creating mechanisms for joint training, shared analysis, and rapid response. In doing so, DFP can evolve into a collective resilience effort, drawing strength from the distributed expertise of the broader national security ecosystem.

Finally, SOF must move from a purely defensive posture to proactive influence. Adversaries exploit digital ecosystems not only to collect intelligence but also to shape narratives. Countering this requires more than just debunking disinformation after the fact. Instead, SOF should invest in rapid counter-disinformation task forces, capable of detecting hostile campaigns early and responding with credible, transparent narratives. Building ethical influence capabilities that align with democratic values will allow SOF to contest the information environment while preserving legitimacy. The goal is not to manipulate, but to reinforce truth, trust, and operational credibility.

Taken together, these measures represent more than a blueprint—they form a doctrine of digital resilience. Education fosters awareness, technical safeguards limit exposure, CI integration detects and neutralizes threats, partnerships extend capacity, and proactive influence secures the information terrain. In this model, digital force protection becomes inseparable from mission readiness, ensuring that SOF can continue to operate in an era where every pixel, post, and data point is a potential vulnerability.

Ethical and Legal Considerations

SOF must avoid overreach. Protecting families from exploitation cannot justify blanket surveillance. International law, including norms articulated in the Tallinn Manual, underscores the importance of proportionality and necessity in cyber operations.[9] The balance lies in safeguarding without undermining the civil liberties SOF ultimately defends.

Conclusion

The information environment has permanently altered the calculus of force protection. SOCMINT and OSINT offer adversaries unprecedented opportunities to target, harass, and manipulate SOF. The cost of inaction is operational surprise, eroded legitimacy, and compromised readiness.

By institutionalizing DFP through education, technical safeguards, CI integration, partnerships, and influence operations, SOF can regain initiative. This is not merely about defending data; it is about preserving trust, resilience, and mission advantage in the digital battlespace.

About the Author

Claire Moravec is a nationally recognized strategic security and risk executive with more than 10 years of experience. A former FBI intelligence leader, Moravec recently served as the Deputy Homeland Security Advisor to the Governor of Illinois and the state's inaugural Deputy Director of Homeland Security. She currently serves as Director of Intelligence Operations for Social Media Exploitation at Sentinel, a global risk intelligence advisory firm.

At the FBI, Claire served as an intelligence and operations leader and was a founding member of the Bureau's Social Media Exploitation team. She was awarded the FBI Medal of Excellence in 2017 for leading digital threat disruption efforts targeting nation-state actors within the Bureau's National Covert Operations Section.

Claire holds degrees from Columbia University and Loyola University Chicago. She further completed executive education through the Naval Postgraduate School's Center for Homeland Defense and Security Executive Leaders Program and is a Federal Emergency Management Agency Vanguard Executive Crisis Leaders Fellow. She is also an adjunct professor at the University of Southern California and the University of Denver, where she teaches graduate and undergraduate courses in emergency management, criminology, and clinical social work.

Notes

1. "Fitness App Strava Lights Up Staff at Military Bases," *BBC News*, January 29, 2018, https://www.bbc.com/news/technology-42853072.
2. Eliot Higgins, *We Are Bellingcat: Global Crime, Online Sleuths, and the Bold Future of News* (Bloomsbury, 2021), 41–45, 72–79.
3. NATO Strategic Communications Centre of Excellence, *Social Media as a Tool of Hybrid Warfare* (NATO STRATCOM COE, 2016), https://stratcomcoe.org/cuploads/pfiles/public_report_social_media_hybrid_warfare_22-07-2016-1.pdf.
4. Lorenzo Vidino and Seamus Hughes, *ISIS in America: From Retweets to Raqqa* (George Washington University, 2015), https://extremism.gwu.edu/isis-america-retweets-raqqa.
5. Elsa Kania, "In Military-Civil Fusion, China is Learning Lessons from the United States and Starting to Innovate," *Strategy Bridge*, August 27, 2019, https://thestrategybridge.org/the-bridge/2019/8/27/in-military-civil-fusion-china-is-learning-lessons-from-the-united-states-and-starting-to-innovate.
6. Darren Loucaides, "How Telegram Became a Terrifying Weapon in the IsraelHamas War." *Wired*, October 31, 2023. https://www.wired.com/story/telegram-hamas-israel-conflict/.
7. James Pearson and Natalia Zinets, "Deepfake Footage Purports to Show Ukrainian President Capitulating," *Reuters*, March 16, 2022, https://www.reuters.com/world/europe/deepfake-footage-purports-show-ukrainian-president-capitulating-2022-03-16/.
8. Christopher Paul and Miriam Matthews, *The Russian "Firehose of Falsehood" Propaganda Model* (RAND Corporation, 2016). https://www.rand.org/pubs/perspectives/PE198.html.
9. Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017), 233–237.

Frail, Fragile, or Both?
An Evaluation of Cyber Resilience in Critical Infrastructure

By Renita Murimi, PhD

Abstract

The scope of critical infrastructure extends widely, impacting personal lives, work environments, and national security interests. The digitization and connectivity of critical infrastructure, while offering the advantages of enhanced usability and functionality, also increases the attack surface available to adversaries who are interested in targeted and widespread disruption of a range of applications and services. Although frailty and fragility have traditionally been used in the context of increased risk of negative health outcomes, the internet and its connected networks, too, have come to exhibit both frailty and fragility, leading to current challenges with the cyber resilience of critical infrastructure. This discussion provides a framework for examining the intricate relationship between frailty, fragility, and the resilience of critical infrastructure.

Introduction

Critical infrastructure assumes a vast scope, and its operations underlie much of what people do in their personal lives, work environments, and operational missions. To consider the scope of what critical infrastructure entails, one needs to only look at the range of the Cybersecurity and Infrastructure Security Agency (CISA) portfolio. As a United States federal agency, CISA is responsible for protecting physical and cyber infrastructure and considers 16 different sectors as core components of critical infrastructure.[1] These include chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial bases, emergency services, energy, financial services, food and agriculture, government services, healthcare and public health, information technology, nuclear, transportation, and water and wastewater systems. While previously many of these critical infrastructure sectors were primarily in the physical world, they are

now rapidly being digitized and connected to the internet to enable automation, remote access, and real-time data processing. This connectivity also opens the attack surface of critical infrastructure by providing adversaries with opportunities to exploit vulnerabilities in these services. For example, in October 2024, several rural water systems in Texas were attacked by the Cyber Army of Russia Reborn, causing the water system to overflow and eventually have to be manually overridden.[2] According to the State of Critical Infrastructure Resilience Report, in 2024 alone, 62 percent of water and power operators in the U.S. and U.K. were hit by cyberattacks, 59 percent of which were launched by nation-state actors.[3]

Threats to critical infrastructure have the potential to disrupt everyday activities with varying degrees of severity.

Threats to critical infrastructure have the potential to disrupt everyday activities with varying degrees of severity. The exploitation of vulnerabilities in critical infrastructure impacts not only cyber resilience but also poses technical and privacy threats to both online and offline environments. Cyber resilience is broadly understood as the ability to anticipate, respond, and recover from cyber incidents.[4] Specifically, the National Institute of Standards of Technology (NIST) SP 800-160 asked if an "organization's strategic activity increases fragility," and the 2024 President's Council on Science and Technology noted "an increasingly fragile society… with often fragile cyber-physical systems."[5] The internet, which is a building block of digitized critical infrastructure, has been called a "robust yet fragile" complex network due to its ability to withstand random component failures while still being vulnerable to attacks on targeted components.[6] Similarly, global information systems have been said to exist in a state of "fragile and inchoate" stability,

calling for strategic cyber plans that consider the capabilities of our adversaries in cyberspace.[7]

This research conceptualizes the frailty and fragility of critical infrastructure systems. In general, fragility evokes notions of rupture and disruption. Objects, beliefs, health, relationships, and networks have all been called fragile based on their tendency to be readily disrupted, ruptured, or damaged while being difficult or impossible to restore. On the other hand, frailty denotes a loss or decline in certain physical, social, and psychological capacities and is commonly associated with age or weakness. Both frailty and fragility are evident in the web and the increasingly digitized critical infrastructure, which are subject to various internal and external pressures.

Contributions are as follows. It argues that there are two linked phenomena in the context of cyber resilience of critical infrastructure: frailty and fragility. These phenomena have traditionally been used in the context of negative health outcomes, but there is a difference between the two. Whereas frailty is described as a consequence of intrinsic factors that cause continuous decline, fragility is described as a consequence of extrinsic factors such as unfavorable social conditions.[8] This research introduces a model for analyzing frailty and fragility of critical infrastructure in the context of cyber resilience, and provides a novel interdisciplinary framework for examining how broader socio-economic and political factors exert a variety of pressures on critical infrastructure.

The rest is organized as follows. An overview of the pace layering framework, which has been used in systems theory to explain how complex systems evolve over time will be presented. The pace laying framework will be used to illustrate how the pace layers induce a range of internal and external pressures on critical infrastructure.

Next, there is a presentation of the model of frailty, fragility, and cyber resilience, along with the limitations and practical implications of this model. But first, frailty and fragility from an interdisciplinary perspective will be examined.

Section 1

Related Work

While fragility has been studied more widely across disciplines, frailty is mostly associated with aging and health. This section will present an overview of these phenomena.

Fragility

In systems theory, fragility has been defined as the state where a system suffers a sudden unexpected failure that propagates fast and is caused by "small disproportionate stimuli."[9] In the field of package design, fragility refers to the amount of mechanical shock an item can survive on its own.[10]

Fragile states are a term often encountered in the area of "state-building," which refers to the context of political relationships between governments and their citizens.[11] Fragility has also been described as an outcome of a failed social contract between citizens of a state and their institutions resulting in the failure of the state to meet its people's expectations, where fragility has been described as the opposite of resilience.[12] In 2015, the Fund for Peace published the Fragile States Index which highlighted the role of geopolitical conflicts, polarized internal politics, and rivalries between the great powers, among other factors in undermining the resilience of states to disruptions.[13] Another characterization of the fragility of states was developed by the Organization for Economic Cooperation and Development, which defined the fragility of a state as "the combination of exposure to risk and insufficient coping capacities of

the state, system and/or communities to manage, absorb or mitigate those risks."[14]

Agreements and compromises have also been studied for their fragility.[15] Compromises have been described as fragile, due to the "pluralities of justifications" of individuals and institutions involved.[16] Fragility has also been studied in the context of belief systems, self-esteem, psychological wellbeing, and interpersonal relationships.[17] Likewise, fragility has been studied in power grids, algorithm design, and financial systems.[18] Other studies of fragility have been conducted in the context of statistical confidence of clinical case trials as well as in the area of ecosystems.[19]

Frailty

Frailty has been primarily studied in the context of aging.[20] Frailty in aging has been described as an "accumulation of deficits," and as a state of health affected by losses in one or more of three domains: physical, physiological, and social.[21] Continuing the theme of deficits and decline, frailty has been described as a state of vulnerability due to a lifetime of declining physiological systems.[22] Physical frailty has been described as an outcome of decline in three systems: musculoskeletal, metabolic, and stress response systems.[23]

The preceding overview of fragility and frailty shows the widespread adoption of the notion of fragility in diverse systems, while the notion of frailty is mostly focused on aging human health. The next section presents an overview of the pace-layering framework, which describes how complex systems evolve over time in response to socio-political and technological factors. Such a view of system evolution is crucial to understanding the pressures on critical infrastructure systems, which possess complexity in both time and scope. The pace-layering framework will provide

the foundation for examining the cyber resilience of critical infrastructure in response to various internal and external pressures.

Section 2

Pace-Layering Framework

In a 2020 article in the *MIT Journal of Design and Science*, Stewart Brand presents a theory of complex systems involving layers. This theory conceptualizes that complex systems have components or layers that move at different paces. From bottom to top, these layers (in order) are: nature, culture, governance, infrastructure, commerce, and fashion/art.[24] In this order, the layers move in increasing speed from the lowest layer, which is the slowest (nature) to the topmost, fastest layer (fashion/art). See Figure 1. Brand used this theory to study the evolution of civilizations over time, as well as macro movements in ecosystems and other complex systems. According to this theory, the pace of individual layers determines the long-term vitality of the system. For example, when a slow-moving layer like nature moves at a much faster pace than

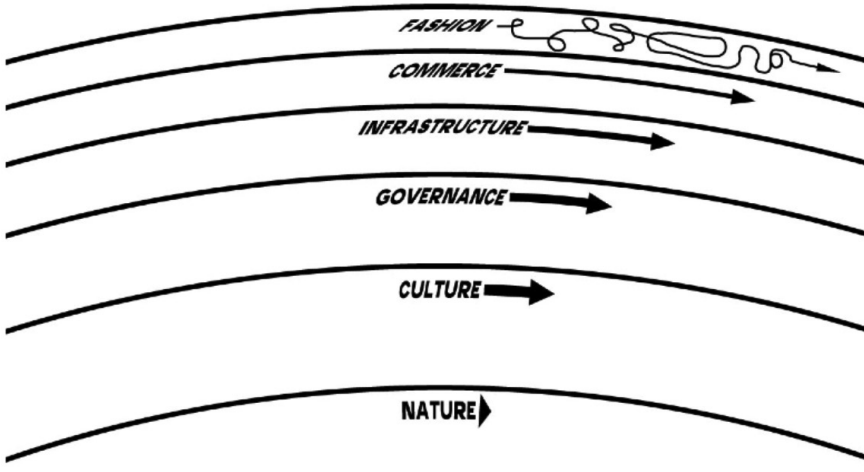


Figure 1. The pace-layering framework. Source: Stewart Brand

its usual slow pace, the abnormal pace of the nature layer can lead to massive disruptions such as those seen during earthquakes and other natural disasters. Similarly, when the governance of a system or society moves at a faster pace than is appropriate for that layer, it leads to social unrest as seen during the French and Russian revolutions. Complex systems need the lower, slower layers for scaffolding and absorbing the shocks that result from the faster pace of the upper layers.

The pace-layering framework's applicability has extended to different domains, including the design of residential structures and sustainable cities.[25] It has also been used to study how collaborative tagging systems found in websites and online social networks operate at the upper layers of information architecture systems.[26] In other applications, the pace layering framework has also been used to study how organizations respond to the introduction of newer (intelligent) technologies, since these technologies cause the layers to change at different rates.[27] Another example of the pace layering framework is in the study of the impact of ransomware incidents on the cyber insurance industry, where it was shown that although ransomware impacts were mostly felt at the commerce layer, ransomware-associated challenges impacted the culture, governance, infrastructure layers as well.[28]

The pace-layering framework[29] is used to explore the pressures exerted on critical infrastructure by the mismatched pace of movement of various layers. The next section presents an overview of these pressures.

Section 3

Pressures on Critical Infrastructure Systems

Critical infrastructure systems are subject to a variety of internal pressures that are a result of sprawling networks and the

hardware and software that connects the networks. In 2024, the North American Electric Reliability Corporation estimated that the number of vulnerabilities in both virtual and physical electric grid infrastructure rose from approximately 22,000 vulnerabilities to approximately 24,000 vulnerabilities, with an increase of about 60 per day.[30] External pressures on critical infrastructure arise from the interdependence of societal, geopolitical, legal, and economic factors. These include regulation and policy initiatives, proliferation of cyber adversaries, and the increasing complexity and interoperability issues of emerging technologies. In the ongoing Russia–Ukraine conflict, groups like Sandworm that are linked to the Russian military intelligence agency have deployed malware against Ukrainian power systems.[31] Conflicts between the two countries have also resulted in information warfare along the lines of psychological operations, where pro-Russia and pro-Ukraine hacktivists (e.g., KillNet vs. Anonymous) waged information and distributed denial of service (DDoS) campaigns globally.[32] Other examples of ideologically-motivated hacktivism include leaks from the group called Guacamaya, which aims to expose corruption and corporate environmental harm.[33]

Hardware attacks and software attacks represent another key source of pressures on critical infrastructure systems. Hardware attacks are not as widespread as software attacks due to the complexity of exploiting existing hardware vulnerabilities or intentionally engineering devices with compromised hardware components. Still, they are becoming more prominent in cyberwarfare, since they can be covertly launched while evading most malware detection software and disabling critical security mechanisms. In 2023, over 50 percent of the most exploited vulnerabilities in critical infrastructure were initially exploited as zero-days.[34] Attacks such as LoJax and Black Lotus use sophisticated attack mechanisms by targeting the firmware and

boot processes, causing the malware to be deployed before the operating system loads. LoJax has been used to target government organizations in Eastern Europe, and Black Lotus has been found for sale on hacker forums.[35] The distributed nature of internet of things (IoT) networks increases the attack surface, since these devices lack the computing power to execute sophisticated cryptographic data protection mechanisms. An example of such an attack is the 2025 data breach at Mars Hydro, a grow-light manufacturer, which resulted in the exposure of 2.7 billion IoT device records including Wi-Fi network names, passwords, IP addresses, and device identifiers.[36] A taxonomy of various hardware challenges is presented in the NIST report on hardware security failure scenarios which categorizes hardware weaknesses in 13 categories and maps it to the Common Weakness Enumeration list.[37]

Human-computer interaction is yet another source of pressure on critical infrastructure. Social engineering, which has consistently been ranked among the top causes for data breaches over the years, is a lucrative mechanism for cyber adversaries for targeting a range of users. Spear-phishing is a commonly employed social engineering attack mechanism and was used in the 2023 LookBack malware through phishing emails with malware in the attachments.[38] Phishing attacks powered by AI were found to have a 54 percent click-through rate, compared to just 12 percent for traditional human-crafted phishing emails.[39] These phishing emails impersonated a U.S.-based engineering licensing board, and the attachment activated remote-access Trojans that enabled the attackers to completely take over the compromised endpoints. The ZipLine phishing attack in 2025 targeted U.S. manufacturing and supply chain-critical companies.[40] Attackers exploited legitimate-looking business interactions to deliver custom malware implants, leading to stolen intellectual property, ransomware extortion, financial fraud, and significant disruptions to critical supply chains. Users also

tend to delegate security responsibilities to others and downplay their individual role in safeguarding their networks.[41] Further, insider threat continues to be a significant source of pressure on information systems, with 83 percent of organizations listing at least one insider attacker in 2024.[42]

Additional pressures on critical infrastructure arise from the incentives inherent in cybercrime activities. In a 2012 *Foreign Policy* article, Josh Rogin called cybercrime the "biggest transfer of wealth in history."[43] In 2024, cybercrime was estimated to have cost the world $9.5 trillion.[44] The pace of adoption of new and emerging technologies poses several risks to critical infrastructure systems, including an increased attack surface, poorly tested operational environments, and lack of user awareness about secure end-user behaviors. Another crucial factor impacting external pressures on critical infrastructure is related to natural disasters, compounding the impact of extreme weather events, pandemics, and simultaneous cyberattacks. A report by the Stimson Center described how the impact of cyberattacks is amplified during natural disasters due to surge in online scams and malicious activities.[45]

The next section presents a model incorporating the pace-layering framework to illustrate the interdependence of pressures, frailty, fragility, and cyber resilience in critical infrastructure.

Section 4

Model of Frailty and Fragility in Critical Infrastructure Systems

One of the first simultaneous explorations of frailty and fragility as distinct but related conditions was conducted in the context of aging.[46] There, the authors denote frailty as a consequence of ongoing decline caused by biological, psychological, economic, and social factors. Frailty resulted in decreased resistance to stressors and was found to be a predictor of negative health outcomes. On

the other hand, the authors describe fragility as an outcome of frailty. Fragility denoted a stable state of social vulnerability, in contrast to frailty, which was an ongoing state of decline.

These insights derive the markers of frailty and fragility in critical infrastructure and their impact on the cyber resilience of critical infrastructure. Figure 2 shows this model of frailty and fragility in critical infrastructure.

While the original pace-layering framework has six layers (nature, culture, governance, infrastructure, commerce, and aesthetic), this model excludes the aesthetic layer due to its minimal relevance to the context of cyber resilience of critical infrastructure. The layers used in this model are indicated on the top left by dotted lines: nature (N), culture (Cu), governance (G), infrastructure (I),

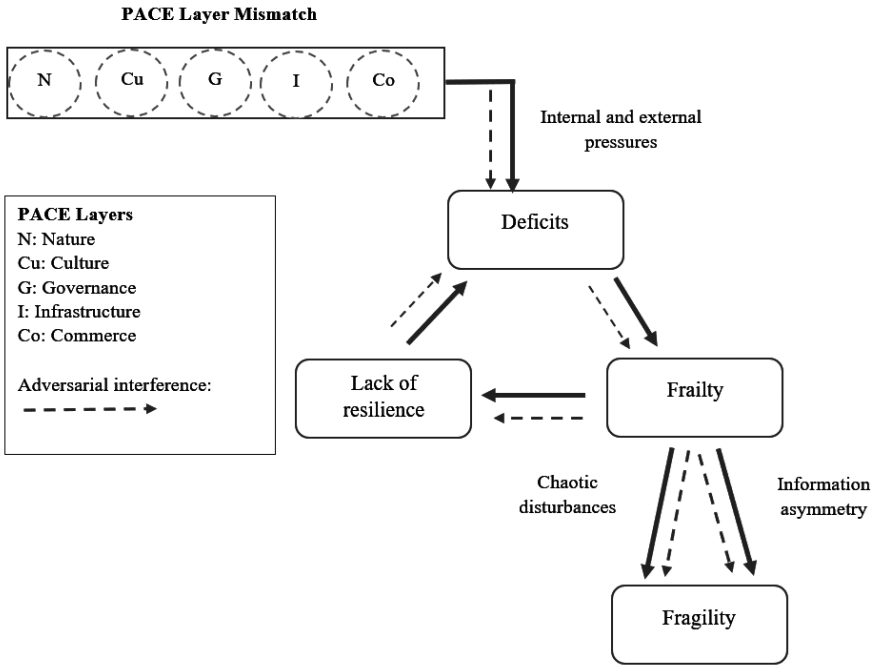


Figure 2: A model of frailty, fragility, and cyber resilience in critical infrastructure. Source: Author

and commerce (Co). Figure 2 shows how mismatched rates of change across these five pace layers are responsible for imposing internal and external pressures on critical infrastructure systems. In turn, these pressures cause deficits (or vulnerabilities) in critical infrastructure, which, when accumulated over time, contribute to the increasing frailty of critical infrastructure. The interplay between the pressures caused by mismatched growth layers, the resulting deficits, and the ensuing frailty negatively impact the cyber resilience of critical infrastructure. Another significant aspect of the model is adversarial interference (indicated by dashed lines), which impacts every aspect of the life cycle of critical infrastructure systems. Adversarial interference arising from various motives for conflict compounds these pressures and deficits, increasing their impact on the frailty, cyber resilience, and fragility of critical infrastructure systems.

It should be noted that critical infrastructure systems can remain in a frail state for extended periods of time while still functioning at some pre-determined baseline level of usability, functionality, and even security. This is mainly due to the distributed nature of software solutions such as patches and software versions that are routinely deployed to improve functionality and security. However, patched solutions alone can't fix the inadequacies of frail and fragile critical infrastructure systems. The variable success rate of the patch lifecycle due to various factors such as inadequate testing, compatibility issues, environment complexity, and process failures means that the success of patching as an intervention for frail systems is uncertain. A recent report suggested that approximately 20 percent of patches failed to install correctly, leading to potential security gaps and increased risk exposure. The report also showed that the energy sector, a critical infrastructure sector, experienced the longest delays in patching, with an average of 90 days to patch

vulnerabilities, while that in financial services (another critical infrastructure sector) averaged 45 days.[47]

Figure 2 shows how frail systems could transition into a state of fragility, although once a critical infrastructure system is in a frail state, it could stay in this state depending on the interventions that are deployed to maintain the system. While patching was described earlier as an intervention for frail systems, another example is compatibility between older and newer technologies. For example, consider critical infrastructure systems with legacy code that co-exists with modern information system components. Such co-existence offers a temporary intervention for the frailty of system components. A 2025 report on legacy code in banks noted that approximately 70 percent of banks globally continue to rely on legacy systems, while over 60 percent of U.S. hospitals operate critical applications on legacy software.[48]

However, not all interventions enable critical infrastructure systems to stay in a state of ongoing decline without further deterioration. Some frail systems, when subject to additional unfavorable external conditions such as chaotic disturbances or information asymmetries, transition into a state of fragility. This is the state in which the critical infrastructure system can be readily disrupted, ruptured, or damaged while being difficult or impossible to restore. These chaotic disturbances are marked by sudden changes in the operating environment of the system and can be spurred by a variety of interacting circumstances. The 2021 attack on the Oldsmar water treatment plant in Florida was caused by a remote attacker who gained access to the software system and increased sodium hydroxide levels in the water. This plant was also running legacy software (Windows 7) with no firewall and used a shared remote desktop software (TeamViewer) on an aging control system.[49]

Approximately 70 percent of banks globally continue to rely on legacy systems, while over 60 percent of U.S. hospitals operate critical applications on legacy software.

Another example of a frail critical infrastructure system pushed into a fragile state by a cyber incident is found in the 2022 power outages in Puerto Rico. In this incident, the electricity grid was attacked by hacktivists resulting in grid instability and frequent blackouts. The grid was also subject to several pressures in the preceding years due to hurricanes damaging an already aging, partially automated control system.[50] In recent years, such chaotic disturbances have affected information systems around the world in various ways as evidenced by the effects of the COVID-19 pandemic, wars and geo-political conflicts, technological disruptions such as AI tools, and broader socio-economic and political influences. For example, a combination of ransomware, organizational transitions, the COVID-19 pandemic, and broader geopolitical conflicts contributed to an Australian beverage company's supply chain disruption.[51] Additionally, information asymmetry involved in cyber defense is a prominent cause of the transition to fragility. In the 2021 Colonial Pipeline attack, a ransomware attack by the DarkSide ransomware group led to a halt in fuel distribution along the east coast of the United States. This problem was compounded by misinformation that suggested that the fuel supply had been destroyed. As this news began to circulate, panic buying ensued, leading to actual fuel shortages and price spikes.

The pressures on critical infrastructure are further deepened by the enterprise-like activity of cyber adversaries, some of whom are funded by nation-state actors and entities with differing ideological motives. Groups such as Lockbit, Conti, and DarkSide are known for

running their adversarial cyber operations like businesses. LockBit offered affiliates malware, an admin/affiliate portal, negotiation templates, and a leak site that pressures victims. Ransomware operations such as those run by DarkSide are equipped with sophisticated currency laundering tactics and leak sites, where the pricing and collections behavior of ransomware operations resembles a predatory business model.[52] For such adversaries, a single hit on a critical infrastructure system is a matter of immense success on several fronts, including but not limited to geopolitical conflict and financial gains.

A critical infrastructure system in a fragile state is at risk of several undesirable outcomes, such as unexpected behaviors; reduced or non-existent assurances of confidentiality, integrity, and availability; vulnerability to breaches and attacks; and even service disruption. In this state, critical infrastructure systems are in need of drastic overhaul. Fragility in critical infrastructure, thus, represents the widest possible range of deficits, pressures, and declines that a system can be subject to before its eventual replacement or removal.

Section 5

This section presents the limitations of this model of frailty and fragility in critical infrastructure and describes areas of future research related to interventions for reducing frailty and fragility.

Limitations

Interdependence of Pace Layers

In the pace-layering framework, each of the six layers is assumed to be independent of the other. In practice, such independence can't be stipulated. For example, the slowest two layers (nature and culture) display elements of interdependence. Changes in the natural environment of a complex system affects the patterns of

social interactions of individuals and organizations inhabiting that natural environment, eventually affecting the culture. The same is true of all other layers in the pace-layering framework, since feedback loops of varying degrees exist not only between adjacent layers but also between non-contiguous layers. In the context of critical infrastructure environments too, this interdependence manifests in terms of correlations between the nature, culture, governance, commerce, and infrastructure layers.[53] As is true of most real-world phenomena, the interdependence between layers is difficult to model due to the inherent complexity of many-to-many relationships. Still, the assumption of independence between the layers remains a limitation in understanding the induced pressures and deficits, and consequently limits our understanding of frailty, fragility, and the cyber resilience of critical infrastructure systems. Thus, additional research is required to understand and model interdependence between layers of frail and fragile critical infrastructure systems.

Information Asymmetries

In this model of frailty and fragility for critical infrastructure, information asymmetry served as a catalyst to transform a system from a state of frailty into a state of fragility. There are various perspectives in the study of information asymmetry. One perspective is that of an imbalance of resources between attackers and defenders in networked environments.[54] Due to this imbalance, defenders are burdened with the responsibilities of constant monitoring and securing all possible entry points and network transactions, while attackers only have to find one flaw or lax entry point through which they can enter a network. Another particularly potent form of information asymmetry is that of the vectors of information spread, along with the social dynamics in which information is embedded and processed. This has led to the current

challenges facing information, where users are unable to discern between its truth or falsity, leading them to evaluate information relative to their local and social concerns.[55] Thus, what is information to one user becomes misinformation for another user and leads to rampant polarization, while being assisted by algorithmic mores and network structures. In the context of cyber defense capabilities, such asymmetries of information coupled with geopolitical and ideological conflict have become drivers of cyberwarfare and have been shown to impact critical infrastructure systems. Future research in this area is crucial in developing a robust understanding of the role of information spread in the resilience of critical infrastructure.

Implications for Future Research

This section presents interventions for frailty and fragility, as well as the need for building adversary and user profiles.

Interventions for Reducing Frailty and Fragility of Critical Infrastructure

Due to the dual urgencies imposed by the evolving threat landscape and the frailty and fragility of critical infrastructure systems, new lines of research into interventions for reducing frailty and fragility and improving cyber resilience are crucial. Future research in these areas will help provide support at all stages of the lifecycle of critical infrastructure from specification and design all the way up to the implementation and ongoing maturity phases.[56]

What is information to one user becomes misinformation for another user and leads to rampant polarization.

Further, frailty and fragility exist on a spectrum. A nuanced understanding of frailty and fragility in critical infrastructure will require models that incorporate varying degrees

of frailty, fragility, and cyber resilience while designing appropriate interventions. Cyber risk is never completely eliminated, so cyber resilience of frail and fragile critical infrastructure requires ongoing cross-disciplinary analysis.

Building Adversary Profiles and User Profiles

A development of cyber resilience for critical infrastructure systems requires an understanding of how users interact with these systems. While the NIST SP 800-160 discusses the notion of building adversary profiles, it is also necessary to understand the different ways to use and interact with critical infrastructure. Thus, along with building adversary profiles, there is a compelling reason to build user profiles for two reasons. Recent research has shown the importance of adaptive cybersecurity and developing user-specific security policies through modeling user behavior.[57] First, while the process of building adversary profiles targets mostly unknown, malicious, and covert entities, the process of building user profiles attempts to garner a nuanced understanding of how users interact with critical infrastructure. Second, due to the information asymmetries in cyber defense, it is challenging to build adversary profiles, since adversarial behavior cannot be enumerated as much as user behavior.

Users interact differently with critical infrastructure systems, and the ways in which users navigate cyberspace require further investigation. An understanding of user profiles in the context of interactions with critical infrastructure can help determine the difference between "what users do" and "what users should do."[58] Such an approach complements the process of building adversary profiles, since certain types of adversaries target certain types of users. Recent research in the area of developing immune systems for cyber resilience benefits from such targeted understanding of user behaviors and helps address issues of system frailty and fragility.[59] With critical

Cyber risk is never completely eliminated, so cyber resilience of frail and fragile critical infrastructure requires ongoing cross-disciplinary analysis.

infrastructure systems too, there is a need for different immune system profiles and interventions to increase cyber resilience.

Conclusion

The causes of frailty and fragility in critical infrastructure as a consequence of broader socio-economic and political factors exert a variety of pressures on critical infrastructure. Using the pace layering framework, this study introduced a model for analyzing frailty and fragility in the context of cyber resilience and provided a novel interdisciplinary framework for examining how critical infrastructure systems react to the different demands placed on them over time. An analysis of frailty and fragility in critical infrastructure creates a pressing need for future research in this area, given several factors such as the aging of critical infrastructure, evolving information systems, user behaviors, burgeoning application domains, and nature of adversarial activities in these environments.

About the Author

Renita Murimi is a professor of instruction in the Jindal School of Management at the University of Texas at Dallas. She holds a PhD and MS in Electrical Engineering from New Jersey Institute of Technology, and a Bachelor of Engineering in Electronics and Communications from Manipal University in India. Her research interests trespass upon many disciplines, including network science, cybersecurity, blockchain, and computational social science. She is passionate about interdisciplinary explorations and was the co-recipient of the 2011 Bill and Melinda Gates Foundation's Grand Challenges Explorations Award for examination of the navigation behavior of the Aedes Aegypti mosquito.

Dr. Murimi has published widely in book chapters, academic journals, and peer-reviewed conference proceedings. Her first book, along with co-author Brett Bourbon, *Organized Skepticism in The Age of Misinformation: Surviving the Kingdom of Gossip* (Routledge, 2025) was the recipient of the American Library Association's Choice commendation. It explores how information spreads in online networks and offers a new understanding of information as a form of gossip, while shedding light on the often overused and confused terms of our time: information, misinformation, and knowledge.

Notes

1. Cybersecurity and Infrastructure Security Agency, "Critical Infrastructure Security and Resilience," CISA, accessed February 27, 2026, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/.

2. Ken Miller, "Rural Texas Towns Report Cyberattacks That Caused One Water System to Overflow," *Texas Tribune*, April 19, 2024, https://www.texastribune.org/2024/04/19/texas-cyberattacks-russia/.

3. Semperis, "The State of Critical Infrastructure Resilience," *Semperis*, April 8, 2025, https://www.semperis.com/the-state-of-critical-infrastructure-resilence/.

4. Igor Linkov and Alexander Kott, "Fundamental Concepts of Cyber Resilience: Introduction and Overview," in *Cyber Resilience of Systems and Networks*, ed. Alexander Kott and Igor Linkov (Cham: Springer, 2019), 1–25.; Mareile Kaufmann, "Exercising Emergencies: Resilience, Affect and Acting Out Security," *Security Dialogue* 47, no. 2 (2016): 99–116, https://doi.org/10.1177/0967010615613209.

5. Frances H. Arnold et al., *PCAST: Report to the President on Strategy for Cyber-Physical Resilience: Fortifying Our Critical Infrastructure for a Digital World* (White House Office of Science and Technology Policy, 2024), https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/02/PCAST_Cyber-Physical-Resilience-Report_Feb2024.pdf.; Ron Ross et al., *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*, NIST Special Publication 800-160, vol. 2, rev. 1 (National Institute of Standards and Technology, 2021), https://doi.org/10.6028/NIST.SP.800-160v2r1.

6. John C. Doyle et al., "The 'Robust Yet Fragile' Nature of the Internet," *Proceedings of the National Academy of Sciences* 102, no. 41 (2005): 14497–502, https://doi.org/10.1073/pnas.0501426102.

7. Richard Danzig, "Surviving on a Diet of Poisoned Fruit" (Center for a New American Security, 2014).

8. Hélène Amieva et al., "Social Vulnerability Predicts Frailty: Towards A Distinction Between Fragility and Frailty?" *The Journal of Frailty & Aging* 11, no. 3 (2022): 318–23, https://doi.org/10.14283/jfa.2022.24.

9. Mahmoud Efatmaneshnik, Joseph Bradley, and Michael J. Ryan, "Complexity and Fragility in System of Systems," *International Journal of System of Systems Engineering* 7, no. 4 (2016): 294–312, https://doi.org/10.1504/IJSSE.2016.080323.

10. Gary J. Burgess, "Product fragility and damage boundary theory," *Packaging Technology and Science* 1, no. 1 (1988): 5–10, https://doi.org/10.1002/pts.2770010104.

11. Harry Blair and Katarina Ammitzboell, "First Steps in Post-Conflict Statebuilding: A UNDP-USAID Study" (U.S. Agency for International Development and United Nations Development Programme, 2007).; Verena Fritz and Alina Rocha Menocal, "Understanding State-Building from a Political Economy Perspective," *Overseas Development Institute* 21 (2007): 13.

12. Bruce Jones et al., "From Fragility to Resilience: Concepts and Dilemmas of Statebuilding in Fragile States" (research paper, Center on International Cooperation at New York University & International Peace Academy, 2008).

13. The Fund for Peace, "Fragile States Index," The Fund for Peace, accessed February 27, 2026, http://fsi.fundforpeace.org/.

14. Andrea Abel et al., "The OECD Fragility Framework," *States of Fragility 2016 Understanding Violence: Understanding Violence* 69 (2016).

15. Rodrigo Cordero, *Crisis and Critique: On the Fragile Foundations of Social Life* (Routledge, 2016).; Jonathan Kuyper, Heike Schroeder, and Björn-Ola Linnér, "The Evolution of the UNFCCC," *Annual Review of Environment and Resources* 43, no. 1 (2018): 343–68, https://doi.org/10.1146/annurev-environ-102017-030119.; Richard Monastersky and Nick Sousanis, "The Fragile Framework: Can Nations Unite to Save Earth's Climate?" *Nature* 527, no. 7579 (2015): S1.

16. Berry Tholen, "Holding It All Together: On the Value of Compromise and the Virtues of Compromising," *Human Studies* 45, no. 3 (2022): 493–508, https://doi.org/10.1007/s10746-022-09638-2.

17. David Snow and Richard Machalek, "On the Presumed Fragility of Unconventional Beliefs," *Journal for the Scientific Study of Religion* 21, no. 1 (1982): 15–26, https://doi.org/10.2307/1385566.; Anthony Ziegelmeyer et al., "Fragility of Information Cascades: An Experimental Study Using Elicited Beliefs," *Experimental Economics* 13, no. 2 (2010): 121–45, https://doi.org/10.1007/s10683-009-9232-x.; Botond Kőszegi, George Loewenstein, and Takeshi Murooka, "Fragile Self-Esteem," *The Review of Economic Studies* 89, no. 4 (July 2022): 2026–60, https://doi.org/10.1093/restud/rdab060.; Arie W. Paradise and Michael H. Kernis, "Self-Esteem and Psychological Well-Being: Implications of Fragile Self-Esteem," *Journal of Social and Clinical Psychology* 21, no. 4 (2002): 345–61, https://doi.org/10.1521/jscp.21.4.345.22598.; Ghassan Baliki et al., "Micro-foundations of Fragility: Concepts, Measurement and Application" (IZA Discussion Paper No. 11188, December 2017), https://hdl.handle.net/10419/174098.; Christopher P. Ditzfeld and Carolin J. Showers, "Self-Structure: The Social and Emotional Contexts of Self-Esteem," in *Self-Esteem*, ed. Michael H. Kernis (Psychology Press, 2013), 21–42.

18. Pierluigi Mancarella and Farhad Billimoria, "The Fragile Grid: The Physics and Economics of Security Services in Low-Carbon Power Systems," *IEEE Power and Energy Magazine* 19, no. 2 (2021): 79–88, https://doi.org/10.1109/MPE.2020.3043570.; Jens Ludwig and Sendhil Mullainathan, "Fragile Algorithms and Fallible Decision-Makers: Lessons from the Justice System," *Journal of Economic Perspectives* 35, no. 4 (2021): 71–96, https://doi.org/10.1257/jep.35.4.71.; Atif Ansar et al., "Big is Fragile," in *The Oxford Handbook of Megaproject Management* (Oxford University Press, 2017), 60–95.; Nassim Nicholas Taleb, *Antifragile: Things That Gain from Disorder* (Random House, 2012).

19. Christopher J. Tignanelli and L. D. Napolitano, "The Fragility Index in Randomized Clinical Trials as a Means of Optimizing Patient Care," *JAMA Surgery* 154, no. 1 (January 2019): 74–79, https://doi.org/10.1001/jamasurg.2018.4318.; Benjamin R. Baer et al., "Fragility Indices for Only Sufficiently Likely Modifications," *Proceedings of the National Academy of Sciences* 118, no. 49 (2021): e2105254118, https://doi.org/10.1073/pnas.2105254411.; Bo Ebenman and Tomas Jonsson, "Using Community Viability Analysis to Identify Fragile Systems and Keystone Species," *Trends in Ecology & Evolution* 20, no. 10 (2005): 568–75.

20. Deborah B. Rolfson et al., "Validity and Reliability of the Edmonton Frail Scale," *Age and Ageing* 35, no. 5 (September 2006): 526–29, https://doi.org/10.1093/ageing/afl041.; Nardi Steverink, "Measuring Frailty: Developing and Testing the GFI (Groningen Frailty Indicator)," *The Gerontologist* 41 (2001): 236.; Ronald J. Gobbens et al., "The Predictive Validity of the Tilburg Frailty Indicator: Disability, Health Care Utilization, and Quality of Life in a Population at Risk," *The Gerontologist* 52, no. 5 (October 2012): 619–31, https://doi.org/10.1093/geront/gnr135.

21. Kenneth Rockwood, Morgan Andrew, and Arnold Mitnitski, "A Comparison of Two Approaches to Measuring Frailty in Elderly People," *Journal of Gerontology: Series A Biological Sciences and Medical Sciences* 62, no. 7 (July 2007): 738–43, https://doi.org/10.1093/gerona/62.7.738.; Arnold B. Mitnitski, Andrew J. Mogilner, and Kenneth Rockwood, "Accumulation of Deficits as a Proxy Measure of Aging," *The Scientific World Journal* 1 (August 8, 2001): 323–36, https://doi.org/10.1100/tsw.2001.58.; Ronald J. Gobbens et al., "Towards an Integral Conceptual Model of Frailty," *Journal of Nutrition, Health & Aging* 14, no. 3 (March 2010): 175–81, https://doi.org/10.1007/s12603-010-0045-6.

22. Andrew Clegg et al., "Frailty in Elderly People," *The Lancet* 381, no. 9868 (2013): 752–62.

23. Linda P. Fried, Alan A. Cohen, and Qi-Long Xue, "The Physical Frailty Syndrome as a Transition from Homeostatic Symphony to Cacophony," *Nature Aging* 1 (2021): 36–46, https://doi.org/10.1038/s43587-020-00017-z.

24. Stewart Brand, "Pace Layering: How Complex Systems Learn and Keep Learning," *Journal of Design and Science* 3 (2018): 1575, https://doi.org/10.21428/7f2e5f08.

25. Laura À. Pérez-Sánchez, Raúl Velasco-Fernández, and Mario Giampietro, "Factors and Actions for the Sustainability of the Residential Sector. The Nexus of Energy, Materials, Space, and Time Use," *Renewable and Sustainable Energy Reviews* 161 (2022): 112388, https://doi.org/10.1016/j.rser.2022.112388.; Rachel Clarke et al., "More-than-human Participation: Design for Sustainable Smart City Futures," *Interactions* 26, no. 3 (2019): 60–63, https://doi.org/10.1145/3319075.

26. D. Grant Campbell and Karl V. Fast, "From Pace Layering to Resilience Theory: The Complex Implications of Tagging for Information Architecture" (paper presented at the Proceedings of IA Summit, 2006).

27. Matthew I. Beane and Paul M. Leonardi, "Pace Layering as A Metaphor for Organizing in the Age of Intelligent Technologies: Considering the Future of Work by Theorizing the Future of Organizing," *Journal of Management Studies* 62, no. 5 (2025): 2025–52, https://doi.org/10.1111/joms.12867.

28. Erin Kenneally, "Ransomware: A Darwinian Opportunity for Cyber Insurance," *Connecticut Insurance Law Journal* 28 (2021): 165.

29. Brand, "Pace Layering."

30. Laila Kearney, "US Electric Grid Growing More Vulnerable to Cyberattacks, Regulator Says," *Reuters*, April 4, 2024, https://www.reuters.com/technology/cybersecurity/us-electric-grid-growing-more-vulnerable-cyberattacks-regulator-says-2024-04-04/.

31. BBC News, "Ukrainian Power Grid 'Lucky' to Withstand Russian Cyber-Attack," *BBC News*, April 8, 2022, https://www.bbc.com/news/technology-61085480.

32. Center for Internet Security, "Killnet Group Targeting Ukraine Supporters with DDoS Attacks," *CIS Security Insights*, August 1, 2022, https://www.cisecurity.org/insights/blog/killnet-group-targeting-ukraine-supporters-with-ddos-attacks/.

33. Sofia Liemann Escobar and James Barr, "Hack-and-Leak Operations in Latin America: The Case of Guacamaya," *Journal of Cyber Policy* 9, no. 3 (2024): 333–50, https://doi.org/10.1080/23738871.2024.2419509.

34. Eclypsium, "CISA: Over Half of Top Routinely Exploited Vulnerabilities in 2023 Affected Network Devices and Infrastructure," *Eclypsium Blog*, November 22, 2024, https://eclypsium.com/blog/cisa-routinely-exploited-vulnerabilities-key-takeaways/.

35. National Security Agency, *UEFI Secure Boot Customization*, NSA Technical Report, March 2023, https://media.defense.gov/2023/mar/20/2003182401/-1/-1/0/ctr-uefi-secure-boot-customization-20230317.pdf.

36. MSSP Alert, "Unsecured Mars Hydro Database Exposes 2.7 Billion Records.".

37. Paul Mell and Inna Bojanova, *Hardware Security Failure Scenarios: Potential Hardware Weaknesses*, NIST IR 8517 (National Institute of Standards and Technology, 2024), https://doi.org/10.6028/NIST.IR.8517.

38. Microsoft Threat Intelligence and Microsoft Defender Experts, "Phishing Campaign Impersonates Booking.com, Delivers a Suite of Credential-Stealing Malware," *Microsoft Security Blog*, March 13, 2025, https://www.microsoft.com/en-us/security/blog/2025/03/13/phishing-campaign-impersonates-booking-com-delivers-a-suite-of-credential-stealing-malware/.

39. Brightside Team, "AI-Generated Phishing vs Human Attacks: 2025 Risk Analysis," *Brightside AI Blog*, October 24, 2025, https://www.brside.com/blog/ai-generated-phishing-vs-human-attacks-2025-risk-analysis/.

40. Industrial Cyber, "ZipLine Phishing Campaign Uses Social Engineering to Target Manufacturing, Critical Supply Chains," *Industrial Cyber*, August 28, 2025, https://industrialcyber.co/manufacturing/zipline-phishing-campaign-uses-social-engineering-to-target-manufacturing-critical-supply-chains/.

41. Samir Jarjoui, Renita Murimi, and Robert Murimi, "Communities Agency and Resilience: A Perspective Addressing Tragedy of the Cyber Commons," *Cyber Defense Review* (2024).

42. Josh Nadeau, "83% of Organizations Reported Insider Attacks in 2024," IBM Think, accessed February 27, 2026, https://www.ibm.com/think/insights/83-percent-organizations-reported-insider-threats-2024.

43. Josh Rogin, "NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History,'" *Foreign Policy*, July 9, 2012, https://www.foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/.

44. Cybersecurity Ventures, "Cybercrime to Cost the World $6 Trillion Annually by 2021," *Cybersecurity Ventures* (blog), accessed February 27, 2026, https://www.cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.

45. Carolyn Gruber and Allison Pytlak, "Cyber and Climate Threats: Shared Risks, Resilience, and Response Strategies," *Stimson Center* (blog), March 4, 2025, https://www.stimson.org/2025/cyber-and-climate-threats-shared-risks-resilience-and-response-strategies/.

46. Amieva, et al., "Social Vulnerability Predicts Frailty."

47. Acronis Threat Research Unit, "The Patch Reality Gap: How Fast SMBs Really Patch and What Are the Risks," *Acronis*, accessed February 27, 2026, https://www.acronis.com/en/tru/posts/the-patch-reality-gap-how-fast-smbs-really-patch-and-what-are-the-risks/.

48. Pragmatic Coders, "2025 Legacy Code Stats: Costs, Risks & Modernization," Pragmatic Coders, accessed February 27, 2026, https://www.pragmaticcoders.com/resources/legacy-code-stats.

49. CISA, "Compromise of U.S. Water Treatment Facility."

50. Jaclyn Diaz, "A Fire and Cyberattack Cause Major Blackouts Across Puerto Rico," *NPR*, June 11, 2021, https://www.npr.org/2021/06/11/1005413481/a-fire-and-cyberattack-cause-major-blackouts-across-puerto-rico.

51. Samir Jarjoui, Robert Murimi, and Renita Murimi, "Hold My Beer: A Case Study of How Ransomware Affected an Australian Beverage Company," in *Proceedings of the 2021 IEEE International Conference on Cyber Situational Awareness, Data Analytics and Assessment* (IEEE, 2021), 1–6, https://doi.org/10.1109/CyberSA52016.2021.9478239.

52. Cybersecurity and Infrastructure Security Agency, "Understanding Ransomware Threat Actors: LockBit," CISA, June 14, 2023, https://www.cisa.gov/sites/default/files/2023-06/aa23-165a_understanding_TA_LockBit_0.pdf.

53. Myriam Dunn Cavelty, Christine Eriksen, and Benjamin Scharte, "Making Cyber Security More Resilient: Adding Social Considerations to Technological Fixes," *Journal of Risk Research* 26, no. 7 (2023): 801–14, https://doi.org/10.1080/13669877.2023.2208146.

54. Graham H. Todd, "Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition," *Air Force Law Review* 64 (2009): 65.; Guy-Philippe Goldstein, "Cyber Defense from 'Reduction in Asymmetrical Information' Strategies," *Military and Strategic Affairs* 5, no. 3 (2013): 129–55.

55. Brett Bourbon and Renita Murimi, *Organized Skepticism in the Age of Misinformation: Surviving the Kingdom of Gossip* (CRC Press, 2025).

56. Georgios Michail Makrakis et al., "Industrial and Critical Infrastructure Security: Technical Analysis of Real-Life Security Incidents," *IEEE Access* 9 (2021): 165295–325, https://doi.org/10.1109/ACCESS.2021.3133348.

57. Arwa AlQadheeb, Siddhartha Bhattacharyya, and Samuel Perl, "Enhancing Cybersecurity by Generating User-Specific Security Policy Through the Formal Modeling of User Behavior," *Array* 14 (2022): 100146, https://doi.org/10.1016/j.array.2022.100146.; Joyce H. Addae et al., "Exploring User Behavioral Data for Adaptive Cybersecurity," *User Modeling and User-Adapted Interaction* 29, no. 3 (2019): 701–50, https://doi.org/10.1007/s11257-019-09236-5.

58. Robert Murimi, Sandra Blanke, and Renita Murimi, "A Decade of Development of Mental Models in Cybersecurity and Lessons for the Future," in *Proceedings of the International Conference on Cybersecurity, Situational Awareness*

and Social Media: Cyber Science, ed. Robert Murimi et al. (Springer Nature, 2023), 105–32.

59. Hussain M. Mustafa et al., "Building Cyber-Attack Immunity in Electric Energy System Inspired by Infectious Disease Ecology," *IEEE Access* 12 (2024): 175338–56, https://doi.org/10.1109/ACCESS.2024.3497896.

Bibliography

Abel, Andrea, David Hammond, Daniel Hyslop, Reza Lahidji, and Daniel Frederik Mandrella. "The OECD Fragility Framework." *States of Fragility 2016 Understanding Violence: Understanding Violence* 69 (2016).

Acronis Threat Research Unit. "The patch reality gap: How fast SMBs really patch and what are the risks." *Acronis* (website). Available at: https://www.acronis.com/en/tru/posts/the-patch-reality-gap-how-fast-smbs-really-patch-and-what-are-the-risks/.

Addae, Joyce H., Xu Sun, Dave Towey, and Milena Radenkovic. "Exploring User Behavioral Data for Adaptive Cybersecurity." *User Modeling and User-Adapted Interaction* 29, no. 3 (2019): 701-750. https://doi.org/10.1007/s11257-019-09236-5.

AlQadheeb, Arwa, Siddhartha Bhattacharyya, and Samuel Perl. "Enhancing Cybersecurity by Generating User-Specific Security Policy Through the Formal Modeling of User Behavior." *Array* 14 (2022): 100146. https://doi.org/10.1016/j.array.2022.100146.

Amieva, Hélène, C. Ouvrard-Brouillou, Jean François Dartigues, Karine Pérès, Maturin Tabue Teguo, and José Alberto Avila-Funes. "Social Vulnerability Predicts Frailty: Towards A Distinction Between Fragility and Frailty?" *The Journal of Frailty & Aging* 11, no. 3 (2022): 318-323. https://doi.org/10.14283/jfa.2022.24.

Ansar, Atif, Bent Flyvbjerg, Alexander Budzier, and Daniel Lunn. "Big is Fragile." *The Oxford Handbook of Megaproject Management* (2017): 60-95.

Arnold, Frances H., Arati Prabhakar, Maria T. Zuber, Dan E. Arvizu, Dennis Assanis, John Banovetz, et al., "PCAST: Report to the President on Strategy for Cyber-Physical Resilience: Fortifying Our Critical Infrastructure for a Digital World." White House Office of Science and Technology Policy (OSTP), Washington, DC (United States), 2024. Available at: https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/02/PCAST_Cyber-Physical-Resilience-Report_Feb2024.pdf.

Baer, Benjamin R., Mario Gaudino, Mary Charlson, Stephen E. Fremes, and Martin T. Wells. "Fragility Indices for Only Sufficiently Likely Modifications." *Proceedings of the National Academy of Sciences* 118, no. 49 (2021): e2105254118. https://doi.org/10.1073/pnas.2105254118.

BBC News. "Ukrainian Power Grid 'Lucky' to Withstand Russian Cyber-Attack." *BBC News*, April 8, 2022. https://www.bbc.com/news/technology-61085480.

Beane, Matthew I., and Paul M. Leonardi. "Pace Layering as A Metaphor for Organizing in the Age of Intelligent Technologies: Considering the Future of Work by Theorizing the Future of Organizing." *Journal of Management Studies* 62, no. 5 (2025): 2025-2052. https://doi.org/10.1111/joms.12867.

Baliki, Ghassan, Tilman Brück, Neil TN Ferguson, and Sindu W. Kebede. "Micro-foundations of Fragility: Concepts, Measurement and Application." *IZA Discussion Papers* no. 11188 (2017). https://hdl.handle.net/10419/174098.

Blair, Harry, and Katarina Ammitzboell. "First Steps in Post-Conflict Statebuilding: A UNDP-USAID Study." *US Agency for International Development and United: Nations Development Programme* (2007).

Bourbon, Brett, and Renita Murimi. *Organized Skepticism in the Age of Misinformation: Surviving the Kingdom of Gossip*. CRC Press, 2025.

Brand, Stewart. "Pace Layering: How Complex Systems Learn and Keep Learning." *Journal of Design and Science* 3 (2018): 1575. https://doi.org/10.21428/7f2e5f08

Brightside Team. "AI-Generated Phishing vs Human Attacks: 2025 Risk Analysis." *Brightside AI Blog*, October 24, 2025. https://www.brside.com/blog/ai-generated-phishing-vs-human-attacks-2025-risk-analysis/.

Burgess, Gary J. "Product fragility and damage boundary theory." *Packaging Technology and Science* 1, no. 1 (1988): 5-10. https://doi.org/10.1002/pts.2770010104.

Campbell, D. Grant, and Karl V. Fast. "From Pace Layering to Resilience Theory: The Complex Implications of Tagging for Information Architecture." Proceedings of IA Summit (2006).

Center for Internet Security. "Killnet Group Targeting Ukraine Supporters with DDoS Attacks." *CIS Security Insights* (blog), August 1, 2022. https://www.cisecurity.org/insights/blog/killnet-group-targeting-ukraine-supporters-with-ddos-attacks/

Clarke, Rachel, Sara Heitlinger, Ann Light, Laura Forlano, Marcus Foth, and Carl DiSalvo. "More-than-human Participation: Design for Sustainable Smart City Futures." *Interactions* 26, no. 3 (2019): 60-63. https://doi.org/10.1145/3319075.

Clegg, Andrew, John Young, Steve Iliffe, Marcel Olde Rikkert, and Kenneth Rockwood. "Frailty in Elderly People." *The Lancet* 381, no. 9868 (2013): 752-762.

Cordero, Rodrigo. *Crisis and Critique: On the Fragile Foundations of Social Life*. Routledge, 2016.

Cybersecurity and Infrastructure Security Agency. "Compromise of U.S. Water Treatment Facility." *CISA* (Cybersecurity Advisory AA21-042A), February 11, 2021. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-042a.

Cybersecurity and Infrastructure Security Agency. "Critical Infrastructure Security and Resilience." *CISA* (website). Accessed February 27, 2026. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/.

Cybersecurity and Infrastructure Security Agency, "Understanding Ransomware Threat Actors: LockBit." *CISA,* June 14, 2023, https://www.cisa.gov/sites/default/files/2023-06/aa23-165a_understanding_TA_LockBit_0.pdf.

Cybersecurity Ventures. "Cybercrime to Cost the World $6 Trillion Annually by 2021." *Cybersecurity Ventures* (blog). Accessed February 27, 2026. https://www.cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.

Danzig, Richard. "Surviving on a Diet of Poisoned Fruit." *Center for a New American Security* (2014).

Diaz, Jaclyn. "A Fire and Cyberattack Cause Major Blackouts Across Puerto Rico." *NPR*. June 11, 2021. https://www.npr.org/2021/06/11/1005413481/a-fire-and-cyberattack-cause-major-blackouts-across-puerto-rico.

Ditzfeld, Christopher P., and Carolin J. Showers. "Self-structure: The social and emotional contexts of self-esteem." In *Self-esteem*, pp. 21-42. Psychology Press, 2013.

Doyle, John C., David L. Alderson, Lun Li, Steven Low, Matthew Roughan, Stanislav Shalunov, Reiko Tanaka, and Walter Willinger. "The "Robust Yet Fragile" Nature of the Internet." *Proceedings of the National Academy of Sciences* 102, no. 41 (2005): 14497-14502. https://doi.org/10.1073/pnas.0501426102.

Dunn Cavelty, Myriam, Christine Eriksen, and Benjamin Scharte. "Making Cyber Security More Resilient: Adding Social Considerations to Technological Fixes." *Journal of Risk Research* 26, no. 7 (2023): 801-814. https://doi.org/10.1080/13669877.2023.2208146.

Ebenman, Bo, and Tomas Jonsson. "Using Community Viability Analysis to Identify Fragile Systems and Keystone Species." *Trends in Ecology & Evolution* 20, no. 10 (2005): 568-575.

Eclypsium, "CISA: Over Half of Top Routinely Exploited Vulnerabilities in 2023 Affected Network Devices and Infrastructure," *Eclypsium Blog*, November 22, 2024, https://eclypsium.com/blog/cisa-routinely-exploited-vulnerabilities-key-takeaways/?utm_source=chatgpt.com.

Efatmaneshnik, Mahmoud, Joseph Bradley, and Michael J. Ryan. "Complexity and Fragility in System of Systems." *International Journal of System of Systems Engineering* 7, no. 4 (2016): 294-312. https://doi.org/10.1504/IJSSE.2016.080323.

Fried, Linda P., Alan A. Cohen, Qi-Long Xue, et al. "The Physical Frailty Syndrome as a Transition from Homeostatic Symphony to Cacophony." *Nature Aging* 1 (2021): 36–46. https://doi.org/10.1038/s43587-020-00017-z.

Fritz, Verena, and Alina Rocha Menocal. "Understanding State-Building from a Political Economy Perspective." *Overseas Development Institute* 21, no. 2009 (2007): 13.

Gobbens, Ronald J., Kim G. Luijkx, Monique T. Wijnen-Sponselee, and Jos M. Schols. "Towards an Integral Conceptual Model of Frailty." *Journal of Nutrition, Health & Aging* 14, no. 3 (March 2010): 175–181. https://doi.org/10.1007/s12603-010-0045-6 .

Gobbens, Ronald J., Martijn A. van Assen, Kim G. Luijkx, and Jos M. Schols. "The Predictive Validity of the Tilburg Frailty Indicator: Disability, Health Care Utilization, and Quality of Life in a Population at Risk." *The Gerontologist* 52, no. 5 (October 2012): 619–631. https://doi.org/10.1093/geront/gnr135 .

Goldstein, Guy-Philippe. "Cyber Defense from "Reduction in Asymmetrical Information" Strategies." *Military and Strategic Affairs* 5, no. 3 (2013): 129-155.

Gruber, Carolyn, and Allison Pytlak. "Cyber and Climate Threats: Shared Risks, Resilience, and Response Strategies." *Stimson Center* (blog). March 4, 2025. https://www.stimson.org/2025/cyber-and-climate-threats-shared-risks-resilience-and-response-strategies/.

Industrial Cyber, "ZipLine Phishing Campaign Uses Social Engineering to Target Manufacturing, Critical Supply Chains," *Industrial Cyber* (website), August 28, 2025, https://industrialcyber.co/manufacturing/zipline-phishing-campaign-uses-social-engineering-to-target-manufacturing-critical-supply-chains/.

Jarjoui, Samir, Renita Murimi, and Robert Murimi. "Communities Agency and Resilience: A Perspective Addressing Tragedy of the Cyber Commons." *Cyber Defense Review* (2024).

Jarjoui, Samir, Robert Murimi, and Renita Murimi. "Hold My Beer: A Case Study of How Ransomware Affected an Australian Beverage Company." In *Proceedings of the 2021 IEEE International Conference on Cyber Situational Awareness, Data Analytics and Assessment*, (2021) 1-6. https://doi.org/10.1109/CyberSA52016.2021.9478239.

Jones, Bruce, Rahul Chandran, Elizabeth Cousens, Jenna Slotin, and Jake Sherman. "From Fragility to Resilience: Concepts and Dilemmas of Statebuilding in Fragile States." *New York: Center on International Cooperation at New York University & International Peace Academy (A Research Paper for the OECD Fragile States Group)* (2008).

Kaufmann, Mareile. "Exercising Emergencies: Resilience, Affect and Acting Out Security." *Security Dialogue* 47, no. 2 (2016): 99-116. https://doi.org/10.1177/0967010615613209.

Kearney, Laila. "US Electric Grid Growing More Vulnerable to Cyberattacks, Regulator Says." *Reuters*, April 4, 2024. https://www.reuters.com/technology/cybersecurity/us-electric-grid-growing-more-vulnerable-cyberattacks-regulator-says-2024-04-04/.

Kenneally, Erin. "Ransomware: A Darwinian Opportunity for Cyber Insurance." *Conn. Ins. LJ* 28 (2021): 165.

Kőszegi, Botond, George Loewenstein, and Takeshi Murooka. "Fragile Self-Esteem." *The Review of Economic Studies* 89, no. 4 (July 2022): 2026–2060. https://doi.org/10.1093/restud/rdab060.

Kuyper, Jonathan, Heike Schroeder, and Björn-Ola Linnér. "The Evolution of the UNFCCC." *Annual Review of Environment and Resources* 43, no. 1 (2018): 343-368. https://doi.org/10.1146/annurev-environ-102017-030119.

Liemann Escobar, Sofia, and James Barr. "Hack-and-Leak Operations in Latin America: The Case of Guacamaya." *Journal of Cyber Policy* 9, no. 3 (2024): 333–350. https://doi.org/10.1080/23738871.2024.2419509.

Linkov, Igor, and Alexander Kott. "Fundamental Concepts of Cyber Resilience: Introduction and Overview." In *Cyber Resilience of Systems and Networks*, pp. 1-25. Springer, Cham, 2019.

Ludwig, Jens, and Sendhil Mullainathan. "Fragile Algorithms and Fallible Decision-Makers: Lessons from the Justice System." *Journal of Economic Perspectives* 35, no. 4 (2021): 71-96. https://doi.org/10.1257/jep.35.4.71.

Makrakis, Georgios Michail, Constantinos Kolias, Georgios Kambourakis, Craig Rieger, and Jacob Benjamin. "Industrial and Critical Infrastructure Security: Technical Analysis of Real-Life Security Incidents." *IEEE Access* 9 (2021): 165295-165325. https://doi.org/10.1109/ACCESS.2021.3133348.

Mancarella, Pierluigi, and Farhad Billimoria. "The Fragile Grid: The Physics and Economics of Security Services in Low-Carbon Power Systems." *IEEE Power and Energy Magazine* 19, no. 2 (2021): 79-88. https://doi.org/10.1109/MPE.2020.3043570.

Mell, Paul, and Inna Bojanova. *Hardware Security Failure Scenarios: Potential Hardware Weaknesses*. NIST Interagency or Internal Report (NIST IR 8517). Gaithersburg, MD: National Institute of Standards and Technology, 2024. https://doi.org/10.6028/NIST.IR.8517.

Microsoft Threat Intelligence and Microsoft Defender Experts. "Phishing Campaign Impersonates Booking.com, Delivers a Suite of Credential-Stealing Malware." *Microsoft Security Blog*, March 13, 2025. https://www.microsoft.com/en-us/security/blog/2025/03/13/phishing-campaign-impersonates-booking-com-delivers-a-suite-of-credential-stealing-malware/.

Miller, Ken (Associated Press). "Rural Texas Towns Report Cyberattacks That Caused One Water System to Overflow." *Texas Tribune*, April 19, 2024. https://www.texastribune.org/2024/04/19/texas-cyberattacks-russia/.

Mitnitski, Arnold B., Andrew J. Mogilner, and Kenneth Rockwood. "Accumulation of Deficits as a Proxy Measure of Aging." *The Scientific World Journal* 1 (August 8, 2001): 323–336. https://doi.org/10.1100/tsw.2001.58.

Monastersky, Richard, and Nick Sousanis. "The Fragile Framework: Can Nations Unite to Save Earth's Climate?" *Nature* 527, no. 7579 (2015): S1.

Murimi, Robert, Sandra Blanke, and Renita Murimi. "A Decade of Development of Mental Models in Cybersecurity and Lessons for the Future." In *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media: Cyber Science*, Springer Nature Singapore, (2023) 105-132.

Mustafa, Hussain M., Sajan K. Sadanandan, Anurag K. Srivastava, Arif R. Sarwari, and Rebecca Reece. "Building Cyber-Attack Immunity in Electric Energy System Inspired by Infectious Disease Ecology." *IEEE Access 12* (2024): 175338-175356. https://doi.org/10.1109/ACCESS.2024.3497896.

Nadeau, Josh. "83% of Organizations Reported Insider Attacks in 2024." *IBM Think* (website). Accessed February 27, 2026. https://www.ibm.com/think/insights/83-percent-organizations-reported-insider-threats-2024.

National Security Agency, "UEFI Secure Boot Customization," *NSA Technical Report*, March 2023, https://media.defense.gov/2023/mar/20/2003182401/-1/-1/0/ctr-uefi-secure-boot-customization-20230317.pdf.

Paradise, Arie W., and Michael H. Kernis. "Self-Esteem and Psychological Well-Being: Implications of Fragile Self-Esteem." *Journal of Social and Clinical Psychology* 21, no. 4 (2002): 345–361. https://doi.org/10.1521/jscp.21.4.345.22598.

Pérez-Sánchez, Laura À., Raúl Velasco-Fernández, and Mario Giampietro. "Factors and Actions for the Sustainability of the Residential Sector. The Nexus of Energy, Materials, Space, and Time Use." *Renewable and Sustainable Energy Reviews* 161 (2022): 112388. https://doi.org/10.1016/j.rser.2022.112388.

Pragmatic Coders. "2025 Legacy Code Stats: Costs, Risks & Modernization." *Pragmatic Coders* (website), https://www.pragmaticcoders.com/resources/legacy-code-stats.

Rockwood, Kenneth, Morgan Andrew, and Arnold Mitnitski. "A Comparison of Two Approaches to Measuring Frailty in Elderly People." *Journal of Gerontology: Series A Biological Sciences and Medical Sciences* 62, no. 7 (July 2007): 738–743. https://doi.org/10.1093/gerona/62.7.738.

Rogin, Josh. "NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History.'" *Foreign Policy*, July 9, 2012. https://www.foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/.

Rolfson, Deborah B., Sunil R. Majumdar, Robert T. Tsuyuki, Adeel Tahir, and Kenneth Rockwood. "Validity and Reliability of the Edmonton Frail Scale." *Age and Ageing* 35, no. 5 (September 2006): 526–529. https://doi.org/10.1093/ageing/afl041.

Ross, Ron, Victoria Pillitteri, Richard Graubart, Deborah Bodeau, and Rosalie McQuaid. "Developing Cyber Resilient Systems: A Systems Security Engineering Approach." *NIST Special Publication (SP) 800-160*, 2, Rev. 1. (2021). https://doi.org/10.6028/NIST.SP.800-160v2r1.

Semperis, "The State of Critical Infrastructure Resilience," *Semperis* (website), April 8, 2025, https://www.semperis.com/the-state-of-critical-infrastructure-resilence/.

Snow, David, and Machalek, Richard. (1982). "On the Presumed Fragility of Unconventional Beliefs." *Journal for the Scientific Study of Religion*, 15-26. https://doi.org/10.2307/1385566.

Steverink, Nardi. "Measuring Frailty: Developing and Testing the GFI (Groningen Frailty Indicator)." *The Gerontologist* 41 (2001): 236.

Taleb, Nicholas. *Things That Gain from Disorder. New York City: Random House & Penguin* (2012).

The Fund for Peace. "Fragile States Index." *The Fund for Peace*. Accessed February 27, 2026. https://fragilestatesindex.org/.

Tignanelli, Christopher J., and L.D. Napolitano. "The Fragility Index in Randomized Clinical Trials as a Means of Optimizing Patient Care." *JAMA Surgery* 154, no. 1 (January 2019): 74–79. https://doi.org/10.1001/jamasurg.2018.4318.

Tholen, Berry. "Holding It All Together: On the Value of Compromise and the Virtues of Compromising." *Human Studies* 45, no. 3 (2022): 493-508. https://doi.org/10.1007/s10746-022-09638-2.

Todd, Graham H. "Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition." *Air Force Law Rev.* 64 (2009): 65.

Ziegelmeyer, Anthony, Frédéric Koessler, Juergen Bracht, and Eyal Winter. "Fragility of Information Cascades: An Experimental Study Using Elicited Beliefs." *Experimental Economics* 13, no. 2 (2010): 121-145. https://doi.org/10.1007/s10683-009-9232-x.

Building a Complex Adaptive National Immune System: Counterintelligence—the Core of This System

By Michael W. Parrott

Disclaimer: *Nothing in this manuscript should be interpreted as representing the official views or positions of the U.S. Government, the National Intelligence College, the Department of War, the United States Special Operations Command, or the Joint Special Operations University. Portions of this manuscript were developed, refined, or edited using Google's generative-AI tool Gemini Notebook and Copilot. The tools were used for research synthesis, structural suggestions, language refinement, and infographic rendition. All ideas, interpretations, and final text were reviewed and approved by the author.*

Abstract

The U.S. confronts an era of strategic competition characterized by continuous, ambiguous, and multi-domain conflicts. In this environment, authoritarian adversaries—principally the People's Republic of China (PRC) and the Russian Federation—conduct unrestricted, hybrid, and techno-cognitive warfare below the threshold of armed conflict. These adversaries operate as complex adaptive ecosystems, leveraging whole-of-state integration, ubiquitous technical surveillance (UTS), and globalized information architectures to erode U.S. advantages and siphon intellectual property. Yet, the U.S. intelligence community (IC) and the broader national security apparatus remain structurally anchored in a Newtonian, industrial-era model characterized by rigid hierarchy, compartmentalization, and bureaucratic complicatedness. Because 80–90 percent of targeted innovation resides in the commercial, academic, and private sectors, the traditional "guardians of secrets" model is obsolete.

The U.S. must abandon its legacy paradigm and adopt a complex adaptive system (CAS) identity, functioning operationally as an agile, learning, whole-of-society "national immune system." Counterintelligence (CI) is the sensory, integrative, and adaptive core of this immune system. By drawing on organizational theory, the Cynefin framework, Morieux and Tollman's Six Simple Rules, and the Anticipate–Adapt–Achieve (AAA) framework, the doctrinal, cultural, and structural reforms necessary to operationalize CI as the central nervous system of a national immune architecture, are postured for implementation. A new CI mindset concludes with a targeted call to action for policymakers, IC leaders, special operations forces (SOF), and private-sector executives to proactively detect, identify, exploit, and neutralize foreign intelligence entity (FIE) activities (see Fig. 1).

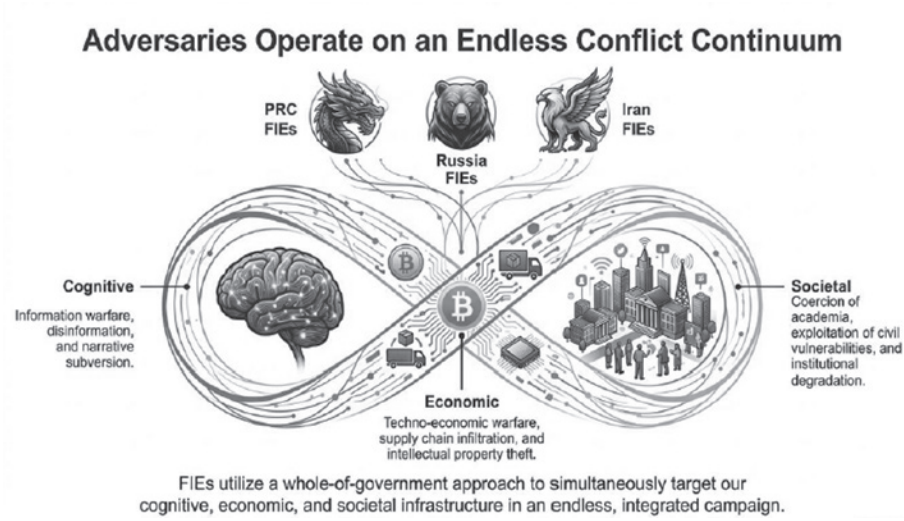


Figure 1 Endless Conflict Continuum–Adversarial Model. Source: Michael W. Parrott, created using Gemini Notebook, February 2026

The Epistemological Rupture and All-Domain Irregular Warfare

The U.S. must confront a fundamental epistemological rupture: the traditional Westphalian binary of peace and war is obsolete (see Fig. 2). Contemporary strategic competition is defined by a deliberate fusion of irregular warfare (IW), political warfare, and gray-zone activities across every domain. Adversaries pursue strategic objectives without triggering thresholds that would provoke a conventional U.S. military response. These adversaries operate along a continuous spectrum of conflict, designing campaigns specifically to bypass U.S.

Contemporary strategic competition is defined by a deliberate fusion of irregular warfare, political warfare, and gray-zone activities across every domain.

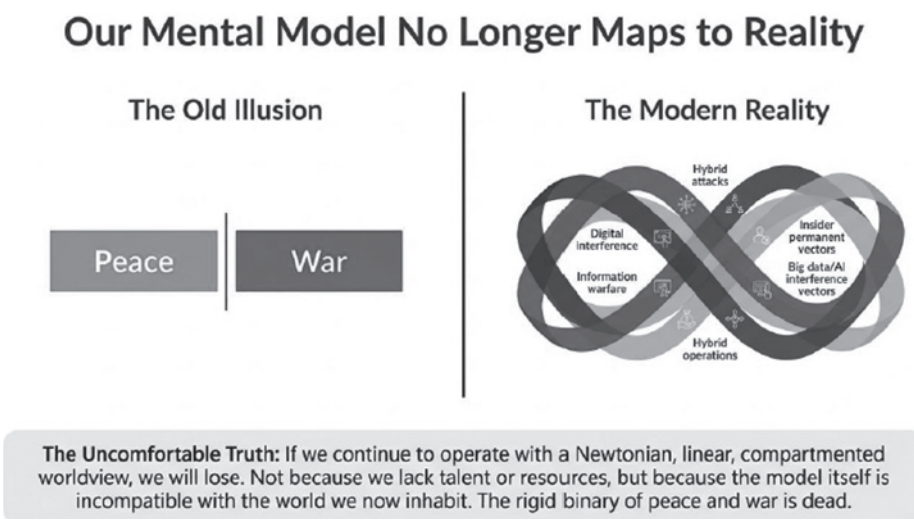


Figure 2. Breaking the Mental Model. Source: Michael W. Parrott, created using Gemini Notebook, February 2026

conventional military overmatch and hollow out our strategic dominance from within. The PRC's doctrine of Unrestricted Warfare asserts that the boundaries between military and civilian affairs have been erased.[1] Russia's hybrid warfare, rooted in the concept of "epistemic disorder," seeks to corrode a society's ability to distinguish truth from falsehood.[2]

Despite these realities, the U.S. remains intellectually and bureaucratically anchored in a Newtonian worldview. The true cost of this mismatch is measured not only in stolen military blueprints, but in lost futures—innovations not realized, markets not captured, and deterrence not maintained. Organizations like the Irregular Warfare Center rightly note that terms like "irregular warfare" must be reframed as "Defense Support to Strategic Competition" to align whole-of-government efforts.[3] This epistemological rupture reveals why the U.S. requires a national immune system capable of continuous sensing and adaptation—and why CI must serve as its core sensory and attribution function.

Structural Mismatch: Abandoning the Newtonian Machine

To understand why the U.S. struggles against networked threats, one must examine its structural DNA. The IC was built upon classical organization theory, emphasizing division of labor, hierarchical control, and rigid functional specialization.[4] This Newtonian machine design was effective for the industrial era but is insufficient against modern, nonlinear threats (see Fig. 3). Bureaucratic complicatedness—defined by Morieux and Tollman as the proliferation of rules, procedures, and oversight mechanisms—has become the default response to complexity.[5] The result is institutional paralysis and an inability to share information effectively across organizational boundaries.

David Snowden's Cynefin framework provides a useful lens (see Fig. 4). Developed by IBM in the late 1990s, Cynefin is a decision-making model that categorizes problems into five domains, namely simple, complicated, complex, chaotic, and disordered, each of which demands a different leadership and organizational response.

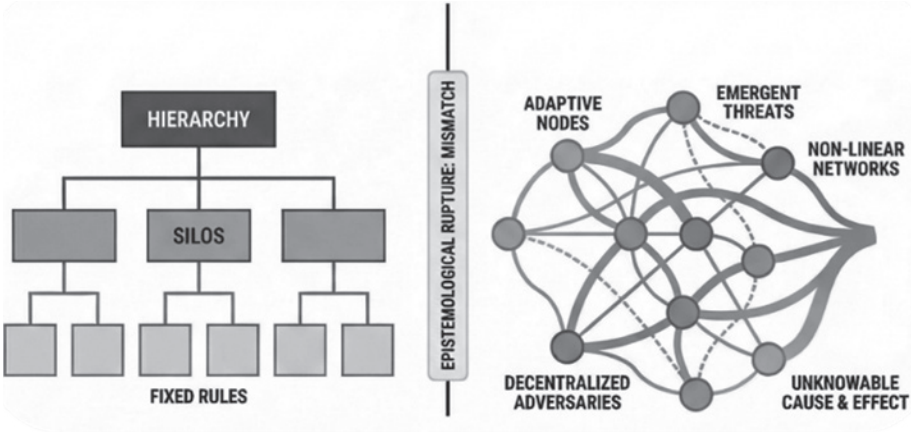


Figure 3. Epistemological Rupture–Mismatch. Source: Michael W. Parrott, created using Gemini Notebook, February 2026

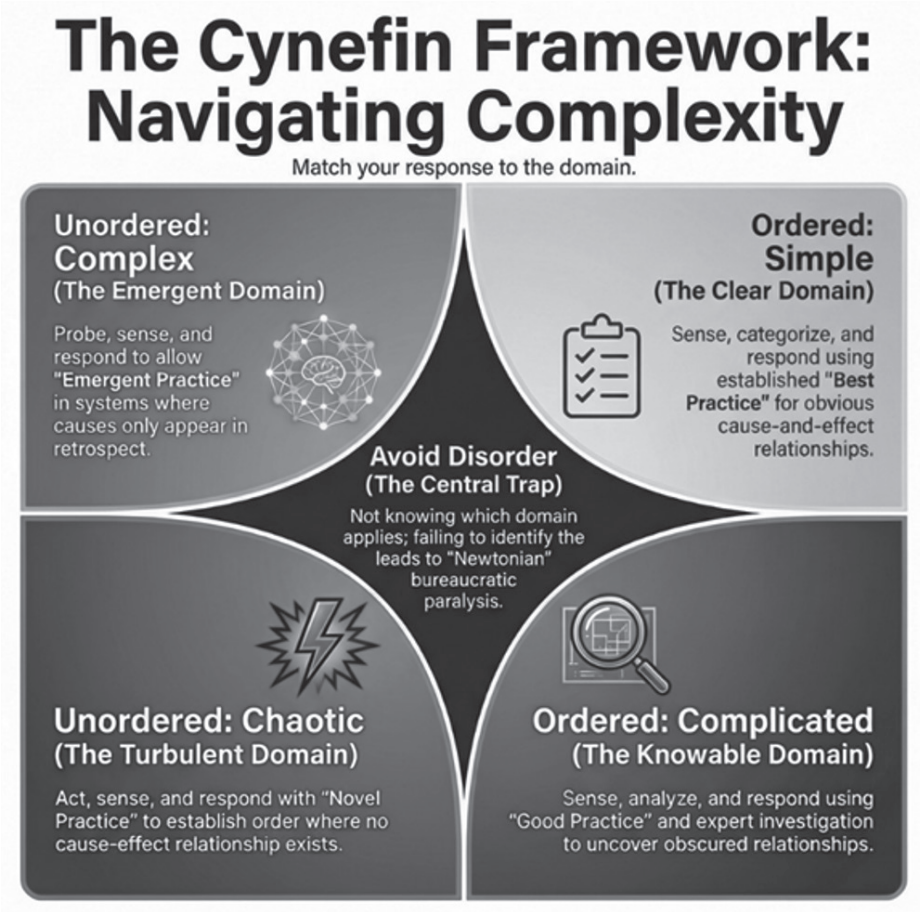


Figure 4. The Cynefin Framework. Source: Michael W. Parrott, created using Gemini Notebook, February 2026; original source Mind Tools "The Cynefin Framework: Using the Most Appropriate Problem-Solving Process," accessed January 1, 2019, https://www.mindtools.com/atddimk/the-cynefin-framework/

Classical bureaucracy, Snowden argues, is only suited for the "complicated" domain, where cause and effect are obscured yet discoverable through expert analysis (Sense-Analyze-Respond).[6]

Today's strategic competition, characterized by UTS, commercial espionage, and military-civil fusion, resides in the "complex" domain. In a complex environment, causality is non-linear, unpredictable, and emergent. A Newtonian machine cannot effectively "Sense-

Analyze-Respond" to a complex ecosystem; it must "Probe-Sense-Respond" through continuous, decentralized adaptation.[7] When IC leaders attempt to solve complex modern challenges using classical administrative structures, they create a "doom loop of management"—layering new compliance rules, offices, and processes on top of old ones, generating paralyzing bureaucratic complicatedness rather than true agility (see Fig. 5).[8] This structural mismatch demonstrates why the IC cannot function as the immune

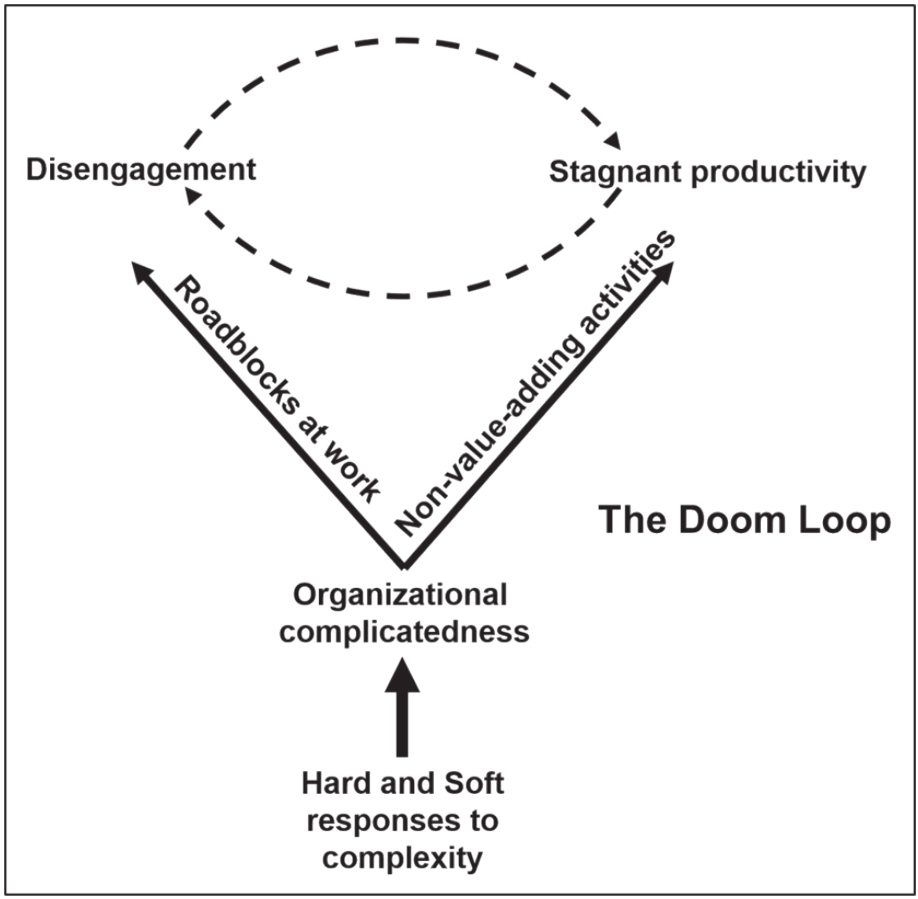


Figure 5. The Doom Loop. Yves Morieux and Peter Tollman. Source: "Six Simple Rules: How to Manage Complexity Without Getting Complicated," HBR Press, 2014

system of a complex national organism—and why CI must be reimagined as the adaptive connective tissue that enables systemic resilience.

Vignette 1: The Illusion of the Vault

For decades, U.S. CI operated under a vault-guarding mentality, where security meant locking classified data behind physical and digital doors and waiting for an adversary to pick the lock. When the PRC breached the Office of Personnel Management (OPM), stealing the clearance records of over 21 million federal employees, the failure was not merely technical; it wasn't just about weak passwords or outdated software. It was a matter of how the problem was framed. The U.S. treated personnel data as an administrative compliance issue whereas the PRC treated it as a strategic intelligence node within a complex targeting ecosystem. A Newtonian machine cannot defend against a systemic pathogen. See Figure 6.

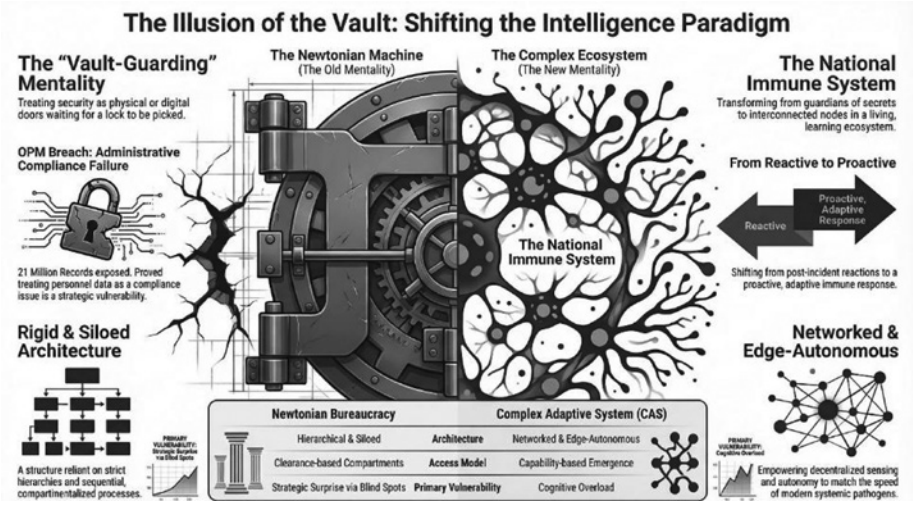


Figure 6. The Illusion of the Vault. Source: Michael W. Parrott, generated using Gemini Notebook, February 2026

The Behavioral Architecture: Smart Simplicity and the Complex Adaptive System Identity

To survive and dominate, reform cannot simply restructure the wiring diagram. Effective reform requires changing the way the IC thinks about complexity. A complex adaptive system (CAS) is characterized by distributed control, nonlinearity, and the ability of independent agents to self-organize and adapt to their environment.[9] The biological manifestation of a CAS is an immune system. Thus, the CI enterprise must evolve from passive guardians of secrets into an active, learning national immune system.

Morieux and Tollman's Six Simple Rules provide the behavioral architecture for this transformation. They argue that managing complexity requires maximizing autonomy and cooperation.[10] These rules counteract bureaucratic complicatedness by reinforcing integrators, increasing reciprocity, and rewarding cooperation. See Figure 7.

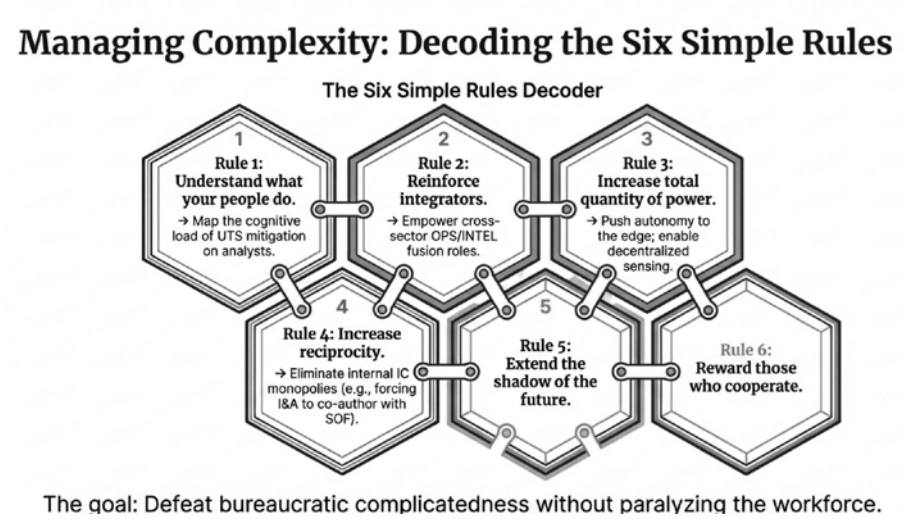


Figure 7. Managing Complexity – Decoding the Six Simple Rules. Source: Michael W. Parrott, image generated using Gemini Notebook and Yves Morieux and Peter Tollman, "Six Simple Rules: How to Manage Complexity Without Getting Complicated," HBR Press, 2014

Research from the National Intelligence University using the Invincibility Belief Index (IBI) demonstrates that intelligence professionals score exceedingly low on "impunity," reflecting a profound fear of punishment and a compliance-driven culture of caution.[11] Yet the IBI also reveals an activation lever for boldness: when professionals know their assessments directly impact lives or strategic outcomes, their comfort with high-confidence judgments increases dramatically. Leaders can activate this lever by applying Rule 5—"extend the shadow of the future"—connecting analytic decisions to operational consequences. For example, when IC analysts are required to directly brief SOF teams deploying to denied areas—or when corporate facility security officers are briefed on the direct financial ruin caused by a specific intellectual property theft—they consistently produce bolder and more operationally relevant assessments. By extending the shadow of the future and applying Rule 6 (*Reward those who cooperate*), leaders break the compliance-based mindset, impel autonomy, and replace bureaucratic timidity with decisive, adaptive agility.[12] These behavioral insights reveal why CI must be empowered as the immune system's adaptive decision-making layer, capable of sensing threats, coordinating responses, and learning faster than adversaries.

Operationalizing the National Immune System: Anticipate, Adapt, Achieve

If Smart Simplicity provides the behavioral substrate for a CAS-based CI enterprise, the AAA framework provides its operational logic. The AAA framework introduces an original CI doctrine that operationalizes CAS theory for strategic competition. It is not an analytic heuristic but a prescriptive model for synchronizing sensing, learning, and action across a whole-of-society CI ecosystem. *Anticipate* is the continuous sensing and forecasting of foreign intelligence campaigns before compromise occurs. *Adapt* is the

rapid reconfiguration of defenses, partnerships, and behaviors across sectors in response to emergent threat patterns. *Achieve* is the deliberate imposition of strategic costs that constrain adversary behavior, degrade hybrid warfare effectiveness, and shape the competitive environment in favor of U.S. interests. While Anticipate and Adapt enable learning and resilience, Achieve represents the framework's center of gravity. A CI enterprise that anticipates and adapts but fails to impose costs merely absorbs pressure. AAA is designed to convert intelligence advantage into strategic effect.

It is a prescriptive model intended to guide how the U.S. CI enterprise plans, integrates, and imposes costs across the gray zone. So, if organizational theory explains *why* we must change, and the Six Simple Rules explain *how* to change the behavioral architecture, the AAA framework provides the necessary output. By treating the CI enterprise as a CAS organism, the AAA framework translates theory into vital biological functions across the public and private sectors (see Table 1).

Table 1. Anticipate–Adapt–Achieve Framework Table

Pillar	Complex Adaptive System Function	Counter-intelligence Purpose	Operational Expressiony
Anticipate	Sensory network	Detect emergent foreign intelligence entity activity before compromise	Forecasting campaigns, data driven analytics and artificial intelligence, digital exhaust management, early-warning indicators
Adapt	Distributed immune response	Rapidly reconfigure defenses across sectors	Counterintelligence (CI)–industry fusion cells, behavioral vetting, secure research enclaves
Achieve	Pathogen neutralizationy	Impose costs and shape adversary behavior	Offensive CI, special operations forces-enabled attribution, strategic intelligence disclosure

Source: Michael W. Parrott, February 2026

- **Anticipate:** Anticipate shifts CI from reactive case management to forward-looking campaign detection in a UTS-saturated environment.
- **Adapt:** Adapt institutionalizes learning by distributing CI authority and responsibility across the national ecosystem.
- **Achieve:** Achieve converts intelligence advantage into strategic effect by imposing real costs on adversaries rather than merely defending against them.

AAA differs from the traditional intelligence cycle, which emphasizes collection and analysis, and from the OODA loop (Observe, Orient, Decide, & Act), which focuses on tactical decision advantage. AAA is oriented toward strategic behavior shaping and cost imposition over time. AAA provides the operational logic for CI to function as the immune system's sensory, adaptive, and cost-imposing mechanism. See Figure 8.

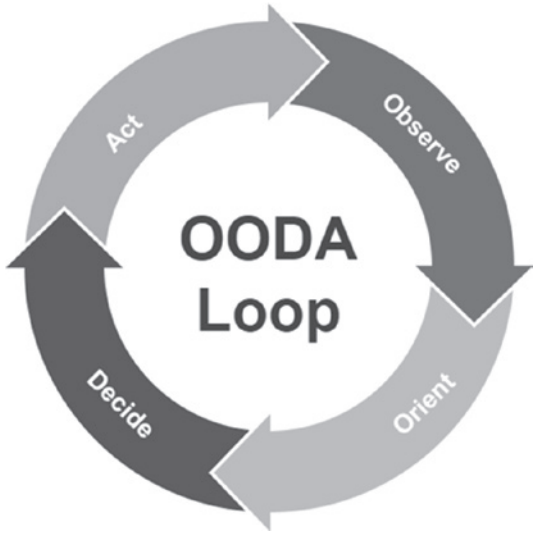


Figure 8. OODA (Observe, Orient, Decide, & Act) Loop Source: Michael W. Parrott, created using Gemini Notebook, January 2026

The Sensory Network (Anticipate): Defeating Ubiquitous Technical Surveillance and Illuminating the Threat

In the modern gray zone, the environment of UTS has collapsed operational anonymity. The democratization of data means that ordinary digital behavior—search histories, device signatures, and mobile metadata—is now persistent, analyzable, and exploitable by foreign intelligence entities (FIEs).[13] A Newtonian response attempts to go dark, which disastrously creates an anomaly of absence that alerts adversary algorithms. Therefore, to *anticipate* these threats, organizations must shift from reactive case-management to forecasting campaigns utilizing data-driven analytics and artificial intelligence (D2A2). D2A2 shifts from detection to deduction campaigns focused on determining adversarial intent through predictive analysis across domain vectors simultaneously (see Fig. 9).

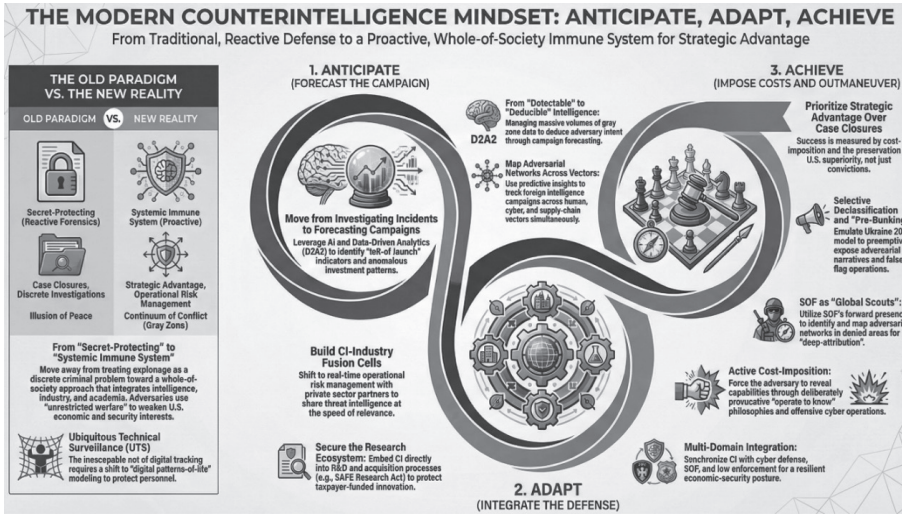


Figure 9. The Modern CI Mindset. Source: Michael W. Parrott, generated using Gemini Notebook, February 2026

Vignette 2: The Covert Deployment Mapped by Mobile Ads

Elite U.S. special operations units preparing for a clandestine mission deployed from critical military hubs. Operating under the assumption of anonymity, the operators practiced traditional physical operational security (OPSEC). However, they bled "digital exhaust" through seemingly innocuous commercial apps and advertising trackers on their smartphones. Analysts utilizing legally purchased, commercially available data tracked the operators' devices as they traveled from the U.S., through international transit points, and eventually clustered at a target location in northern Syria.[14]

The CAS/Immune System Takeaway: To survive UTS, a CAS approach requires operators to *anticipate* this commercial surveillance and actively manage, spoof, or blend their digital signatures into the local noise.

The Cellular Response (Adapt): Counterintelligence Industry Fusion-Industry Fusion

Because 80 to 90 percent of targeted innovation resides in the commercial and academic sectors, the U.S. government cannot be the sole defender. A CAS organism requires distributed immunity. The fallacy that fundamental research is immune to adversarial exploitation must be abandoned. Permanent, cross-boundary CI-industry fusion cells must be established utilizing frameworks like the Hoover Institution's Global Engagement Maturity Model (GEMM), a structured tool that helps research institutions assess and manage the risks of foreign engagement across five progressive levels of organizational readiness (see Fig. 10).[15] This shifts corporate and academic entities from ad-hoc participants into fully integrated, adaptive nodes of the national immune system. The GEMM CI-Industry Fusion Cycle accomplishes this end-state with four easy steps as depicted in the graphic. This anticipatory CI mindset

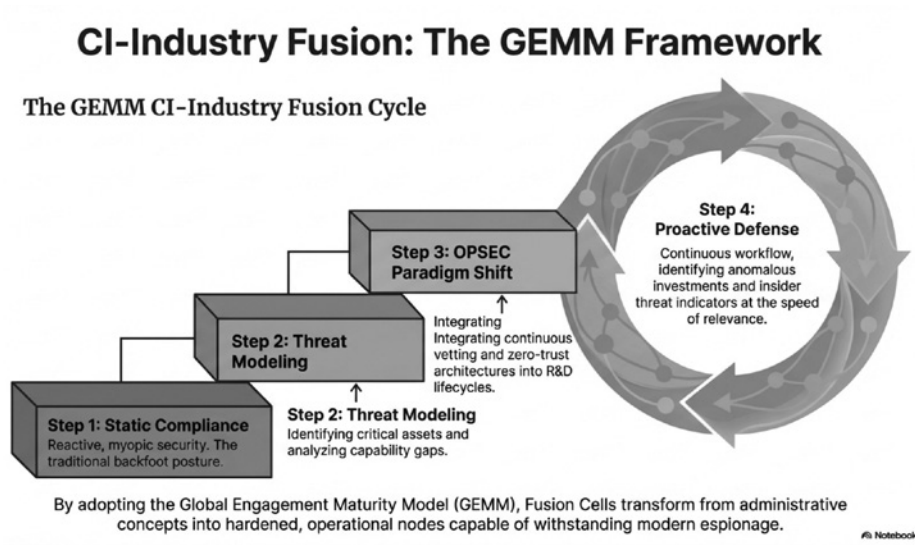


Figure 10. The GEMM-CI-Industry Fusion Cycle. Source: Michael W. Parrott, generated using Gemini Notebook and Glenn Tiffert, Jeffrey Stoff, and Kevin Gamache, "Global Engagement: Rethinking Risk in the Research Enterprise" (Hoover Institution Press, 2020), 120–135

requires commercial executives to treat CI as a strategic asset, leveraging supply-chain illumination and economic intelligence to map foreign investment vectors *before* proprietary data is legally siphoned away.

Vignette: The "Fox in the Henhouse" Academic Exploitation

A 2024 Congressional investigation revealed that over 700 U.S. Department of Defense (DoD)-funded research papers published between 2023 and 2025 were conducted in partnership with entities affiliated with China's defense research and industrial base.[16] In one instance, a 2025 publication on two-dimensional materials, funded by the Air Force Office of Scientific Research (AFOSR), was co-authored with researchers from China's National University of Defense Technology (NUDT)—the PLA's premier scientific research university, which has been on the U.S. Entity List since 2015.[17]

To achieve strategic advantage, the complex adaptive system organism must be prepared to confront and impose costs on adversaries, shed the intelligence community's legacy of absolute secrecy, and leverage offensive counterintelligence.

The CAS/Immune System Takeaway: Operating as a Newtonian bureaucracy, DoD Research and Engineering relied on outdated, rigid interpretations of National Security Decision Directive-189 (NSDD-189) regarding "fundamental research," treating grant funding merely as an administrative process. Adaptation means implementing secure computing enclaves and continuous behavioral vetting so that universities transition from being soft targets into critical nodes of early warning.[18]

Neutralizing the Pathogen (Achieve): Offensive Counterintelligence and SOF

To achieve strategic advantage, the CAS organism must be prepared to confront and impose costs on adversaries, shed the IC's legacy of absolute secrecy, and leverage offensive CI. The most potent weapon against Russian hybrid warfare and the doctrine of reflexive control is strategic intelligence disclosure (SID). Unlike traditional information operations, SID is rooted in verifiable intelligence, which makes it uniquely effective against hybrid warfare strategies that depend on plausible deniability. By selectively and preemptively declassifying intelligence, the IC establishes credible counter-narratives before an adversary's disinformation can take root. SID transforms intelligence from a hoarded commodity into an instrument of strategic shaping—it is emergent, offensive CI.

The U.S. application of *SID* prior to Russia's 2022 invasion of Ukraine illustrates SID in practice. By selectively declassifying

intelligence on Russian invasion timelines, false-flag preparations, and proxy narratives, the U.S. preempted Moscow's reflexive control strategy and denied it narrative surprise. This disclosure did not deter the invasion, but it materially constrained Russia's diplomatic maneuver space, fractured its information campaign, and enabled faster allied alignment, demonstrating how SID can impose strategic cost without military escalation.

Furthermore, SOF and CI professionals must be deployed as the global scouts of this immune system (see Fig. 11). Within a CI-CAS construct, SOF are not merely consumers of intelligence but active generators of CI effect. Operating persistently in denied and semi-permissive environments, SOF are uniquely postured and positioned to detect adversary proxy networks, commercial cutouts, and influence vectors that never rise to the threshold of traditional intelligence collection. SOF map adversarial proxy networks and generate the deep-attribution intelligence necessary to unhinge an adversary's decision-making cycle.[19] When integrated early with CI professionals, SOF planning can incorporate digital signature management, attribution generation, and partner-force vetting as core mission variables rather than ancillary OPSEC concerns. In this sense, SOF function as forward CI nodes-testing adversary-sensing mechanisms, mapping hybrid infrastructure, and feeding real-time data back into the national immune system. In the Achieve phase, SOF-enabled attribution—combined with offensive CI and selective disclosure—allows the U.S. to expose, disrupt, or delegitimize adversary networks without crossing kinetic thresholds.

Vignette: The Private Sector as the Arsenal

A major U.S. logistics and shipping firm partnered proactively with federal agencies through a CI-industry fusion cell to identify illicit procurement networks. By merging the firm's commercial

supply-chain telemetry with IC threat intelligence, the partnership identified a Russian "disposable agent" network attempting to acquire restricted unmanned aerial vehicle—UAV—components via shell companies. The U.S. government leveraged this data to enact targeted counter-threat finance sanctions, freezing the cryptocurrency wallets funding the network and dismantling the procurement pipeline (see Fig. 11).

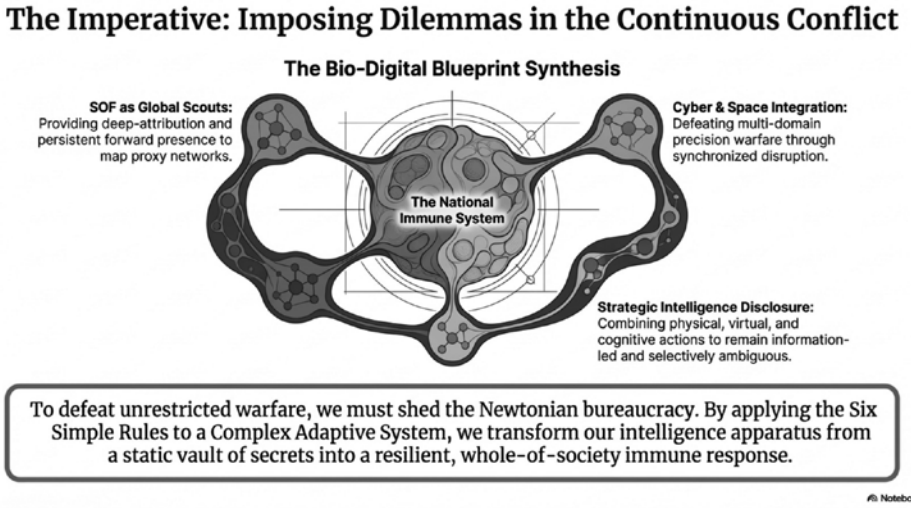


Figure 11. The Imperative: Imposing Dilemmas in the Continuous Conflict. Source: Michael W. Parrott, created using Gemini Notebook, February 2026

Vignette: The Smiao/RiverMerge LinkedIn Operation

A 2025 investigation uncovered a sophisticated Chinese intelligence operation targeting recently laid-off U.S. government and defense-sector employees. Operatives created a network of fake-front companies—such as "RiverMerge Strategies" and "DU Strategy"—complete with plagiarized websites, cloned logos, and synthetic personas. They used platforms like LinkedIn to post fake job listings for "strategic intelligence services" and "policy analysis,"

aiming to lure cleared personnel into providing sensitive insights under the guise of corporate consulting.[20]

The CAS/Immune System Takeaway: When adversaries weaponize commercial platforms and the global gig economy to conduct espionage, traditional security perimeters are meaningless. Achieving strategic advantage requires a whole-of-society immune response where private-sector threat intelligence (such as the FDD analysis uncovering the Smiao network) is rapidly fused with federal law enforcement to identify, expose, and neutralize the threat before cleared personnel are compromised.[21]

A Structural Counterargument: The Case for Intelligence-Based Bureaucracy

A serious critique holds that the IC's intelligence-, or INT-, based structure—CIA for human intelligence (HUMINT), National Security Agency for signals intelligence (SIGINT), National Reconnaissance Office /National Geospatial-Intelligence Agency for imagery—was a rational solution to the dysfunction of the pre-1947 era. Prior to the National Security Act, U.S. intelligence was fragmented across departments, producing redundant collection and interservice rivalry. Mark Lowenthal, former assistant director of Central Intelligence for Analysis & Production, adjunct professor at John Hopkins University, and acclaimed writer on the topic of intelligence, notes that INT-based organizations were designed to impose "unity of expertise" and clear functional responsibility.[22] From this perspective, the evolution of INT-based bureaucracies was not a pathology but a rational response to earlier chaos.

This historical logic underpins a broader critique: if HUMINT, SIGINT, geospatial intelligence (GEOINT), and open-source intelligence (OSINT) are not anchored in specific organizations with statutory authorities, budgetary control, and leadership accountability, they

risk becoming everyone's responsibility and no one's priority. The 9/11 Commission acknowledged that some redundancy is desirable to preserve analytic diversity and avoid single-point failure.[23] Competition between agencies—while often inefficient—has historically generated innovation, alternative analytic perspectives, and resilience. A CAS-based model that emphasizes integration and cooperation may inadvertently suppress the competitive tension that has driven advances in technical collection and analytic tradecraft.

A deeper critique argues that the IC is embedded in a Newtonian administrative state characterized by hierarchical departments, statutory authorities, and risk-averse legal cultures.[24] Reforming the IC into a CAS while the rest of the federal government remains bound by industrial-era governance may be structurally incoherent. As scholars of public administration have long noted, bureaucratic form is not merely an organizational choice but a reflection of constitutional design, political oversight, and administrative law.[25] If the IC depends on the Departments of State, Defense, Justice, and the White House for authorities, funding, and policy direction, can it realistically operate as a CAS without broader administrative reform?

Finally, critics argue that adversaries themselves are bureaucratic. The PRC and Russia are hierarchical and often sclerotic. If authoritarian systems cannot adopt CAS behavior, the U.S. IC's Newtonian character may be a shared condition of modern states. These critiques sharpen the need to clarify CI's role within the national immune system—not as a replacement for INTs, but as the integrative physiology that connects them.

Response and Synthesis: Why the Complex Adaptive System Model Still Prevails

These critiques are historically grounded and analytically serious but do not undermine this thesis. The first and most important point

The first and most important point is that the complex adaptive system model does not advocate abolishing human intelligence, signals intelligence, geospatial intelligence, or open-source intelligence organizations.

is that the CAS model does not advocate abolishing HUMINT, SIGINT, GEOINT, or OSINT organizations. Functional INT expertise remains indispensable. The critique is not of specialization but of governance and interaction. INTs remain the organs of the intelligence body; CAS is the physiology that connects them. This aligns with the 9/11 Commission's call for "unity of effort" and with ODNI's mission-management model, which—despite its limitations—was designed to improve integration without eliminating organizational identities, rather than structural dissolution.[26] CAS reform preserves functional expertise while rewiring incentives, feedback loops, and integration mechanisms that govern how INTs interact.

The counterargument that redundancy can be healthy is also correct. CAS does not eliminate redundancy; it disciplines it by seeking to eliminate pathological redundancy—multiple agencies competing for the same mission without shared awareness. CAS preserves multiple sensors, multiple analytic perspectives, and multiple pathways to insight but disciplines redundancy through integrators, shared incentives, and campaign-level coordination. Morieux and Tollman's rules reinforce integrators, reward cooperation, and extend the shadow of the future.[27] The Hoover Institution's GEMM provides a practical example: it does not dissolve universities into the IC; it creates maturity stages and feedback loops that align behavior with national-security risk.[28] GEMM provides a practical example of structured, incentive-driven cooperation.[29] CAS is not a return to pre-1947 chaos but a bounded autonomy model.

The administrative-state critique does not preclude reform. Goldwater-Nichols reshaped jointness without restructuring the entire DoD. U.S. Special Operations Command's creation introduced a functional, cross-cutting command without abolishing the services. Similarly, the Foreign Investment Risk Review Modernization Act (or FIRRMA) reformed the Committee on Foreign Investment in the U.S. (or CFIUS) processes without restructuring the Department of the Treasury. These examples show that targeted, functional reforms can succeed even when embedded in a broader Newtonian administrative state. CAS-aligned CI reform—through CI-industry fusion cells, the National Research Security, Integrity, and Compliance Center (or NRSICC), SID, and research-security baselines—can be implemented incrementally without requiring wholesale administrative revolution.

The U.S. does not need to mirror adversaries' political systems; it needs to match—and exceed—their adaptive capacity.

Finally, the critique that adversaries are themselves bureaucratic does not negate the need for U.S. adaptiveness. While the PRC and Russia are hierarchical, their behavior in key domains—technology acquisition, cyber operations, influence campaigns, and hybrid warfare—exhibits CAS-like emergent properties. PRC Military-Civil Fusion integrates state, industry, academia, and diaspora networks into a single techno-security ecosystem.[30] Russian hybrid warfare leverages decentralized proxies, criminal networks, and emergent influence operations that adapt rapidly to Western countermeasures.[31] The U.S. does not need to mirror adversaries' political systems; it needs to match—and exceed—their adaptive capacity. Indeed, the U.S. is uniquely

positioned to build a CAS national immune system because it possesses a dynamic private sector, autonomous universities, a culture of innovation, civil-society networks, and U.S. SOF with global access and persistent presence. CAS reform is therefore not about becoming like China or Russia; it is about becoming more like the U.S. at its best.

Integrative Supposition: Reconciling Structure, History, and Strategic Necessity

The counterarguments sharpen the thesis rather than weaken it. They demonstrate that INT-based organizations must remain intact, that bureaucratic identity is not the enemy—bureaucratic complicatedness is—and that CAS reform must be bounded, targeted, and incentive-driven. They also show that the U.S. can reform the IC without reforming the entire administrative state, and that adversaries' bureaucratic weaknesses make U.S. adaptiveness even more decisive.
The CAS national immune system model is not a rejection of the IC's history; it is the next evolutionary step. It preserves the functional strengths of INT-based organizations while addressing the structural, cultural, and cognitive limitations that adversaries exploit. In doing so, it provides a path for the U.S. to transition from absorbing foreign intelligence blows to shaping adversary decision-making at scale. The question is no longer whether the U.S. can afford to adopt a CAS-based CI posture. The question is whether it can afford not to. This synthesis demonstrates that CI is uniquely positioned to serve as the immune system's core because it alone spans government, industry, academia, and SOF, and because it alone integrates sensing, attribution, and cost imposition.

Conclusion: Counterintelligence as the Core of the National Immune System

The U.S. cannot win strategic competition using a rigid, compliance-driven machine rooted in industrial-era theory. Foreign intelligence activity by the PRC, Russia, and Iran represents the largest unmanaged strategic loss in the U.S. national power system. To survive and dominate, the U.S. must build a complex adaptive national immune system capable of sensing, learning, and adapting faster than adversaries—operationalizing the *Six Simple Rules*, leveraging the *Invincibility Belief Index* and extending the *shadow of the future*.

CI is the core of this immune system. CI is the organism's sensory network, detecting anomalies and mapping adversary campaigns. CI is the integrative tissue, fusing insights across government, industry, academia, and SOF. CI is the adaptive layer, enabling rapid reconfiguration of defenses. And CI is the cost-imposing mechanism, neutralizing threats through attribution, disruption, and SID. See Figure 12.

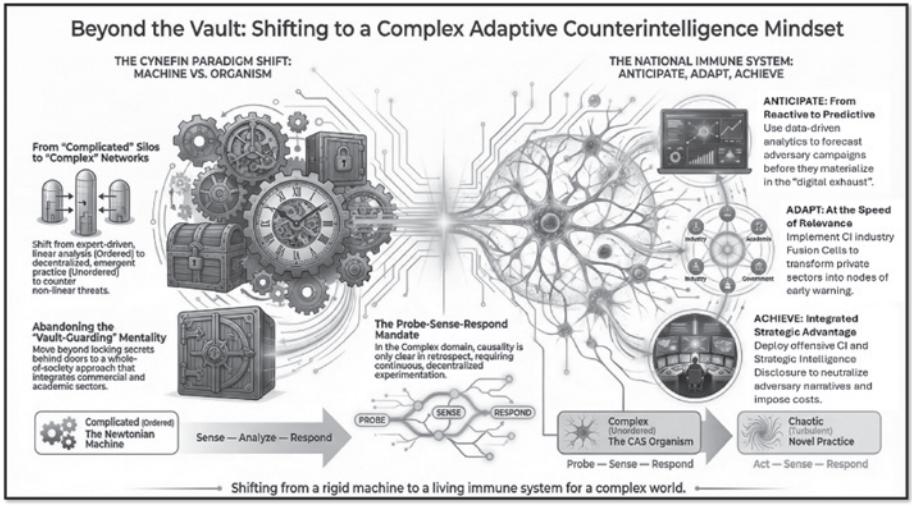


Figure 12. Beyond the Vault. Source: Michael W. Parrott, created using Gemini Notebook, February 2026

A theory of victory for CI in strategic competition requires a national immune system that senses, learns, and adapts faster than adversaries; a distributed CI architecture that integrates government, industry, academia, and SOF; a cost-imposing posture that shapes adversary behavior through SID, attribution, and techno-economic warfare; and a cultural transformation that replaces compliance-driven timidity with adaptive boldness. This requires immediate, irreversible action from the stewards of American power:

To Policy Makers in Congress: Build the legal and structural scaffolding for a national immune system. Close the systemic vulnerabilities exploited through Military-Civil Fusion by aggressively enforcing provisions such as Section 1286 of the National Defense Authorization Act (NDAA).[32] Provide the resources and legal mandates necessary to transition the U.S. from a defensive posture to an offensive, cost-imposing enterprise.

To Intelligence Community Leaders: Abandon the comfort of hierarchical control and the antiquated guardians of secrets identity. Lead the transition to a CAS by breaking down bureaucratic stovepipes and sharing threat intelligence with the private sector at the speed of relevance. Execute SID to proactively pre-bunk FIE weaponized narratives before they take root.

To SOF Professionals: As the forward sensors of the national immune system, embrace the role as global scouts. To survive in the glass house of UTS, master active signature reduction—spoofing and manipulating digital exhaust to maintain freedom of maneuver in denied areas.[33]

To Commercial and Private-Sector Executives: Recognize that the market is no longer neutral; it is the primary battlespace. Treat CI as a strategic investment essential to protecting profit margins, intangible assets, and market share. Embed CI into enterprise risk

The era of peace is an illusion. Every day, the U.S. remains organized as a Newtonian machine, its adversaries operate as adaptive organisms.

management, implement Zero-Trust architectures, and participate actively in CI-industry fusion cells.

The era of peace is an illusion. Every day, the U.S. remains organized as a Newtonian machine, its adversaries operate as adaptive organisms. They do not wait for permission. They do not file compliance reports. They probe, learn, and evolve. America will face an existential CI failure; it is inevitable. The question is whether the nation will have the institutional courage to reform before that failure arrives. A national immune system is not a theoretical ideal; it is a strategic necessity. The tools exist. The framework exists. Talent exists. What remains is a choice: adapt now, on domestic terms, or adapt later, on adversarial terms. America must change now to compete in the future.

By operationalizing the AAA framework to build a complex adaptive national immune system, the U.S. can move from absorbing foreign intelligence blows to shaping adversary decision-making at scale by detecting, identifying, exploiting, and neutralizing foreign intelligence threats, securing American prosperity and strategic dominance for the 21st century (see Fig. 13).

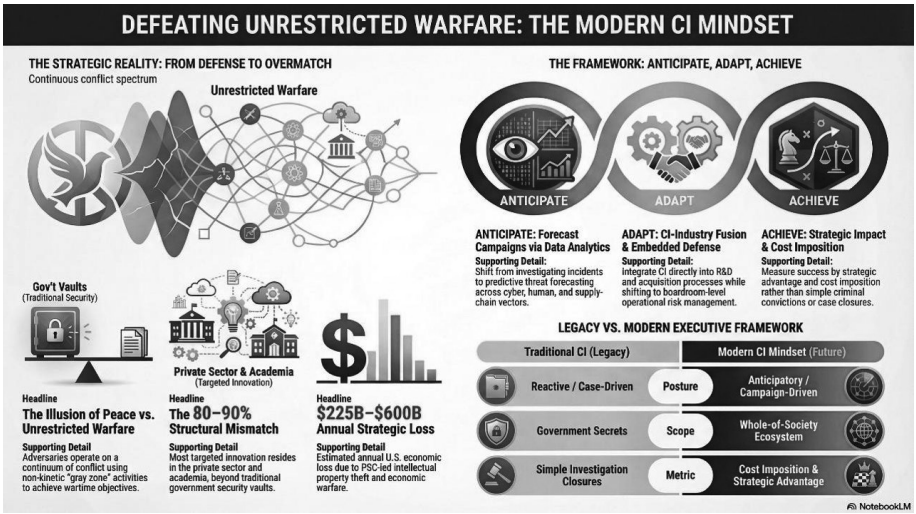


Figure 13. The Strategic Reality. Source: Michael W. Parrott, created using Gemini Notebook, January 2026

About the Author

Michael W. Parrott is a veteran U.S. Army CI technician, an academic chair at the Joint Special Operations University's Enlisted Academy, and an adjunct professor at the National Intelligence College, where he teaches graduate-level seminars on special operations, counterintelligence, insider threat, and strategic intelligence competition. He specializes in gray zone and IW, CI mindset reform, and the integration of academic rigor with operational relevance for senior government and intelligence community audiences. Mr. Parrott also volunteers as the International Association for Intelligence Education (IAFIE) Programs Director. IAFIE is a non-profit focused on advancing research, knowledge, and professional development in intelligence education to strengthen the global intelligence workforce.

Notes

1. Liang Qiao and Wang Xiangsui, *Unrestricted Warfare* (PLA Literature and Arts Publishing House, 1999), 11–12. https://www.c4i.org/unrestricted.pdf.

2. Timothy L. Thomas, "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies* 17, no. 2 (2004): 237–56, https://impiousdigest.com/wp-content/uploads/2017/08/Thomas_2004.pdf.

3. Irregular Warfare Center, *Defense Support to Strategic Competition* (Department of Defense, 2023), https://irregularwarfarecenter.org/publications/insights/reframing-the-term-irregular-warfare-in-times-of-peace-into-the-contemporary-idea-of-defense-support-to-strategic-competition/.

4. Jay Shafritz, J. Steven Ott, and Yong Suk Jang, *Classics of Organization Theory*, 6th ed. (Wadsworth, 2008), 52–96.

5. Yves Morieux and Peter Tollman, *Six Simple Rules: How to Manage Complexity Without Getting Complicated* (HBR Press, 2014), 5.

6. David J. Snowden and Mary Boone, "A Leader's Framework for Decision Making," *Harvard Business Review* (November 2007), https://strategicleadership.com.au/wp-content/uploads/2017/06/A-Leader's-Framework-for-Decision-Making-HBR-Nov-2007.pdf.

7. Serena Chan, "Complex Adaptive Systems," ESD.83 Research Seminar in Engineering Systems, Massachusetts Institute of Technology, October 31, 2001, https://web.mit.edu/esd.83/www/notebook/Complex%20Adaptive%20Systems.pdf.

8. Michael W. Parrott, "U.S. Intelligence Reform: Applying the Six Simple Rules" (master's thesis, National Defense University, 2019), 38–44.

9. Kelly Tongol, *Look or Leap? Unpacking Risk Propensity in Intelligence Professionals* (National Intelligence University, 2024), 5–11, https://www.govinfo.gov/content/pkg/GOVPUB-D5_200-PURL-gpo248066/pdf/GOVPUB-D5_200-PURL-gpo248066.pdf.

10. Parrott, "U.S. Intelligence Reform," 14–23.

11. Craig W. Gruber et al., "Ubiquitous Technical Surveillance: A Ubiquitous Intelligence Community Issue," *Fostering Innovation in the Intelligence Community*, (Springer, 2023), 1–17, https://link.springer.com/chapter/10.1007/978-3-031-29807-3_1.

12. Parrott, "U.S. Intelligence Reform," 14–23.

13. Gruber et al., "Ubiquitous Technical Surveillance: A Ubiquitous Intelligence Community Issue," 1–17.

14. Department of Justice, *Audit of the FBI's Efforts to Mitigate the Effects of Ubiquitous Technical Surveillance*, report 25-065 (June 2025), 17–18, https://oig.justice.gov/sites/default/files/reports/25-065_t.pdf.

15. Glenn Tiffert, ed., *Global Engagement: Rethinking Risk in the Research Enterprise* (Hoover Institution Press, 2020), 120–135, https://www.hoover.org/events/global-engagement-rethinking-risk-research-enterprise.

16. U.S. Congress, House, Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, *Fox in the Henhouse: The U.S. Department of Defense Research and Engineering's Failures*

to Protect Taxpayer-Funded Defense Research, 118th Cong., 2nd sess., 2024, 15, https://chinaselectcommittee.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/fox-in-the-henhouse-report-compressed_0.pdf.

17. U.S. Congress, *Fox in the Henhouse*.

18. Cask Government Services, "Cybersecurity for Universities: Balancing Innovation & Research," *Cask Government Services*, (blog, cybersecurity) March 10, 2025, https://caskgov.com/resources/cybersecurity-for-universities/.

19. Howard G. Coombs and Christopher Marsh, eds., *Operating on the Margins: SOF in the Gray Zone* (JSOU Press, 2023), 5–15, https://jsou.edu/Press/PublicationDashboard/228.

20. Max Lesser, "FDD Uncovers Likely Chinese Intelligence Operation Targeting Recently Laid-Off U.S. Government Employees," Foundation for Defense of Democracies, May 16, 2025, https://www.fdd.org/wp-content/uploads/2025/05/fdd-memo-fdd-uncovers-likely-chinese-intelligence-operation.pdf.

21. Lesser, "FDD Uncovers Likely Chinese Intelligence Operation."

22. Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 8th ed. (CQ Press, 2016).

23. Philip Zelikow et al., "9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States," official government ed. (Government Printing Office, July 22, 2004), 408, accessed on March 20, 2026.

24. Paul C. Light, *The True Size of Government* (Brookings Institution Press, 1999).

25. Shafritz, Ott, and Jang, *Classics of Organization Theory*, 52–96.

26. National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Government Printing Office, 2004), https://www.federalregister.gov/documents/2004/06/17/04-13733/public-hearing.

27. Morieux and Tollman, *Six Simple Rules*, 16–17.

28. Tiffert, ed., *Global Engagement: Rethinking Risk in the Research Enterprise*, 120–135.

29. Tiffert, *Global Engagement: Rethinking Risk in the Research Enterprise.*

30. U.S. Department of Defense, "Military-Civil Fusion Strategy Assessment," press release (Department of Defense, 2023), https://www.war.gov/News/Releases/Release/Article/3561549/dod-releases-2023-report-on-military-and-security-developments-involving-the-pe/.

31. U.S. Department of State, *Russia's Hybrid Warfare Toolkit* (U.S. State Department, 2022), https://2021-2025.state.gov/ukraine-and-russia/.

32. U.S. Department of Defense, *FY24 Section 1286 List for Public Release, Academic Research Security Program*, Basic Research Office, accessed March 26, 2026, / https://rt.cto.mil/wp-content/uploads/2025/06/FY24-Section-1286-List-for-public-release_V2.pdf.

33. Christopher Moede, "Ubiquitous Technical Surveillance and the Renewal of Irregular Warfare," *Small Wars Journal* (2024), https://smallwarsjournal.com/2026/02/13/ubiquitous-technical-surveillance/.

Bibliography

Cask Government Services. "Cybersecurity for Universities: Balancing Innovation & Research." *Cask Government Services*. Published March 10, 2025. https://caskgov.com/resources/cybersecurity-for-universities.

Center for International and Security Studies at Maryland. *The Future of Intelligence Analysis, Volume I Final Report*. University of Maryland, March 10, 2006.

Chan, Serena. "Complex Adaptive Systems." ESD.83 Research Seminar in Engineering Systems. Massachusetts Institute of Technology, October 31, 2001.

Coombs, Howard G., and Christopher Marsh, eds. *Operating on the Margins: SOF in the Gray Zone*. JSOU Press, 2023.

Cruden, Chris, and Doug Livermore. "OSS 2.0: Emphasizing the Importance of Human Intelligence in Irregular Warfare for Great Power Competition." *IW Perspectives*, January 8, 2025.

Evanina, William R. "Counterintelligence: Changing Landscape, Unprecedented Threat." *IRTPA*, 2024.

U.S. Department of Justice. *Audit of the Federal Bureau of Investigation's Efforts to Mitigate the Effects of Ubiquitous Technical Surveillance*. Report 25-065. Department of Justice, June 2025.

Gamache, Kevin R. "Protecting American Innovation: Industry, Academia, and the National Counterintelligence and Security Center." U.S. Senate Select Committee on Intelligence, September 21, 2022.

Gruber, Craig W., Benjamin Trachik, Catherine Kirby, Sara Dalpe, Lila Silverstein, Siobhan Frey, and Brendon W. Bluestein. "Ubiquitous Technical Surveillance: A Ubiquitous Intelligence Community Issue." In *Fostering Innovation in the Intelligence Community: Scientifically-Informed Solutions to Combat a Dynamic Threat Environment*, edited by Craig W. Gruber and Benjamin Trachik, 1–17. Springer, 2023.

Hannas, William C., James Mulvenon, and Anna B. Puglisi. *Chinese Industrial Espionage: Technology Acquisition and Military Modernization*. Routledge, 2013.

Hazelrig, Kirsten. *Surveillance Technologies Are Imbedded Into the Fabric of Modern Life—The Intelligence Community Must Respond*. MITRE Corporation, 2023.

Intelligence and National Security Alliance (INSA). "Insider Threats and Commercial Espionage: Economic and National Security Impacts." INSA, 2021/2025.

Irregular Warfare Center. *Defense Support to Strategic Competition.* Department of Defense, 2023.

Lesser, Max. "FDD Uncovers Likely Chinese Intelligence Operation Targeting Recently Laid-Off U.S. Government Employees." *Foundation for Defense of Democracies*, May 16, 2025.

Light, Paul C. *The True Size of Government*. Brookings Institution Press, 1999.

Lowenthal, Mark M. *Intelligence: From Secrets to Policy*. 8th ed. CQ Press, 2019.

Moede, Christopher. "Ubiquitous Technical Surveillance and the Renewal of Irregular Warfare." Small Wars Journal (2024).

Morieux, Yves, and Peter Tollman. *Six Simple Rules: How to Manage Complexity Without Getting Complicated*. HBR Press, 2014.

National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report*. Government Printing Office, 2004.

National Intelligence University. *Look or Leap? Unpacking Risk Propensity in Intelligence Professionals*. NIU Press, 2024.

Office of the Director of National Intelligence. *National Counterintelligence Strategy of the United States of America 2020-2022*. ODNI, 2020.

Office of the Director of National Intelligence. *National Counterintelligence Strategy 2024*. ODNI, August 2024.

Parrott, Michael W. "Foreign Intelligence Threats to SOF—Why Counterintelligence Integration Is Vital." *Tip of the Spear*, October 2023.

Parrott, Michael W. *U.S. Intelligence Reform: Applying the Six Simple Rules*. Master's thesis, National Defense University, 2019.

Qiao, Liang, and Wang Xiangsui. *Unrestricted Warfare*. PLA Literature and Arts Publishing House, 1999.

Robert Lansing Institute. "Russian Espionage Targeting NATO Unmanned Systems in Europe." 2025.

Shafritz, Jay, J. Steven Ott, and Yong Suk Jang. *Classics of Organization Theory*. 6th ed. Wadsworth, 2008.

Snowden, David J., and Mary Boone. "A Leader's Framework for Decision Making." *Harvard Business Review*, 2007. "The Shadow of the Future: Extending Strategic Accountability." Internal Assessment, 2025.

Tiffert, Glenn, ed. *Global Engagement: Rethinking Risk in the Research Enterprise*. Hoover Institution Press, 2020.

Thomas, Timothy L. "Russia's Reflexive Control Theory and the Military." *Journal of Slavic Military Studies* 17, no. 2, (2004): 237–56.

U.S. Congress. House. Committee on Oversight and Accountability. *CCP Political Warfare: Federal Agencies Need a Government-Wide Strategy*. 118th Cong., 2nd sess., 2024.

U.S. Congress. House. Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party. *Fox in the Henhouse: The U.S. Department of Defense Research and Engineering's Failures to Protect Taxpayer-Funded Defense Research*. 118th Cong., 2nd sess., 2024.

U.S. Department of Defense. *FY24 Section 1286 List for Public Release*. Academic Research Security Program, Basic Research Office. Accessed March 26, 2026. https://rt.cto.mil/wp-content/uploads/2025/06/FY24-Section-1286-List-for-public-release_V2.pdf.

U.S. Department of Defense. *Military-Civil Fusion Strategy Assessment*. Department of Defense, 2023.

U.S. Department of State. *Russia's Hybrid Warfare Toolkit*. Department of State, 2022.

Walton, Calder, and Greg Levesque. "An All-of-Society Approach to US Counterintelligence." *The Cipher Brief*, December 13, 2024.

Zelikow, Philip, et al. *9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*. Official government ed. Government Printing Office, July 22, 2004. Accessed March 20, 2026. https://www.federalregister.gov/documents/2004/06/17/04-13733/public-hearing.

Digital Force Protection: Lessons from China's Global Television Network Economic Messaging and Market Dynamics

By Sonny S. Patel, PhD, MPhil, MPH, and
Carol Kay Winkler, PhD, MA

Acknowledgments

The authors would like to thank Dr. Keyu Chen Glanz and Dr. Ayşe Lokmanoğlu for their valuable insights and contributions to this research. This research is supported in part by the U.S. Air Force Office of Scientific Research of the U.S. Department of War, under Grant FA9550-22-1-0331. All opinions and conclusions expressed are those of the authors.

Abstract

China Global Television Network's (CGTN) economic messaging operates at the intersection of mediated public diplomacy, financial markets, and strategic competition, which makes it a useful case for examining how open-source data-analytic tools can create or mitigate digital force protection risks for special operations forces (SOF). This study analyzes 74,926 CGTN economic-related posts on Facebook and Instagram, 2018–2023, and links them to monthly returns for the S&P 500, NASDAQ Composite, SSE Composite, and CSI 300 indices. BERTopic identifies nine salient economic themes, monthly platform-level volumes and topic frequencies are aligned with index returns, and linear regressions, vector autoregressions (VAR), and Granger causality tests assess contemporaneous and lagged relationships. Platform-level economic post volume does not Granger-cause any of the four indices, whereas several topics show significant lagged effects on especially Chinese indices, and in some cases indices Granger-cause subsequent changes in topic salience or Instagram output. These asymmetric feedback loops illustrate how state-run economic narratives and markets form a coupled system. The CGTN case demonstrates the feasibility of integrating large-scale media and financial data into a single analytic architecture. It shows that a small set of open-source narratives can function as sensitive indicators of real-world conditions. It also points to concrete ways SOF can use similar data analytics systems

to identify, measure, and mitigate open-source intelligence exposure that threatens digital force protection for personnel, daily work, and operational missions.

Introduction

States are expanding their online media systems to gain influence over foreign audiences, potentially creating new protection risks for special operations forces (SOF). Their growth produces large volumes of open-source information that adversaries can use to alter patterns of life, economic confidence levels, and reactions to governmental actors. For example, China now uses the China Global Television Network (CGTN), Xinhua, China Daily, and People's Daily to promote its official global narratives about economic development, global governance, and security issues, with expenditures reaching as high as $7–$10 billion annually.[1] CGTN functions as one such digital force multiplier, surpassing the BBC in 2016 as Facebook's most followed global news page.[2]

While research increasingly examines China's media content, media scholars bemoan the lack of focus on context and its intersection with media messaging.[3] The oversight is unfortunate, because contexts shape how messaging works. Political, economic, and technological conditions influence objectives, tools, messages, and involved audiences.[4] Context does not stand apart from discourse; it is co-produced with texts and gains meaning only in relation to other texts and situations.[5] Efforts that ignore context risk mistaken assumptions and losing contact with "discourse as it appears in the world."[6] The increased use of digital media platforms magnifies the challenge by adding contextual features, algorithms, interface design, and audience communities that condition message design and circulation patterns.[7] These contextual features also influence digital traces left behind in public-facing systems, which

Digital force protection for SOF should involve AI and machine learning to enhance situational awareness of stock market indices at home and abroad, enrich potential indicators of instability, and help understand what an adversary could extrapolate from open-source patterns.

hostile actors can aggregate and analyze to develop operational profiles and movement patterns.

The few extant context studies of China's global media campaigns explore how narratives of economic success, partnership, and solidarity function for audiences in Africa, Latin America, and Australia. Such efforts produce mixed results,[8] with local actors and U.S. media campaigns offering some competing perspectives.[9] Less examined are how foreign media efforts interact with economic factors. One study finds that shifts in CGTN's economic messaging strategies on social media correspond to changes in the yuan's value.[10] Related economic work focusing on the online publications of Russia and ISIS demonstrates links between economic narratives, currency valuations, and oil prices.[11] These studies suggest that state-run online media outlets not only seek to shape perceptions but create feedback loops that tie their messaging to observable economic indicators.

Missing from previous analysis is a focus on stock market returns of near-peer competitors. Analysts do not yet know whether economic narratives from outlets such as CGTN generally predict shifts in national indices, follow them, or move independently. They also do not understand whether aggregate or topic-specific output carry more weight. Examinations of negative country coverage outside the U.S. has depressed local stock markets, especially

where press freedom is low and macroeconomic indicators influence foreign media's descriptions of a country's economy,[12] whether immediately or after some delay.[13] Conversely, stock market returns may influence digital media output, since exchange rates and benchmark indices shape the tone of foreign news coverage about countries.[14]

Bidirectional relationships between open-source narratives and economic indicators are relevant both to investors and digital force protection, as they infer real-world conditions from public data streams. Understanding the economic context matters to SOF because economic narratives and financial conditions are key factors in shaping online and offline environments. Economic confidence affects elite bargaining power, public support for governments and external forces, and vulnerability of partner states to coercion. Thus, adversaries can utilize state-run social media platforms to frame economic developments to erode confidence in U.S. policy, legitimize alternative economic orders, and shift blame for local hardships.

Digital force protection for SOF should involve AI and machine learning to enhance situational awareness of stock market indices at home and abroad, enrich potential indicators of instability, and help understand what an adversary could extrapolate from open-source patterns. This study makes the case by analyzing the economic messaging of CGTN and U.S. and Chinese stock returns as a pilot project to show how social media content and stock market returns over time can be modeled together. The analysis employs topic modeling and vector autoregression with Granger causality tests to map how specific economic narratives and market indicators move in relation to each other. The core empirical questions concern whether platform-level economic output and topic-specific coverage preceded or followed changes in major stock indices between 2018 and 2023, and whether these relationships differ across market

contexts. The broader intent shows how similar tools could help SOF and U.S. Special Operations Command (USSOCOM) identify threats that arise from adversaries exploiting open-source, economic media data, and how such tools can be repurposed to measure and mitigate digital exposure risks for forces and missions.

Research question 1: Do changes in CGTN's economic posting volume on Facebook and Instagram influence stock returns in major U.S. and Chinese markets, and do these stock returns, in turn, influence changes in CGTN's platform-level economic output?

Research question 2: Do changes in the frequency of prominent economic topics in social media posts by CGTN influence stock returns, and do these returns influence subsequent changes in topic frequency?

Research question 3: Does the strength, direction, and timing of these platform- and topic-level relationships differ between U.S. and Chinese stock markets?

The Importance of Media Reporting and Stock Markets

Research on media and stock markets generally examines corporate-level effects. Traditional media studies of corporate impacts reach mixed conclusions. Some find that news coverage influences the stock valuations of specific firms.[15] Studies stress the key role of reporting tone,[16] organizational crisis resilience,[17] and attention to risk premiums, term premiums, or industrial growth rates for shaping U.S. stock returns.[18] Other work, however, argues that media coverage has little direct effect.[19] Nonetheless, longitudinal analyses show that bad news volume impacts market downturns.[20]

Similarly, online media research points to links between content strategies and stock market performance. Inside China,

media coverage appears to affect stock valuations of listed firms.[21] Audience behaviors such as search engine activity,[22] negative word of mouth about brands,[23] and financial blogging[24] correlate with corporate outcomes. Messaging characteristics such as tweet valence[25] and multimodal presentation[26] also matter in online media efforts. Finally, news tone, salience, and timing can affect firm-level valuations and trading behavior, although results are not always consistent.[27]

Materials and Methods

Data Collection and Sample

On January 31 and August 31 of 2023, Facebook and Instagram posts were collected from 14 CGTN accounts using CrowdTangle, Meta's public research platform. Duplicate posts were removed, and the study was restricted to the timespan of 9/1/2018 through 8/31/2023. The beginning date corresponds to when China consolidated its major state-run broadcasters under direct party-state control,[28] and the ending date precedes Meta's suspension of general CrowdTangle access. As a result, 490,090 posts were found. Of these, posts were filtered further using a validated multilingual economic dictionary containing 266 terms,[29] yielding an economic sub-corpus of 74,926 posts, 15.3 percent of all CGTN posts during the study's timeframe.

Economic Topic Modeling

To identify recurring economic strategies, BERTopic,[30] an unsupervised topic model with transformer-based embeddings and class-based term frequency-inverse document frequency (TF-IDF), was applied. Prior evaluations document BERTopic's ability to generate coherent, multilingual topics for social-media corpora.[31] All the economic-related posts were aggregated across

languages, document embeddings were computed, and the posts were clustered into topics. Native speakers reviewed and refined the validity of topic labels. A minimum cluster size was set to at least 5 percent of the economic sub-corpus, omitting posts assigned to smaller clusters or labeled as noise by the algorithm.

The final model grouped 67,951 posts (90.7 percent of the economic sub-corpus) into nine topics: Africa in Turmoil, China–Global South Cooperation, China–Latin America Relations, China Success Model, U.S. Economic Concerns, China–U.S. Trade Relations, Covid-19 Impact, Russia–Ukraine Conflict, and China–Arab Cooperation.

Stock Market Data

The connections between media and stock market returns must be examined in light of contextual complexity. Stock markets differ in their sectoral composition, weighting schemes, and institutional features. Cultural norms shape investor behavior.[32] Accounting practices vary by country,[33] and exchanges differ in how efficiently they record and disseminate trade information.[34] Social media messaging campaigns are also not uniform. State-run outlets employ different strategies across platforms and issue areas to target distinct audiences.[35]

Accordingly, stock index returns were measured using four benchmarks. U.S. markets were measured using the S&P 500 to capture broad market performance and the NASDAQ Composite to include technology-heavy growth stocks.[36] For China, the Shanghai Stock Exchange (SSE) Composite was used to capture state-linked enterprise performance, and the CSI 300 was used to capture large, liquid firms in Shanghai and Shenzhen.[37]

For each index, the cost value was calculated as the difference between the closing value on the first trading day and the closing

value on the last trading day of each month. Monthly aggregation was chosen to smooth short-term noise and align with the volume of CGTN postings, which varies meaningfully on a monthly scale.

Platform Weighting and Alignment

The economic output of CGTN was heavily skewed toward Facebook, with 63,172 economic posts on Facebook and 4,779 on Instagram. To prevent this imbalance from overwhelming the analyses, an inverse-weighting scheme was applied, assigning weights proportional to the inverse of each platform's share of total posts.[38] Facebook's normalized weight was 0.072, and Instagram was 0.928. The monthly platform totals were multiplied by these weights before aggregation. All media and stock variables were aligned at the monthly level over the study's time span, yielding 60 months of data per series.

Statistical Analysis

A two-stage analytic strategy was used. Initially, linear regressions were run to assess contemporaneous associations between monthly stock returns and, in separate models, platform-level economic post volumes and topic frequencies. These models provided effect estimates but did not address temporal ordering. Then, vector autoregression (VAR) models were estimated, with Granger causality tests used to examine lagged, potentially bidirectional relationships between media and markets.

For each index, one VAR system was estimated that included the index's monthly returns and the weighted Facebook and Instagram economic post totals, and a second VAR system that included returns and the nine-topic series. Augmented Dickey–Fuller tests guided transformations, and stock returns were stationary. All VAR models included one to three monthly lags.

Within each VAR, Wald χ^2 tests were used to assess Granger causality (i.e., whether lagged values of one series jointly improved prediction of another series beyond that series' own lagged values). A conservative rule for interpretation was adopted: only relationships where the Granger test was significant at $p < .05$ and at least one individual lag coefficient in the relevant equation was significant at $p < .05$ were retained. All tests were two-tailed.

Results

Platform-Level Associations

Regression models suggested only modest contemporaneous associations between media strategies and stock market returns. Facebook economic post volume tended to move in the same direction as S&P 500 and NASDAQ returns; Instagram volume tended to move in the opposite direction of NASDAQ returns, but model R^2 values never exceeded .12 and several models were non-significant (all $p > .05$). These patterns hinted at possible relationships but did not provide clear evidence that the overall economic output shared by CGTN on a platform directly moved any of the four indices.

VAR models clarified the effects' timing and direction. Table 1 summarizes whether Facebook or Instagram activity significantly preceded changes in returns (Media ➔ Markets) and whether returns significantly preceded changes in subsequent Facebook or Instagram activity (Markets ➔ Media) for each index, along with the significance of relevant one-month (L1), two-month (L2), or three-month (L3) lags. Table 2 reports the Wald χ^2 statistics and p-values for these Granger causality tests.

Across all four indices, neither Facebook nor Instagram economic output significantly predicted later stock returns (all $p > .05$; Table 2, Panel A). No evidence existed that more CGTN economic posts

by platform led to higher or lower returns on the four stock indices during the following three months (Table 1, Media ➔ Markets panel).

Table 1. Monthly Relationships between Stock Market Returns and CGTN Economic Post Content (2018-09-01 and 2023-08-31)

Media ➔ Markets (platform totals predicting returns)				
Media series	**S&P 500**	**NASDAQ**	**SSE**	**CSI 300**
Facebook totals				
Instagram totals (Δ)				
Markets ➔ Media (returns predicting platform totals)				
Media series	**S&P 500**	**NASDAQ**	**SSE**	**CSI 300**
Facebook totals				
Instagram totals (Δ)	L1, L3 (+)	L1, L3 (+)	L3 (+)	

Note: CGTN = China Global Television Network; S&P 500 = Standard and Poor's 500; NASDAQ = National Association of Security Dealers Automated Quotations; SSE = Shanghai Stock Exchange; L1, L2, L3 = lags; positive/negative = effect directions; Δ = indicates Instagram series was differenced before inclusion; blank cell indicates no significant lag result found. All totals were weighted. Source: Author

In contrast, three of the four indices significantly predicted later changes in CGTN Instagram activity (Table 1, Markets ➔ Media panel; Table 3, Panel B). For the SSE Composite, months with higher returns preceded increased CGTN economic postings on Instagram three months later ($p < .05$), whereas Facebook output did not yield significant results. For the S&P 500, months with higher returns preceded more Instagram economic posts one and three months later ($p < .05$), again with no corresponding effect on Facebook. For the NASDAQ Composite, higher returns were preceded by increased Instagram economic posting after one and three months ($p < .05$), with no significant effect on Facebook. CSI 300 returns did not show statistically significant relationships with Facebook or Instagram output under our criterion ($p > .05$).

Table 2. Wald χ^2 Granger Causality Tests for PlatformLevel Relationships between CGTN Economic Output and Stock Index Returns (2018–2023)

Panel A. Media → Markets (Do platform totals Granger cause later returns?)				
Media series	**S&P 500**	**NASDAQ**	**SSE**	**CSI 300**
S&P 500	Facebook + Instagram totals (joint)	6	11.78	0.067
S&P 500	Facebook totals only	3	2.02	0.569
S&P 500	Instagram totals only	3	7.35	0.062
NASDAQ Composite	Facebook + Instagram totals (joint)	6	10.22	0.116
NASDAQ Composite	Facebook totals only	3	2.9	0.408
NASDAQ Composite	Instagram totals only	3	5.38	0.146
SSE Composite	Facebook + Instagram totals (joint)	6	7.02	0.319
SSE Composite	Facebook totals only	3	5.45	0.142
SSE Composite	Instagram totals only	3	1.61	0.658
CSI 300	Facebook + Instagram totals (joint)	6	9.04	0.171
CSI 300	Facebook totals only	3	7.51	0.057
CSI 300	Instagram totals only	3	1.4	0.706
Panel B. Markets → Media (Do returns Granger cause later platform totals?)				
Outcome (media)	**Predictor (returns)**	**df**	**Wald χ^2**	**p value**
Facebook totals	S&P 500	3	6.25	0.1
Instagram totals (Δ)	S&P 500	3	14.16	0.003
Facebook totals	NASDAQ Composite	3	4.07	0.254
Instagram totals (Δ)	NASDAQ Composite	3	16.34	0.001
Facebook totals	SSE Composite	3	0.56	0.905
Instagram totals (Δ)	SSE Composite	3	7.99	0.046
Facebook totals	CSI 300	3	1.66	0.645
Instagram totals (Δ)	CSI 300	3	6.81	0.078

Notes: Δ indicates that the Instagram series was differenced before inclusion in the VAR models.

Note: S&P 500 = Standard and Poor's 500; NASDAQ = National Association of Security Dealers Automated Quotations; SSE = Shanghai Stock Exchange.
Source: Author

The platform-level results indicate that the economic posting volume of CGTN on Facebook and Instagram did not drive stock market movements in the four indices. However, U.S. and Chinese market performance, especially for the S&P 500, NASDAQ, and SSE, did precede changes in its economic presence on Instagram. Markets acted as signals for CGTN to adjust its Instagram economic output after delays of roughly one to three months. No evidence supported the reverse direction. From a digital force protection perspective, these platform-level findings demonstrate how access to open financial data and social-media archives can detect and model systematic, time-lagged adjustments in state-run messaging in response to market conditions.

Topic-Level Associations

Regression models on the nine economic topics as contemporaneous predictors of monthly returns did not reach significance for any stock market index ($p>0.05$ and adjusted R^2 values were near zero or negative). Static, one-shot models therefore understated the relationships between topic salience and returns.

Topic-based VAR models told a different story. When the researchers accounted for lags and bidirectional effects, the nine topics jointly explained about 59 percent of the variance in S&P 500 returns, 52 percent in NASDAQ returns, 66 percent in SSE Composite returns, and 60 percent in CSI 300 returns. Table 3 indicates whether the topic significantly predicted later returns, including lags (L1–L3) and effect directions (positive or negative) for each topic and model (Media ➔ Markets panel). It also shows where stock returns significantly predicted later changes in topic salience (Markets ➔ Media panel). Table 4 presents the corresponding Wald χ^2 statistics and the Granger tests' p-values.

Table 3. Relationships between Monthly Stock Market Returns and CGTN Topics on Facebook and Instagram (2018-09-01 and 2023-08-31)

Media → Markets (topics predicting returns)				
CGTN Economic Topic	**S&P 500**	**NASDAQ**	**SSE**	**CSI 300**
Africa in Turmoil Δ				
China Global South Cooperation			L1 (–)	
China Success Model			L1 (–)	L1 (–)
China US Trade Relations			L1, L2 (–)	L2 (–)
Russia Ukraine Δ			L1 (–)	L1 (–)
COVID 19 Impact Δ	L1 (–), L2, L3 (+)	L2, L3 (+)		
China Arab Cooperation	L1 (+)		L1(+),L2 (–)	L1 (+)
China Latin America Relations Δ				
US Economic Concerns Δ			L1 (–)	
Markets → Media (returns predicting topics)				
CGTN Economic Topic	**S&P 500**	**NASDAQ**	**SSE**	**CSI 300**
Africa in Turmoil Δ				
China Global South Cooperation				
China Success Model	L3 (+)	L3 (+)		
China US Trade Relations				
Russia Ukraine Δ			L3 (+)	
COVID 19 Impact Δ			L2 (+), L3 (–)	L3 (+)
China Arab Cooperation				
China Latin America Relations Δ				
US Economic Concerns Δ			L2 (+)	L2 (+)

Note: L1, L2, L3 = lags; positive/negative = effect directions; Δ = denotes differenced topic series used in the VAR models; blank cell indicates no significant lag result found. Source: Author

For the SSE Composite, five topics significantly predicted later returns ($p < .05$; Table 4, Panel A). Greater coverage of China–Global South Cooperation, China–U.S. Trade Relations, Russia–Ukraine

Conflict, and U.S. Economic Concerns preceded lower SSE returns, generally at one-month lags and, for China–U.S. Trade Relations also at two months (Table 3, Media ➔ Markets). In contrast, China–Arab Cooperation coverage showed a mixed pattern, with higher SSE returns one month after an increase in this topic but lower returns two months later. SSE returns also significantly preceded changes in several topics (Table 3, Markets ➔ Media; Table 4, Panel B): higher SSE returns were followed by increased coverage of Russia–Ukraine Conflict, COVID-19 Impact, and U.S. Economic Concerns after delays of two to three months.

For the S&P 500, two topics significantly predicted returns (Table 4, Panel A). Increases in COVID-19 Impact coverage preceded lower S&P 500 returns one month later but higher returns two and three months later ($p < .05$), consistent with an initial shock followed by partial recovery (Table 3). Greater emphasis on China–Arab Cooperation predicted higher S&P 500 returns at a one-month lag ($p < .01$). S&P 500 returns, however, did not significantly predict later changes in any of the topic series (all $p > .05$; Table 3, Markets ➔ Media).

For the NASDAQ Composite, COVID-19 Impact was again the only topic that significantly predicted later returns ($p = .001$; Table 4). Higher COVID-19 coverage preceded higher NASDAQ returns two months later, with a smaller, marginally positive association at three months (Table 3). NASDAQ returns did not significantly precede changes in any of the topic series ($p > .05$).

For the CSI 300, three topics significantly predicted returns (Table 4, Panel A). Increased attention to China Success Model and China–U.S. Trade Relations preceded lower CSI 300 returns, at one- and two-month lags respectively ($p < .05$), while greater coverage of China–Arab Cooperation predicted higher CSI 300 returns one month later ($p < .01$; Table 3). CSI 300 returns did not

Table 4. Wald χ^2 Granger Causality Tests for TopicLevel Relationships between CGTN Economic Narratives and Stock Index Returns (2018–2023)

Panel A. Media → Markets (Do topics Granger-cause later returns?)				
Outcome (returns)	**Topic (predictor)**	**df**	**Wald χ^2**	**p value**
SSE Composite	China–Global South Cooperation	3	11.56	0.009
SSE Composite	China–U.S. Trade Relations	3	12.72	0.005
SSE Composite	Russia–Ukraine Conflict (Δ)	3	18.93	<.001
SSE Composite	China–Arab Cooperation	3	18.58	<.001
SSE Composite	U.S. Economic Concerns (Δ)	3	8.59	0.035
S&P 500	Covid 19 Impact (Δ)	3	23.33	<.001
S&P 500	China–Arab Cooperation	3	10.74	0.013
NASDAQ Composite	Covid 19 Impact (Δ)	3	16.05	0.001
CSI 300	China Success Model	3	8.21	0.042
CSI 300	China–U.S. Trade Relations	3	9.87	0.02
CSI 300	China–Arab Cooperation	3	16.94	0.001
Panel B. Markets → Media (Do returns Granger cause later topic salience?)				
Outcome (topic)	**Predictor (returns)**	**df**	**Wald χ^2**	**p value**
Russia–Ukraine Conflict (Δ)	SSE Composite	3	8.55	0.036
Covid 19 Impact (Δ)	SSE Composite	3	17.93	<.001
U.S. Economic Concerns (Δ)	SSE Composite	3	19.67	<.001
Instagram totals (Δ)	CSI 300	3	6.81	0.078

Note: Δ denotes differenced topic series used in the vector autoregressions models. Only topic–index combinations with significant Granger tests at $p < .05$ are listed; nonsignificant χ^2 tests for other topics and indices are omitted for brevity.

For SOF digital force protection, the key insight is that economic topics and market indicators should be treated as jointly evolving variables in a data-analytic system.

significantly predict later shifts in any of the topics under the joint criterion ($p > .05$).

Two topics, Africa in Turmoil and China–Latin America Relations, did not show significant relationships with any of the indices, and most related individual coefficients were small and non-significant ($p > .05$). Thus, for the indices in the period studied, media–market linkages were concentrated in topics related to China's economic model, China–U.S. trade and economic concerns, Covid-19, the Russia–Ukraine conflict, and China–Arab cooperation. For SOF, the topic-level patterns illustrate how specific themes in open-source content can function as sensitive indicators of broader economic conditions and responses.

Discussion

This analysis of CGTN economic messaging and stock market dynamics reveals an asymmetric, topic-specific feedback system rather than a uniform media effect. Aggregate economic post volume on Facebook and Instagram did not predict stock index returns, while returns in the S&P 500, NASDAQ, and SSE composites predicted lagged increases in economic content by CGTN on Instagram. In contrast, topic-level analyses uncovered robust lagged relationships between specific economic narratives and returns, particularly for Chinese indices, and in some cases, returns fed back into shifts in topic frequency. The contrast between weak platform-level effects and strong topic-level effects demonstrates

the lack of need to monitor an entire media corpus to detect meaningful linkages. A small set of topic-specific series is more revealing about how messaging and real-world indicators move together over time.

These findings show that China's economic messaging both adapts to and, at times, anticipates market conditions. CGTN increased Instagram economic output after favorable market movements but also intensified coverage of themes such as trade tensions, COVID-19, and U.S. economic problems in ways that preceded declines in Chinese indices. Topics about China–Arab cooperation tended to precede modest gains across all four indices, which suggests that investors interpreted messaging about diversified partnerships and energy cooperation as a positive signal. These patterns imply that state-run outlets can tie narrative themes to economic responses and operate within feedback loops. These loops can be mapped using off-the-shelf, open-source analytical tools by friendly or hostile actors for other domains.

For SOF digital force protection, the key insight is that economic topics and market indicators should be treated as jointly evolving variables in a data-analytic system. Topic-level results indicate:

- Economic topic content and timing matter more than overall volume. Specific topics such as China–U.S. trade tensions or U.S. economic concerns reliably preceded negative movements in SSE and CSI 300 returns, whereas aggregated economic output did not.
- Markets embedded in more centralized political economies like China's appear more sensitive to state-run economic topics than U.S. markets, which rely on a more diversified information environment. This finding has implications for how adversary messaging may impact partner or competitor economies with similar structures.[39]

- Feedback loops between markets and topics can serve as both indicators and levers. Increases in external-blame topics following SSE gains suggest attempts to contextualize volatility, and positive cooperation topics that precede rebounds suggest opportunities for stabilizing messaging.

From a digital force protection perspective, these same system features also define a class of risk. An adversary analyst who can identify a handful of topics that reliably move with key indicators does not need comprehensive access to learn something useful about conditions in a theater. Even partial and noisy open-source traces can suffice to reconstruct how populations, elites, or markets are reacting to events that may include SOF presence or operations.

SOF and USSOCOM can adapt the analytic architecture used here to support economic information operations in several ways. Analysts can build pipelines that ingest open-source content from adversary and partner state-run media outlets, filter for economic and security-relevant terms, and apply transformer-based topic models to identify recurring narratives.[40] By aligning monthly or weekly topic frequencies with local stock indices, currency values, or commodity prices, and estimating VAR models with Granger tests, analysts can identify which media strategies reliably precede economic stress or recovery.[41] Presenting these findings in concise dashboards that highlight a small set of high-leverage topics with realistic lag structures would allow integration into situational awareness, early-warning frameworks, and assessment processes. These same dashboards can also serve as red-team tools for digital force protection. They can reveal what an adversary might infer about the impact of operations or the vulnerability of partner economies based purely on open-source trajectories.

Early-warning applications include monitoring surges in economic grievance or external-blame narratives that historically precede protests, capital flight, or elite fragmentation in partner states. Media assessment applications include tracking whether U.S. and partner narratives about reform, anti-corruption, or alternative economic partnerships gain salience in state and social media and whether their timing aligns with improvements in key economic indicators. Counter-propaganda applications include prioritizing responses to adversary economic narratives that show strong links to market destabilization, and deprioritizing narratives with little measurable effect. These applications highlight a two-sided risk for SOF. Adversaries can push economic narratives to shift perceptions of partnered missions, and they can also watch economic and messaging data to infer when and where those missions are affecting the environment, even when operators themselves remain silent online.

Capacity building with partner institutions offers another avenue. SOF, working with interagency partners, can help train select partner analysts to apply simplified versions of these tools to their own media and market data, which improves local resilience against economic disinformation and aligns with irregular warfare's emphasis on working by, with, and through indigenous structures.[42] Digital force protection should be part of that training. Partners need to understand not only how to craft narratives but also how hostile actors could utilize publicly released economic data, policy

Early-warning applications include monitoring surges in economic grievance or external-blame narratives that historically precede protests, capital flight, or elite fragmentation in partner states.

SOF information focused only on counts of adversary posts or on generic sentiment scores risks overlooking which specific themes carry economic weight.

announcements, or social-media activity to monitor joint activities or target sensitive individuals and units.

Implications for Digital Force Protection of SOF

The CGTN case illuminates how adversary economic narratives and financial indicators function as a jointly evolving system with direct implications for situational awareness of SOF. It shows how machine learning and time-series methods applied to open-source data can extract sensitive patterns about how populations and markets respond to events and messaging without any need to compromise personal devices or closed networks.

The findings suggest that economic topic content and timing matter more than raw output volume of economic posts. SOF information focused only on counts of adversary posts or on generic sentiment scores risks overlooking which specific themes carry economic weight. Topic-level modeling that identifies themes such as trade disputes, sanctions, infrastructure deals, external blame, or alliances can reveal narratives tightly coupled to economic confidence or market stresses. As such, an adversary does not need comprehensive surveillance of every message. It needs only to track and model a limited set of narratives that function as proxies for the effects of sanctions, deployments, or partnered operations, which in turn map or anticipate consequences associated with SOF activities.

Denser, more negative topic-based relationships observed for Chinese indices illustrate how markets embedded in centralized

political economies may be especially sensitive to state-run narratives about risk and opportunity. Partner or adversary economies resemble this pattern, with their heavy state ownership, constrained press, and close party-state ties, SOF should expect that shifts in official economic messaging can signal or reinforce movements in markets that matter for regime stability, elite cohesion, and public tolerance of hardship. These sensitivities also give adversaries indirect visibility into how pressure levers work. They can watch for economic or narrative shifts that follow specific covert or partnered actions, then update their understanding of SOF tactics, and leverage points without ever observing the units or individuals directly.

The existence of bidirectional feedback loops between topics and stock indices suggests that economic narratives can serve as indicators and levers. Rapid increases in themes that externalize domestic downturns may flag attempts to manage domestic discontent. Conversely, periods when cooperative narratives reliably precede market rebounds, as with China–Arab cooperation in this case, may indicate when positive economic messaging is most effective in stabilizing or redirecting expectations. For digital force protection, these loops illustrate the potential for adversaries to fine-tune economic disinformation or pressure campaigns by reading public financial responses. All the while, adversaries can simultaneously exploit the same data to infer when partner societies are receptive to SOF presence or cooperation.

SOF and USSOCOM can translate these insights into a practical analytics framework. A machine-learning pipeline modeled on this study's methods would:

1) Systematically collect open-source media from state-run and proxy outlets in priority theaters alongside relevant financial

indicators such as local stock indices, currency values, and commodity prices.

2) Apply multilingual topic modeling to cluster content into interpretable themes relatable to situational awareness (e.g., sanctions, corruption, protests, security cooperation, or abandonment narratives).

3) Use VAR and Granger causality tests to identify which topics tend to precede economic stress or recovery, and which appear mainly reactive over time.

4) Present the resulting patterns in accessible forms for planners and operators, emphasizing a small set of high-leverage themes and realistic lag structures.

Once such a pipeline exists, it can also serve as a standing digital force-protection tool, as adversaries can run the same models on the same open-source data.

Such a system would support several situational awareness functions. In early warning, analysts could flag surges in topics that historically precede economic crises or protests in partner states, giving SOF and interagency partners time to adjust posture, messaging, or assistance. In campaign assessment, teams could track whether U.S. and partner narratives about economic reform, anti-corruption, or alternative trade relationships show up in topic models and whether their frequency predicts market or behavior changes. In countering adversary economic information operations, specialists should prioritize hostile narratives that warrant rapid response.

Capacity building with partner forces also stands to benefit. Training selected partner analysts or ministries in basic topic analysis and time-series thinking, tailored to their local platforms and data constraints, can strengthen their ability to counter economic

narratives that erode resilience or invite coercion. Digital force protection training should encourage partners to view their own open-source economic and media outputs as potential sensors and potential vulnerabilities.

These applications require careful attention to classification, access, and resourcing, but they do not demand high-end technology. This CGTN analysis relied on publicly available data, standard topic modeling tools, and widely used statistical packages. The main challenges lie in curating appropriate corpora, validating topics with regional expertise, and integrating outputs into SOF decision cycles. Because the tools and data are widely available, the barrier to entry is low for both adversaries and for SOF, which strengthens the case for making analytic red-teaming of open-source economic and narrative data a routine part of digital force protection.

Future Directions

Future work should incorporate additional economic context variables as potential influences on state-run media content. Multivariate analyses that include trade balances, major economic summits, gross domestic product growth, inflation, and interest rates could clarify how macroeconomic events shape both messaging strategies and market responses over time.

A second avenue concerns alignments between economic conditions and non-economic messaging. State-run outlets may

Digital force protection training should encourage partners to view their own open-source economic and media outputs as potential sensors and potential vulnerabilities.

shift coverage of territorial disputes, demographic policies, or alliance structures when economic indicators deteriorate or improve. Time-series designs could test whether changes in these security-focused narratives precede or follow market movements in ways that bear on irregular warfare.

A third priority involves visual content. Platforms such as Instagram rely heavily on images and short videos. Multimodal analyses that combine text-based topic models with computer vision or human coding of visual frames would provide a fuller account of how state-run media package economic messages for different audiences.

Future research should also widen the platform scope. While Facebook and Instagram reach global audiences, platforms such as YouTube and TikTok carry significant state-linked content. Domestically focused platforms like Weibo, WeChat, and Douyin serve users primarily inside China and may show different relationships between economic narratives and local market indicators. Comparative platform studies could identify how audience segmentation, technical affordances, and regulatory environments mediate media–market linkages that matter.

An additional line of work should focus on economic disinformation as a specific digital force protection problem. Adversaries can deploy false or distorted economic narratives about inflation, shortages, sanctions, or investment flight to undermine support for partner governments or the presence of U.S. and allied forces. They can attempt to poison the data streams that analytic systems rely on by introducing synthetic accounts, coordinated inauthentic behavior, or manipulated statistics. Future studies should examine how disinformation campaigns interact with genuine economic indicators over time and identify which fabricated or exaggerated themes most effectively move markets or public

sentiment and behavior. A robust topic-and-time-series pipeline can further reveal impactful data manipulation. Because economic disinformation can spread through the same personal devices and social networks that SOF personnel and local partners use in daily life, understanding these dynamics will strengthen the digital force protection strategy.

Conclusion

The global economic media strategies used by CGTN on Facebook and Instagram did not move major stock indices through sheer volume, but specific economic narratives showed systematic, lagged relationships with U.S. and especially Chinese stock returns. Markets in turn shaped some aspects of the CGTN Instagram output. These patterns illustrate a situational awareness feedback system in which state-run narratives both respond to and help shape economic expectations.

For SOF, this case demonstrates that integrating large-scale media content and financial indicators in a single analytic architecture can track how economic narratives and market conditions interact over time. The same architecture highlights what a capable adversary can do with open-source data: identify a small

Adapting this architecture to adversary and partner outlets would allow SOF and U.S. Special Operations Command to harness data-analytic systems for situational awareness, providing early warning of economic information operations, supporting campaign assessment, and informing targeted responses that engage economic narratives where they matter most.

set of public narratives and indicators that reveal far more about real-world conditions than they were intended to disclose. Adapting this architecture to adversary and partner outlets would allow SOF and USSOCOM to harness data-analytic systems for situational awareness, providing early warning of economic information operations, supporting campaign assessment, and informing targeted responses that engage economic narratives where they matter most. These results show how analytic pipelines can either threaten or protect SOF depending on who runs them and how their outputs are used, and they argue for treating such methods as a standing component of efforts to identify, measure, and mitigate risks to improve digital force protection.

About the Authors

Sonny S. Patel has a PhD from Georgia State University and is a presidential fellow in the Transcultural Conflict and Violence Initiative at GSU. He is a former non-resident fellow at the Joint Special Operations University, a former Fogarty Global Health Scholar at the National Institutes of Health, and a former visiting scientist at the Harvard T.H. Chan School of Public Health. Patel's research interests span information warfare, public health challenges, and disaster resilience amid geopolitical tensions. Patel's first book on community resilience is featured in Springer Nature's Advanced Science and Technologies for Security Applications book series and is part of the JSOU library collection. His research has garnered accolades and recognition, including the 2021 Emerald Publishing Literati Award for Outstanding Research Paper and Wiley's Top Cited Article for 2022-2023. Patel has developed and implemented protocols, programs, and training workshops worldwide, focusing on strategic communication, resiliency, and emerging technologies for social good.

Carol K. Winkler has a PhD from the University of Maryland in College Park and is a distinguished professor of communication studies at Georgia State University. Her research interests focus on multimodal communication and conflict, focusing on terrorism and near-peer states' media campaigns. Having received funding from the Department of Defense, the Air Force Office of Scientific Research (AFOSR), the Army War College's Strategic Studies Institute, the Department of Justice, Global Network of Terrorism Researchers, and Global Internet Forum to Counter Terrorism, she analyzes global communication strategies of U.S. adversaries and responses to them. Author of six books, five edited volumes, and more than 70 journal articles and book chapters, her research team won the 2022 Directors Award for AFSOR's Trust and Influence Division and the National Conference on Argumentation's

lifetime achievement award. From the National Communication Association (NCA), she has won the most outstanding article award on visual communication, the outstanding book award in political communication, and NCA's Robert Kibler Memorial Award for overall excellence.

Notes

1. Anne-Marie Brady, *Marketing Dictatorship: Propaganda and Thought Work in Contemporary China* (Rowman & Littlefield, 2009); Keyu Alexander Chen et al., "Montevideo Convention and CGTN: Defining Statehood for Global Outreach," *International Journal of Communication* 17 (2023): 6833–6856; Yu Zhang and David O. Ong'ong'a, "Unveiling China's Digital Diplomacy: A Comparative Analysis of CGTN Africa and BBC News Africa on Facebook," *Asian Journal of Comparative Politics* 7, no. 3 (2022): 661–683, https://doi.org/10.1177/20578911211068217; Ben Dubow, "The Rise of China's International Propaganda Empire," Center for European Policy Analysis, March 15, 2021, https://cepa.org/article/the-rise-of-chinas-international-propaganda-empire/.

2. Dubow, "Rise of China's International Propaganda Empire."

3. Craig Hayden, "Logics of Narrative and Networks in US Public Diplomacy: Communication Power and US Strategic Engagement," *Journal of International Communication* 19, no. 2 (2018): 196–218, https://doi.org/10.1080/13216597.2013.775070; Andrea Pavón-Guinea, "It's the Context, Stupid: The European Union's Public Diplomacy in Times of Ontological Insecurity," *Communication & Society* 36, no. 2 (2023): 291–309, https://doi.org/10.15581/003.36.2.291-309.

4. Pavón-Guinea, "It's the Context, Stupid: The European Union's Public Diplomacy in Times of Ontological Insecurity."

5. Jennifer Andrus, "Beyond Texts in Context: Recontextualization and the Co-Production of Texts and Contexts in the Legal Discourse, Excited Utterance Exception to Hearsay," *Discourse & Society* 22, no. 2 (2011): 115–136, https://doi.org/10.1177/0957926510392119.

6. Michael C. McGee, "Text, Context, and the Fragmentation of Contemporary Culture," *Western Journal of Communication* 54, no. 3 (1990): 274–289.

7. Natalia Levina and Manuel Arriaga, "Distinction and Status Production on User-Generated Content Platforms: Using Bourdieu's Theory of Cultural Production to Understand Social Dynamics in Online Fields," *Information Systems Research* 25, no. 3 (2014): 468–488, https://doi.org/10.1287/isre.2014.0535.

8. Brady, *Marketing Dictatorship: Propaganda and Thought Work in Contemporary China*; Hasan Saliu, "Narratives of Public Diplomacy in the Post-Truth Era: The Decline of Soft Power," *Communication & Society* 36, no. 2 (2023): 209–224, https://doi.org/10.15581/003.36.2.209-224; Amelia Arsenault, "Public Diplomacy 2.0," in *Toward a New Public Diplomacy: Redirecting US Foreign Policy*, ed. P. Seib (Palgrave Macmillan, 2009), 135–153, https://doi.org/10.1057/9780230100855_7; Soheil Kafiliveyjuyeh and Lance Porter, "Diplomatic Webs: The Influential Figures Shaping U.S. Policy in Israel, Qatar, and Iraq," Online Media & Global Communication 3, no. 3 (2024): 333–369, https://doi.org/10.1515/omgc-2024-0028; Lassi Rikkonen, Pekka Isotalus, and Hiski Haukkala, "Listening in a Masspersonal Context: Examining Professional Diplomats' Interaction Involvement on Twitter," International Journal of Listening 37, no. 3 (2023): 185–198, https://doi.org/10.1080/10904018.2022.2065276.

9. Keyu Alexander Chen, "Digital Nationalism: How Do the Chinese Diplomats and Digital Public View 'Wolf Warrior' Diplomacy?" *Global Media and China* 8, no. 2 (2023): 138–154, https://doi.org/10.1177/20594364231171785; Natalia Grincheva and Jiayi Lu, "BRICS Summit Diplomacy: Constructing National Identities through Russian and Chinese Media Coverage of the Fifth BRICS Summit in Durban, South Africa," *Global Media & Communication* 12, no. 1 (2016): 25–47, https://doi.org/10.1177/1742766515626827; Aimei Yang, Anna Klyueva, and Maureen Taylor, "Beyond a Dyadic Approach to Public Diplomacy: Understanding Relationships in a Multipolar World," *Public Relations Review* 38, no. 5 (2012): 652–664, https://doi.org/10.1016/j.pubrev.2012.07.005.

10. Mitchell John Hobbs, Jolynna Sinanan, and Mei Li, "Grand Strategy and Public Diplomacy: A Case Study on China's Belt and Road Initiative and Its Reception in the Australian Press," *Public Relations Review* 49, no. 5 (2023): 102384, https://doi.org/10.1016/j.pubrev.2023.102384.

11. Claudia Labarca, María Montt-Strabucchi, and Ingrid Bachmann, "Nuances of Public Diplomacy: China in Chilean Op Eds (2018–2021)," *Communication & Society* 36, no. 2 (2023): 339–353, https://doi.org/10.15581/003.36.2.339-353; Yu-Shan Wu, "China's Media and Public Diplomacy Approach in Africa: Illustrations from South Africa," *Chinese Journal of Communication* 9, no. 1 (2016): 81–97, https://doi.org/10.1080/17544750.2016.1139606 ; Maria Repnikova and Keyu Alexander Chen, "Asymmetrical Discursive Competition: China–United States Digital Diplomacy in Africa," *International Communication Gazette* 85, no. 1 (2023): 15–31, https://doi.org/10.1177/17480485221139460.

12. Zhe OuYang et al., "Information Asymmetry and Investor Reaction to Corporate Crisis: Media Reputation as a Stock Market Signal," *Journal of Media Economics* 30, no. 2 (2017): 82–95, https://doi.org/10.1080/08997764.2017.1364256; Bertram Scheufele, Alexander Haas, and Hans-Bernd Brosius, "Mirror or Molder? A Study of Media Coverage, Stock Prices, and Trading Volumes in Germany," *Journal of Communication* 61, no. 1 (2011): 48–70, https://doi.org/10.1111/j.1460-2466.2010.01526.x; Aeron Davis, "Media Effects and the Question of the Rational Audience: Lessons from the Financial Markets," *Media, Culture & Society* 28, no. 4 (2006): 603–625, https://doi.org/10.1177/0163443706065035; Jiyao Xun and Biao Guo, "Twitter as Customers' eWOM: An Empirical Study on Their Impact on Firm Financial Performance," *Internet Research* 27, no. 5 (2017): 1014–1038, https://doi.org/10.1108/IntR-07-2016-0223.

13. Mark Rosso, ABM Nasir, and Mohsen Farhadloo, "Chilling Effects and the Stock Market Response to the Snowden Revelations," *New Media & Society* 22, no. 11 (2020): 1976–1995, https://doi.org/10.1177/1461444820924619.

14. Ricardo Leiva-Soto, "The Media Reputation of Spain during the Global Financial Crisis," *Comunicación y Sociedad* 27, no. 2 (2014): 1–20, https://doi.org/10.15581/003.27.36002.

15. Gunther Capelle-Blancard and Aurélien Petit, "Every Little Helps? ESG News and Stock Market Reaction," *Journal of Business Ethics* 157, no. 2 (2019): 543–565, https://doi.org/10.1007/s10551-017-3667-3; Toni G. L. A. van der Meer and Rens Vliegenthart, "The Consequences of Being on the Agenda: The Effect of Media and Public Attention on Firms' Stock Market

Performance," *Communications* 43, no. 1 (2018): 5–24, https://doi.org/10.1515/commun-2017-0027.

16. Harald J. van Heerde, Els Gijsbrechts, and Koen Pauwels, "Fanning the Flames? How Media Coverage of a Price War Affects Retailers, Consumers, and Investors," *Journal of Marketing Research* 52, no. 5 (2015): 674–693, https://doi.org/10.1509/jmr.13.0260; Joanna Strycharz, Nadine Strauss, and Damian Trilling, "The Role of Media Coverage in Explaining Stock Market Fluctuations: Insights for Strategic Financial Communication," *International Journal of Strategic Communication* 12, no. 1 (2018): 67–85, https://doi.org/10.1080/1553118X.2017.1378220.

17. Christian Fieseler and Christian Pieter Hoffmann, "Linking Corporate Reputation and Journalistic Perception in Capital Markets," *Studies in Communication Sciences* 8, no. 1 (2008): 115–133, https://doi.org/10.5169/seals-791008; OuYang et al., "Information Asymmetry and Investor Reaction to Corporate Crisis: Media Reputation as a Stock Market Signal."

18. Takashi Kaneko and Bong-Soo Lee, "Relative Importance of Economic Factors in the US and Japanese Stock Markets," *Journal of the Japanese and International Economies* 9, no. 3 (1995): 290–307, https://doi.org/10.1006/jjie.1995.1015.

19. Scheufele et al., "Mirror or Molder? A Study of Media Coverage, Stock Prices, and Trading Volumes in Germany."

20. Davis, "Media Effects and the Question of the Rational Audience: Lessons from the Financial Markets."

21. Xun and Guo, "Twitter as Customers' eWOM: An Empirical Study on Their Impact on Firm Financial Performance"; Jiwei Wang and Kangtao Ye, "Media Coverage and Firm Valuation: Evidence from China," *Journal of Business Ethics* 127, no. 3 (2015): 501–511.

22. van der Meer and Vliegenthart, "The Consequences of Being on the Agenda: The Effect of Media and Public Attention on Firms' Stock Market Performance."

23. Maria Petrescu et al., "Reciprocal Influences and Effects of Viral NWOM Campaigns in Social Media," *Journal of Marketing Communications* 26, no. 7 (2020): 685–702, https://doi.org/10.1080/13527266.2018.1545244.

24. Gregory D. Saxton and Ashley E. Anker, "The Aggregate Effects of Decentralized Knowledge Production: Financial Bloggers and Information Asymmetries in the Stock Market," *Journal of Communication* 63, no. 6 (2013): 1054–1069, https://doi.org/10.1111/jcom.12060.

25. Ewelina Lacka et al., "Measuring the Real Time Stock Market Impact of Firm Generated Content," *Journal of Marketing* 86, no. 5 (2022): 58–78, https://doi.org/10.1177/00222429211042848.

26. Hui Yuan et al., "Exploring the Influence of Multimodal Social Media Data on Stock Performance: An Empirical Perspective and Analysis," *Internet Research* 31, no. 3 (2021): 871–891, https://doi.org/10.1108/INTR-11-2019-0461.

27. Hongmei Li, "The Chinese Diaspora and China's Public Diplomacy: Contentious Politics for the Beijing Olympic Float in the Pasadena Rose Parade," *International Journal of Communication* 6 (2012): 2245–2279; Zhuqing Cheng, Guy J. Golan, and Spiro Kiousis, "The Second Level Agenda Building Function of the Xinhua News Agency," *Journalism Practice* 10, no. 6 (2016):

744–762, https://doi.org/10.1080/17512786.2015.1063079; Xiaoling Zhang, Herman Wasserman, and Winston Mano, "China's Expanding Influence in Africa: Projection, Perception and Prospects in Southern African Countries," *Communicatio* 42, no. 1 (2016): 1–22, https://doi.org/10.1080/02500167.2016.1143853; Keyu Alexander Chen Glanz et al., "Adapting to Economic Shifts: CGTN's Economic Public Diplomacy on Facebook and Instagram," *Place Branding and Public Diplomacy* (2025): 1–10; George Hondroyiannis and Evangelia Papapetrou, "Macroeconomic Influences on the Stock Market," *Journal of Economics and Finance* 25, no. 1 (2001): 33–49, https://doi.org/10.1007/BF02759685; Ayse D. Lokmanoğlu et al., "The Economy and Public Diplomacy: An Analysis of RT's Economic Content and Context on Facebook," arXiv (2024), http://arxiv.org/abs/2405.01798.

28. State Media Monitor, "China Media Group," 2025, https://statemediamonitor.com/2025/08/china-media-group/.

29. Lokmanoğlu et al., "The Economy and Public Diplomacy"; Glanz et al. "Adapting to China's Currency Valuation Shifts: CGTN's Economic Public Diplomacy on Facebook and Instagram," 1–10.

30. Maarten Grootendorst, "BERTopic: Neural Topic Modeling with a Class Based TF IDF Procedure," arXiv (2022), https://doi.org/10.48550/arXiv.2203.05794.

31. Lokmanoğlu et al., "The Economy and Public Diplomacy"; Julian D. Romero et al., "Evaluating the Performance of Topic Modeling Techniques with Human Validation to Support Qualitative Analysis," *Big Data and Cognitive Computing* 8, no. 10 (2024): 132, https://doi.org/10.3390/bdcc8100132.

32. Eelke de Jong and Radislav Semenov, "Cross Country Differences in Stock Market Development: A Cultural View," University of Groningen/UMCG Research Database (2002).

33. Miguel Arce and Araceli Mora, "Empirical Evidence of the Effect of European Accounting Differences on the Stock Market Valuation of Earnings and Book Value," *European Accounting Review* 11, no. 3 (2002): 573–599, https://doi.org/10.1080/09638180220125616.

34. Jianbo Gao et al., "Complexity Changes in the US and China's Stock Markets: Differences, Causes, and Wider Social Implications," *Entropy* 22, no. 1 (2020): 75, https://doi.org/10.3390/e22010075.

35. Chen et al., "Montevideo Convention and CGTN: Defining Statehood for Global Outreach," 6833–6856; Kareem El Damanhoury et al., "Signalling Media Professionalism: Comparative Social Constructions of RT and CGTN," *The Journal of International Communication* 30, no. 2 (2024): 347–371, https://doi.org/10.1080/13216597.2024.2359715; Virginia Massignan et al., "Digital Influence Strategies in Information Warfare: A Multimodal, Cross-Platform Comparative Analysis of Russia Today and China Global Television Network," in *Advancing the SOF Warrior Mind: Essays from the JSOU Academic Year 2025 Call for Special Operations Papers* (JSOU Report 25-20, Joint Special Operations University Press, 2025), 199–217, https://www.jsou.edu/Press/PublicationDashboard/290.

36. T. A. H. Dilpriya et al., "Analysing the S&P 500 Index in Relation to the Google Trends of Stock Market Related Words in the United States," in *Transformative Applied Research in Computing, Engineering, Science and Technology*, ed. D. Dahanayake and M. Rabindrakumar (CRC Press, 2024), 133–140, https://doi.org/10.1201/9781003616368-17; Magnus Pedersen,

"Comparison of U.S. Stock Indices," SSRN (2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2667556; Suneel Maheshwari and Deepak Raghava Naik, "Efficiency in Operations of NASDAQ Listed Technology Companies from 2011 to 2023," *Journal of Risk and Financial Management* 17, no. 5 (2024): 205, https://doi.org/10.3390/jrfm17050205.

37. Dahong Guan, "Study on Relativity Between China's Nominal GDP and the Shanghai Securities Composite Index," *Journal of Service Science and Management* 11, no. 5 (2018): 527–542, https://doi.org/10.4236/jssm.2018.115036; Chuan Wang, Zoltan Murgulov, and Janto Haman, "Impact of Changes in the CSI 300 Index Constituents," *Emerging Markets Review* 24 (2015): 13–33, https://doi.org/10.1016/j.ememar.2015.05.005.

38. Graham Kalton and Ismael Flores-Cervantes, "Weighting Methods," *Journal of Official Statistics* 19, no. 2 (2003): 81–97.

39. Gao et al., "Complexity Changes in the US and China's Stock Markets," 75; Hayden, "Logics of Narrative and Networks in US Public Diplomacy," 196–218; Guan, "Study on Relativity Between China's Nominal GDP," 527–542; Wang et al., "Impact of Changes in the CSI 300 Index Constituents," 13–33.

40. Arsenault, "Public Diplomacy 2.0," 135–153; Wu, "China's Media and Public Diplomacy Approach in Africa," 81–97; Lokmanoğlu et al., "The Economy and Public Diplomacy"; Roman Egger and Joanne Yu, "A Topic Modeling Comparison Between LDA, NMF, Top2Vec, and BERTopic to Demystify Twitter Posts," *Frontiers in Sociology* 7 (2022): 886498, https://doi.org/10.3389/fsoc.2022.886498; Grootendorst, "BERTopic: Neural Topic Modeling with a Class-Based TF-IDF Procedure"; Romero et al., "Evaluating the Performance of Topic Modeling Techniques," 132; Dilpriya et al., "Analysing the S&P 500 Index," 133–140;.

41. Hondroyiannis and Papapetrou, "Macroeconomic Influences on the Stock Market," 33–49; Kaneko and Lee, "Relative Importance of Economic Factors in the US and Japanese Stock Markets," 290–307; Lokmanoğlu et al., "The Economy and Public Diplomacy"; Capelle-Blancard and Petit, "Every Little Helps?" 543–565; Xuejun Jin, Cheng Chen, and Xiaolan Yang, "The Effect of International Media News on the Global Stock Market," *International Review of Economics & Finance* 89 (2024): 50–69, https://doi.org/10.1016/j.iref.2023.07.096; Darius Fatemi et al., "Effect of Media Freedom on Liquidity and Information Asymmetry: Evidence from Non-U.S. Stocks in the NYSE," *Journal of Media Economics* 36, nos. 3–4 (2024): 93–111, https://doi.org/10.1080/08997764.2024.2411982; Rosso et al., "Chilling Effects and the Stock Market Response to the Snowden Revelations," 1976–1995; Leiva-Soto, "The Media Reputation of Spain during the Global Financial Crisis," 1–20; de Jong and Semenov, "Cross-Country Differences in Stock Market Development"; Arce and Mora, "Empirical Evidence of the Effect of European Accounting Differences on the Stock Market Valuation of Earnings and Book Value," 573–599.

42. Maria-José Canel, Evandro Samuel Oliveira, and Vilma Luoma-aho, "Exploring Citizens' Judgments about the Legitimacy of Public Policies on Refugees: In Search of Clues for Governments' Communication and Public Diplomacy Strategies," *Journal of Communication Management* 21, no. 4 (2017): 355–369, https://doi.org/10.1108/JCOM-02-2017-0025; James Pamment, Alexandra Olofsson, and Rachel Hjorth-Jenssen, "The Response of Swedish and Norwegian Public Diplomacy and Nation Branding Actors to the

Refugee Crisis," *Journal of Communication Management* 21, no. 4 (2017): 326–341, https://doi.org/10.1108/JCOM-03-2017-0040; Hobbs et al., "Grand Strategy and Public Diplomacy," 102384; Labarca et al., "Nuances of Public Diplomacy," 339–353; Li, "The Chinese Diaspora and China's Public Diplomacy," 2245–2279.

Digital Force Protection in the Public Sensorium: A Counterintelligence Playbook for SOF Against Open-Source Intelligence Targeting, Narrative Preconditioning, and Ambient Data Trails

By Chief Warrant Officer 3 (Ret.)
Wayne N. Taylor, EdD, PhD(c)

Abstract

As special operations forces (SOF) increasingly operate in environments where digital traces are as consequential as physical presence, counterintelligence (CI) must adapt to the reality of a ubiquitous, participatory information environment—the "public sensorium." This article advances a conceptual playbook for digital force protection, outlining strategies to mitigate risks posed by open-source intelligence (OSINT) targeting, adversarial narrative preconditioning, and the exploitation of ambient data trails. Drawing on scholarship in intelligence studies,[1] critical security studies,[2] and media theory,[3] the article argues that adversaries increasingly weaponize openness, algorithmic amplification, and ubiquitous data to shape perceptions and exploit vulnerabilities. The proposed framework emphasizes operational security (OPSEC), digital hygiene, and cognitive resilience as essential complements to traditional CI doctrine.

Introduction

Historically, force protection emphasized keeping people, equipment, and facilities safe from physical threats. Yet—as Clausewitz would likely remind us—the character of war changes with the "spirit of the age," even as its underlying nature endures.[4] Today's social and technological conditions have shifted much of the exposure surface from the kinetic to the informational, making protection in the information environment as consequential as body armor and blast walls. This shift is inseparable from the rise of the platformed, "datafied" internet. Social media has been weaponized by states, criminal networks, and movements, turning feeds into battlespaces and attention into terrain.[5] Meanwhile, the commercial location-data economy shows how "anonymous" device pings can be tied back to real people and places—at scale—posing obvious risks to personnel and missions.[6] U.S. defense leaders responded to

adjacent risks by restricting geolocation features on devices in 2018, underscoring how digital exhaust can become an OPSEC liability.[7] Practically, every Instagram story, passive geolocation ping, or unguarded narrative fragment contributes to a composite, targetable identity. Scholars describe this broader condition as datafication and participatory surveillance—a socio-technical environment in which users, platforms, and data brokers continuously produce and trade signals that can re-identify individuals and infer sensitive attributes (home/work, health, beliefs).[8] Research shows that seemingly benign social metadata and older app behaviors can pinpoint users' addresses and "sensitive" visits with high accuracy, while U.S. Army OPSEC guidance now explicitly warns troops and families about geotagging and oversharing.

For SOF, whose operational edge relies on anonymity, precision, and surprise, this ambient exposure creates both strategic and tactical liabilities. We call the contemporary battlespace the public sensorium: a participatory, always-on, distributed ecology in which people, algorithms, and infrastructures generate, archive, and amplify signals. Within this sensorium, adversaries can manipulate, extract, and weaponize information at low cost and with limited attribution—patterns documented in recent histories of disinformation and in U.S. testimony calling for cognitive security.[9] Case studies—such as the Strava heatmap revealing activity around sensitive facilities—illustrate how ordinary digital traces can compromise operational patterns and locations.[10]

Open-Source Intelligence Targeting and the SOF Profile

OSINT has moved well beyond hand-curated clippings and ad hoc searches. Contemporary OSINT pipelines are algorithmically augmented: adversaries fuse cross-platform collection with machine-learning classifiers (e.g., natural language processing

> ***For SOF, the paradox is stark: operational secrecy collides with the ambient digital presence of operators, families, contractors, and local partners.***

on social streams, image/video feature extraction, network clustering) to surface targets and vulnerabilities at scale.[11] These toolchains are increasingly "productized"—from automated account discovery and topic clustering to templated persona generation—compressing the time between discovery, targeting, and narrative activation. For defenders, this means the relevant attack surface is not only what an operator posts but also the metadata and correlations that arise when disparate, seemingly benign traces are aggregated and modeled.

Recent cases highlight the scope of the threat:

- Fitness apps like Strava's global heatmap visualized users' workouts in ways that exposed base perimeters and habitual routes—an object lesson in how "anonymous" aggregates can reveal sensitive patterns.[12]
- Family social media posts provide adversaries with indicators of unit deployment, rotations, and morale. Official OPSEC guidance warns that seemingly benign posts about deployments, rotations, and unit routines can be assembled into a larger picture useful to adversaries.[13]
- Data brokers aggregate innocuous-seeming consumer data (e.g., ridesharing histories, purchases, Internet of Things [IoT] signals) into actionable intelligence.[14] Commercial data brokers aggregate mobility, purchase, app-usage, and advertising telemetry into highly granular profiles. U.S. regulators have documented the breadth of this market[15]

and, more recently, prohibited firms from selling or sharing precise/sensitive location data.[16] In parallel, the Office of the Director of National Intelligence (ODNI) issued an Intelligence Community framework acknowledging both the utility and national security risks of commercially available information (CAI).[17]

For SOF, the paradox is stark: operational secrecy collides with the ambient digital presence of operators, families, contractors, and local partners. CI frameworks must therefore assume adversaries can collect, correlate, and weaponize public and commercial data at speed. Practically, this implies (1) pre-mission digital hygiene for units and families; (2) continuous OSINT telemetry and indicators monitoring (e.g., sudden engagement spikes, cross-platform narrative synchronization); and (3) integrating analytic rigor—such as capture, lay out, examine, align, reflect (CLEAR) mapping and challenge-based structured analytic techniques—into digital force protection to stress-test assumptions before they become liabilities.[18]

Adversaries no longer merely react to events; they work to shape the interpretive lens before events occur.

Narrative Preconditioning

Adversaries no longer merely react to events; they work to shape the interpretive lens before events occur. In communication research, this combines classic framing—selecting and emphasizing certain aspects of reality to promote a particular problem definition or moral evaluation[19]—with agenda-setting, which elevates some topics (and attributes of those topics) to salience so that audiences are primed to notice them.[20] In influence tradecraft, related concepts include pre-suasion (preparing audiences' "state of mind" before a message)

and, in military studies, reflexive control (shaping an opponent's perceptions and expected utility to steer decisions).[21] Collectively, these practices amount to narrative preconditioning: seeding frames, tropes, and discourses ahead of time so that subsequent facts are interpreted within an adversary-favorable storyline.[22]

Three techniques are particularly relevant for SOF:

1. **Planting disinformation (pre-event "receipts")**: Adversaries introduce plausible claims—civilian casualty allegations, corruption narratives, or "illegitimacy" frames—before deployments or operations commence. This leverages the "firehose of falsehood" model: high-volume, multichannel messaging with rapid, continuous, and repetitive content that overmatches traditional refutation and leaves durable doubt even after corrections.[23] Contemporary assessments of coercive information operations note similar patterns: pre-crisis shaping and public opinion "priming" that narrows policy options once an incident occurs.[24]

2. **Exploiting cultural fissures (domestic alignment)**: Narrative preconditioning is most potent when it maps onto existing social divisions. Empirical work on the Internet Research Agency shows systematic amplification of U.S. divisions (race, religion, guns, immigration, etc.) and even orchestration of opposing rallies to pre-shape audience interpretations of later events.[25] Public health research similarly documents troll/bot activity injecting polarizing frames into vaccine debates to erode consensus before outbreaks or policy changes.[26] Strategic analysis places this squarely within modern "political warfare," where states and proxies prepare the ground by polarizing targets long in advance.[27]

3. **Amplifying ambiguity (manufacturing doubt)**: Rather than persuading audiences of a single falsehood, adversaries flood

the zone with contradictory takes, "just asking questions," and authenticity challenges that muddy verification.[28] RAND's Firehose model highlights why refutations struggle under such conditions.[29] The deepfake literature warns of a related "liar's dividend"—once people know sophisticated manipulation exists, malicious actors can dismiss authentic evidence as fake, compounding uncertainty and softening accountability.[30]

As Rid (2020)[31] emphasizes in his history of active measures, effective disinformation leans on fragments of truth and strategic ambiguity to seed doubt—and doubt, not belief in any single false claim, is often the operational end state. For SOF, this means entering battlespaces that are already narratively tilted: reputational baselines are degraded, stakeholder perceptions have been pre-shaped, and tactical incidents are interpreted through hostile frames that reduce freedom of maneuver in both the operational and informational domains.[32]

Ambient data trails create a double vulnerability.

Ambient Data Trails

Modern life generates what Zuboff (2019) calls "digital exhaust"—continuous byproducts of everyday activity such as location traces, biometric signals, purchase histories, app telemetry, and IoT device logs.[33] For SOF, these ambient data trails create a double vulnerability: they can reveal operational patterns (e.g., routes, rhythms, associations) and compromise personal/family security through doxxing, stalking, or targeted influence. U.S. defense leaders have acknowledged the operational risk of geolocation exhaust—restricting geolocation features on devices in 2018—while public episodes like the Strava heatmap incident demonstrate

how "anonymous" aggregates can expose base perimeters and habitual movements.[34]

- **Persistence:** Once generated, many data traces are durable—replicated, backed up, and archived across platforms, clouds, and broker warehouses—often beyond any single individual's control. Mayer-Schönberger argued that digital memory's low cost and ubiquity erode the natural "forgetting" that once protected privacy, while U.S. regulators have documented how data brokers collect, retain, and resell large volumes of personal data over time.[35] Intelligence Community policy similarly flags that CAI can reveal sensitive details about individuals and therefore requires heightened safeguards when acquired or retained.[36]
- **Aggregability:** Disparate crumbs—fitness app logs, loyalty card purchases, rideshare histories, ad-tech telemetry, and IoT signals—can be linked and fused into granular behavioral profiles.[37] Classic re-identification work shows that just four spatiotemporal points can uniquely identify the vast majority of people in a mobility dataset.[38] Public investigations and research syntheses describe how commercial brokers and ad-tech "identity graphs" stitch device IDs, IP addresses, and home/work geofences to build persistent dossiers.[39] Within national security context, reporting and records disclosures show U.S. government entities have purchased app-derived location data (e.g., Venntel/Babel Street), underscoring how readily these profiles can be operationalized.[40]
- **Opacity:** Operators and families often underestimate the volume, persistence, and accessibility of their digital traces. The National Institute of Standards and Technology's (NIST) guidance highlights the privacy risks of IoT ecosystems, where data flows are complex and non-transparent.41

> The ODNI's CAI framework explicitly warns that CAI, while useful, also poses privacy, civil liberties, and CI risks because it can reveal "sensitive and intimate information" when aggregated.[42] Press and policy analyses—such as the One Nation, Tracked series—show how "anonymous" location files allow reconstruction of identities and sensitive visits, making opacity a practical, not merely theoretical, problem.[43]

In CI terms, ambient data trails constitute inadvertent self-disclosure: continuous, passive, and exploitable. Unlike a discrete human intelligence (HUMINT) leak, this disclosure is systemic and infrastructural—emerging from the routine operation of commercial platforms, advertising markets, and consumer devices—and thus requires force-protection responses that combine policy (e.g., geolocation restrictions), technical controls (e.g., device/app hygiene), and analytic monitoring of CAI-driven indicators.

Working Toward a Counterintelligence Playbook

The proposed CI playbook for digital force protection emphasizes proactive, layered strategies:

1. Digital hygiene & training (operator + household)

Objectives: Reduce discoverable signatures; raise baseline CI awareness across operators and their family networks; institutionalize periodic self-audits.

Core practices:

- **Quarterly OSINT self-audits (red-team simulations):** Task CI/cyber red teams to enumerate open-source indicators (addresses, vehicles, workplaces, children's schools, fitness routes, club memberships, home photos, etc.), then

brief remediation steps. Use defender frameworks (e.g., disinformation analysis and risk management [DISARM]/ adversarial information influence tactics and techniques [AMITT]) to map likely influence/collection tactics, techniques, and procedures (TTP) and plan mitigations.[44]

- **Family network education:** Issue a short, recurring brief to spouses/partners and adult family members that covers location privacy, social media posting norms, and phishing recognition. The National Security Agency's (NSA) "Keeping Safe on Social Media" and the Department of War's (DoW) OPSEC student guide provide practical, family-friendly checklists.[45]
- **Social media conduct ("Think. Type. Post."):** Adopt and enforce the Army's well-known triad across units and family readiness groups; point to official Army personal-use guidance pages in welcome packets and pre-deployment briefs.[46]
- **Command-level OPSEC refreshers:** Re-baseline against current doctrine (e.g., Navy TTP 3-13.3; Air Force Doctrine Publication [AFDP]/ Field Manual [FM] 3-61 for public affairs [PA]/communication strategy), emphasizing signatures, associations, profiles, contrasts, and exposure and how seemingly "benign" posts aggregate into targetable patterns.[47]

Why it matters: OPSEC training notes that adversaries combine small, unclassified "puzzle pieces" from social and open sources to infer deployments and capabilities; assessing that aggregation risk is a required step.[48]

2. Narrative immunization (prebunking + wargaming)

Objectives: Inoculate forces against adversarial narratives before contact; practice response under realistic tempo; align CI/PA/psychological operations (PSYOP) lanes.

Core practices:

- **Pre-briefs using inoculation theory:** Short "prebunking" modules (what claims you'll likely see; how they manipulate emotion/identity; how to spot cheap fakes) improve resistance across cultures and platforms.[49]
- **Disinformation tabletop exercises and wargames:** Run pre-deployment Information Warfighter Exercise (IWX)-style injects (rumors, doxxing, deepfakes, edited body-worn camera violations) with time pressure and PA/legal injects.[50] RAND's IWX rulebook and Johns Hopkins University Applied Physics Laboratory's national-level recommendations provide off-the-shelf scaffolds.
- **Defender tactics playbooks:** Use the DISARM/AMITT matrices to map adversary TTP (e.g., seeded leaks, troll amplification, sock puppets) to specific mitigations (rapid provenance checks, "truth sandwich" responses, platform reporting).[51]
- **Doctrine-aligned public communication:** Coordinate counternarratives through PA vice ad hoc responses; tie messages to mission legality, proportionality, and local partnerships.[52]

Why it matters: Psychological "inoculation" (forewarning + refutational preemption) measurably reduces susceptibility to manipulation. Competing in the information environment is now a core DoW imperative, not a supporting activity.[53]

3. Ambient data awareness (mobile + IoT + data brokers)

Objectives: Detect and minimize passive signatures from phones, wearables, vehicles, and smart homes, and constrain brokered data reuse.

Core practices:

- **Mission-integrated IoT risk reviews:** Include NIST Interagency or Internal Report 8228–style IoT privacy/cyber risk considerations in concept of operations (device inventory, default creds, telemetry paths, firmware update posture, cloud sync behavior, etc.).[54]
- **Device minimization and geolocation controls:** For high-risk phases, physically secure or leave all wireless devices (including wearables) at a non-sensitive location. If devices must be carried, apply NSA's location-exposure mitigations.[55]
- **Household posture hardening:** Extend those mitigations to family devices and vehicles (e.g., infotainment telematics, smart doorbells, cameras); pair with NSA social media safety guidance.[56]
- **Geolocation policy compliance:** Enforce the 2018 DoW restriction on geolocation features for government personnel and devices, and brief implications for personal devices in proximity to operations.[57]
- **Broker risk management:** Apply ODNI's 2024 CAI framework to any acquisition or use of commercially available data (e.g., sensitivity test, purpose limitation, re-evaluation cadence, safeguarding) and harmonize with NIST privacy guidance.[58]

Why it matters: Location and telemetry exposures are inherent to modern devices and cloud services. Even with GPS off, Wi-Fi/Bluetooth and sensor fusion can reconstruct movements (NSA, 2020). IoT and "smart home" ecosystems expand the attack surface to family spheres, while data brokers turn innocuous trails into actionable profiles.[59]

4. Cognitive & cultural resilience (people + partners)

Objectives: Build operator media literacy, interpretive skepticism, and cultural fluency; reinforce public trust through doctrine-aligned PA; integrate with SOF information capabilities.

Core practices:

- **Media literacy standards and drills:** Incorporate evidence-based standards to counter "truth decay" and rehearse rapid source-verification and lateral reading during operations.[60]
- **Cultural awareness for narrative anticipation:** Use FM 3-24 and Boyd-derived decision-advantage thinking to map local grievances, honor codes, and identity frames adversaries may exploit.[61]
- **Public engagement via PA:** Align community engagement and transparency with Joint Publication (JP)/Service PA doctrine to sustain legitimacy and preempt rumor cascades.[62]
- **SOF information integration:** Leverage U.S. Special Operations Command's (USSOCOM) role as joint proponent for internet-based PSYOP and the Joint MISO WebOps Center (JMWC) for synchronized, policy-compliant effects and partner support.[63]

Why it matters: Adversaries exploit polarized environments and low trust. Building cognitive immunity and communicating within doctrine preserves freedom of maneuver in the information domain.[64]

Implications for Counterintelligence and SOF Doctrine

Traditional U.S. CI emphasizes deception detection, insider-threat mitigation, and HUMINT-centric investigations, underpinned by analytic tradecraft such as Structured Analytic Techniques.[65] In the platformed information environment, however, digital force protection reframes CI as proactive and anticipatory. Adversaries' primary weapons are increasingly the aggregation and weaponization of open, ambient, and narrative data—CAI, publicly available information, and platform telemetry—rather than physical infiltrators or planted doubles.[66] This evolution aligns with joint doctrine's elevation of information as a joint function and with the Joint Concept for Operating in the Information Environment (JCOIE), which directs commanders to build information into operational art.[67]

Hybrid Threat Recognition

SOF planning and assessment should treat digital indicators—narrative shifts, bot-driven amplification, CAI exposure, location-exhaust patterns—as coequal with kinetic indicators during mission analysis, joint intelligence preparation of the environment (JIPOE), and rehearsal.[68] JP 3-05 stresses SOF integration with the joint force, while service doctrine (e.g., AFDP 3-13) codifies the informational aspects of all actions[69] (JP 3-05; AFDP 3-13). The Government Accountability Office (GAO) has likewise urged the DoW to better integrate operations in the information

environment (OIE) across functions and to address governance gaps revealed in recent reviews.[70]

Doctrine implications include:

- Making information environment (IE) variables (e.g., audience frames, data-broker exposure, platform dynamics) explicit in the intelligence estimate and JIPOE annexes (JP 2-0/Service 2-0)
- Adding CAI/publicly available information risk and narrative-preconditioning checks to SOF mission approval processes

Cross-Domain Collaboration

Current policy (Department of Defense Directive [DoDD] 5240.02; DoDD 5240.06) defines CI authorities and awareness requirements, but they must be operationalized alongside cyber defense, PA, and psychological operations (PSYOP) for digital force protection.[71] USSOCOM's role as the DoW's coordinating authority for internet-based MISO and sponsor of the JMWC provides an organizational bridge between CI risk sensing and information effects. Recent posture statements and oversight reviews highlight both progress and capability gaps.[72] Command-level synchronization with service doctrine (e.g., AFDP 3-13) and JCOIE closes seams between CI detection, cyber hardening, and narrative maneuver.[73]

Doctrine implications include:

- Needing to formalize a CI–Cyber–MISO battle rhythm (e.g., shared indicators, cross-cueing, rapid content provenance checks)
- Treating publicly available information and CAI acquisition and use as a CI-relevant activity governed

by ODNI's CAI framework (privacy, sensitivity tests, cataloging, re-evaluation)[74]

Continuous Adaptation

Platform affordances, broker markets, and AI-enabled manipulation techniques change rapidly, and doctrine and TTP must adapt accordingly.[75] JCOIE and subsequent service doctrine call for deliberate integration of information into operations. GAO findings and Congressional Research Service primers underscore the need for enduring governance and resourcing for OIE.[76] Complementary guidance from ODNI on CAI and NATO/StratCom analyses on AI-driven precision persuasion provide current benchmarks for policy-compliant adaptation.[77]

Doctrine implications include:

- Establishing quarterly CI/OIE update cycles (platform policy changes, new CAI sources, adversary TTP)
- Integrating prebunking/inoculation modules and OIE tabletops into SOF certification—tying analytic standards (Intelligence Community Directive 203–style tradecraft) to response playbooks

Conclusion

Operating inside a public sensorium compels a fundamental reset of SOF CI.[78] Digital force protection is no longer an accessory to tradecraft; it is the precondition for mission credibility, survivability, and freedom of maneuver. When OSINT targeting, narrative preconditioning, and ambient data trails are treated as primary threat vectors, units can blunt adversaries who weaponize openness and scale.[79] What must change is both how we fight and who we believe is on the battlefield. First, the center of effort moves from perimeters to patterns: it is the aggregate of tiny, routine emissions—

posts, pings, purchase histories, platform correlations—that exposes units and families. Second, the decisive point shifts from secrecy to hygiene: disciplined, repeatable behaviors by operators and households often do more for survivability than any single technical control. Third, readiness becomes continuous: platform affordances, broker markets, and AI-enabled manipulation evolve too quickly for annual refreshers or static standard operating procedures (SOPs); CI must iterate at "platform speed."[80]

Translating this into doctrine and practice means institutionalizing four non-negotiables:

1. **Hybrid threat recognition.** Treat digital indicators—narrative shifts, bot-amplification patterns, CAI exposure, location exhaust—as coequal with kinetic indicators during intelligence preparation of the battlefield/JIPOE, rehearsals, and mission approval.

2. **Cross-domain choreography.** Bind CI to cyber defense, PSYOP, and PA through shared indicators, cross-cueing, rapid provenance checks, and preapproved response playbooks that protect civil liberties while preserving narrative initiative.

3. **Family-inclusive protection.** Extend pre-deployment briefs and device posture hardening to spouses/partners and adult dependents; build household posture into unit readiness just as we do medical/dental and gear.

4. **Quarterly adaptation.** Update CI/OIE playbooks on a fixed cadence (quarterly as a floor): platform policy changes, new CAI sources, adversary TTPs, and lessons from after action reports (AARs) feed directly into training blocks and SOPs.

To ensure these reforms endure, commanders should demand measurable outcomes—not just good intentions. Useful metrics include time to detect a narrative spike, time to verify content

provenance, percentage of devices meeting hardened baselines, rate of location-leak incidents, coverage of family brief participation, red-team OSINT findings closed within a defined window, and the false-positive rate of alerts so units don't drown in noise. These measures of performance and measures of effectiveness must be linked to certification events and AARs to create a learning loop. Ethically, success requires operational restraint and transparency. Digital force protection must be bound by data minimization, purpose limitation, and clear guardrails for any CAI or publicly available information use. Doing the right thing procedurally—documenting what was collected, why, and for how long—is part of maintaining the moral high ground that SOF relies on for access, local consent, and strategic legitimacy.[81]

Success requires operational restraint and transparency.

Finally, a realistic research and development agenda should accompany doctrine: automated provenance and deepfake triage at the edge, broker-market mapping and risk scoring for common data feeds, inoculation training that travels well across cultures and partner forces, and evaluation designs that tie information-domain readiness to real operational effects. Partnerships with interagency teams, academia, and vetted industry can accelerate this work without compromising authorities or ethics.[82]

If SOF integrates these disciplines—linking CI with cyber defense, PSYOP/PA, legal, and privacy frameworks—and measures them with the same rigor applied to kinetic tasks, it will retain initiative in contested information environments. The operational objective is simple and non-negotiable: arrive with surprise, operate with legitimacy, and depart without a trace—even when the adversary is watching through a million civilian sensors.[83]

About the Author

Chief Warrant Officer 3 (Ret.) Wayne N. Taylor is an assistant professor of homeland security and emergency management at Eastern Kentucky University. He served in the U.S. Army as an Area Intelligence Officer and Counterintelligence Agent with support to special operations forces and Tier 1 units. Prior to EKU, he directed the Office of Veteran Success at the University of South Florida, leading strategic initiatives that secured a $10 million legislative allocation and helped establish Florida's Purple Star Collegiate Program. His teaching and research focus on intelligence studies, experiential and gamified learning, veteran transitions in higher education, and a meta-cognitive framework for transparent, bias-aware reasoning. Dr. Taylor holds a bachelor's degree in security management and a master's degree in administration of justice and security, earned an Ed.D. in program development, and is completing a Ph.D. in curriculum and instruction at the University of South Florida.

Notes

1. Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (Farrar, Straus and Giroux, 2020); Randolph Pherson and Richards Heuer, *Structured Analytic Techniques for Intelligence Analysis* (CQ Press, 2011).

2. Ronald Deibert, *Black Code: Inside the Battle for Cyberspace* (Signal, 2013); Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs, 2019).

3. Danah Boyd, *It's Complicated: The Social Lives of Networked Teens* (Yale University Press, 2014); Guy Debord, *The Society of the Spectacle* (Black & Red, 1977).

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

5. P. W. Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media* (Houghton Mifflin Harcourt, 2018).

6. Jennifer Valentino-DeVries et al., "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret," *The New York Times*, December 10, 2018, https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

7. U.S. Deputy Secretary of Defense to Chief Management Officer of the Department of Defense et al., "DoD Policy on the Use of Geolocation-Capable Devices, Applications, and Services," August 3, 2018.

8. Yves-Alexandre de Montjoye et al., "Unique in the Crowd: The Privacy Bounds of Human Mobility," *Scientific Reports* 3 (2013).

9. Rid, *Active Measures*; Rand Waltzman, *The Weaponization of Information: The Need for Cognitive Security,* 115th Cong. (2017) (testimony of Rand Walzman, RAND Corporation).

10. Alex Hern, "Fitness Tracking App Strava Gives Away Location of Secret U.S. Army Bases," *The Guardian*, January 28, 2018, https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases.

11. John Gentry, *Strategic Warning Intelligence: History, Challenges, and Prospects* (Georgetown University Press, 2018); "ACT Strategic Foresight Work," NATO Allied Command Transformation, accessed October 16, 2025, https://www.act.nato.int/activities/allied-command-transformation-strategic-foresight-work/; Rolf Fredheim, *Virtual Manipulation Brief 2023/1: Generative AI and Its Implications for Social Media Analysis* (NATO Strategic Communications Centre of Excellence, 2023), https://stratcomcoe.org/publications/virtual-manipulation-brief-20231-generative-ai-and-its-implications-for-social-media-analysis/286; Gundars Bergmanis-Korats et al., *AI in Precision Persuasion. Unveiling Tactics and Risks on Social Media* (NATO Strategic Communications Centre of Excellence, 2024), https://stratcomcoe.org/publications/ai-in-precision-persuasion-unveiling-tactics-and-risks-on-social-media/309; Katerina Sedova et al., "AI and the Future of Disinformation Campaigns Part 2: A Threat Model" (Center for Security and Emerging Technology, December 2021), https://doi.org/10.51593/2021CA011.

12. Hern, "Fitness Tracking App Strava Gives Away Location of Secret US Army Bases."

13. U.S. Department of Defense, *Operations Security (OPSEC) Program Manual*, DoD Manual 5205.02 (Department of Defense, 2021); Joint Chiefs of Staff, *Operations Security,* Joint Publication 3-13.3 (Joint Chiefs of Staff, 2020); "U.S. Army Social Media Guide – Safety and Security Guidance," U.S. Army, accessed October 15, 2025; https://www.army.mil/socialmedia/safety/.

14. Julie Brill, "Demanding Transparency from Data Brokers," *The Washington Post, August 15,* https://www.ftc.gov/sites/default/files/documents/public_statements/demanding-transparency-data-brokers/130815databrokers.pdf.

15. Federal Trade Commission, *Data Brokers: A Call for Transparency and Accountability*, U.S. Government Report (Federal Trade Commission, May 2014), https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014.

16. Federal Trade Commission, "FTC Takes Action Against Gravy Analytics, Venntel for Unlawfully Selling Location Data Tracking Consumers to Sensitive Sites," December 3, 2024, https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-takes-action-against-gravy-analytics-venntel-unlawfully-selling-location-data-tracking-consumers.

17. Office of the Director of National Intelligence (ODNI), *Intelligence Community Policy Framework for Commercially Available Information*, U.S. Government Report (Office of the Direction of National Intelligence, May 2024), https://archive.dni.gov/files/ODNI/documents/CAI/Commercially-Available-Information-Framework-May2024.pdf.

18. Sedova et al., "AI and the Future of Disinformation Campaigns Part 2: A Threat Model."

19. Robert M. Entman, "Framing: Toward Clarification of a Fractured Paradigm," *Journal of Communication* 43, no. 4 (Autumn 1993): 51–58, https://doi.org/10.1111/j.1460-2466.1993.tb01304.x.

20. Maxwell E. McCombs and Donald L. Shaw, "The Agenda-Setting Function of Mass Media," *Public Opinion Quarterly* 36, no. 2 (Summer 1972): 176–187, https://www.jstor.org/stable/2747787.

21. Robert B. Cialdini, *Pre-Suasion: A Revolutionary Way to Influence and Persuade* (Simon & Schuster, 2016); Maria W. R. de Goeij, "Reflexive Control: Influencing Strategic Behavior," *The U.S. Army War College Quarterly: Parameters* 53, no.4 (Winter 2023): 97–107, https://press.armywarcollege.edu/parameters/vol53/iss4/14/; Timothy Thomas, "Russia's Reflexive Control Theor and the Military," *The Journal of Slavic Military Studies* 17 no. 2 (2004): 237–256, https://doi.org/10.1080/13518040490450529.

22. Remington Whiteside, "Narrative Manipulation, Malinfluence Operations, and Cognitive Warfare Through Large Language Model Poisoning with Adversarial Noise," *MI Professional Bulletin*, October 1, 2025, https://mipb.ikn.army.mil/issues/jul-dec-2025/narrative-manipulation-malinfluence-operations-and-cognitive-warfare-through-large-language-model-poisoning-with-adversarial-noise/.

23. Christopher Paul and Miriam Matthews, *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It* (RAND Corporation, 2016), https://www.rand.org/pubs/perspectives/PE198.html.

24. U.S. Army War College, *Information Operations Primer: Fundamentals of Information Operation* (U.S. Army War College, 2011), https://nsarchive.gwu.edu/sites/default/files/documents/3002260/Document-04.pdf.

25. Phillip Howard et al., "Computational Propaganda," Oxford Internet Institute, University of Oxford, January 2016–August 2021, https://www.oii.ox.ac.uk/research/projects/computational-propaganda/.

26. David A. Broniatowski et al., "Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate," *American Journal of Public Health* 108, no. 10 (October 2018): 1378–1384, https://doi.org/10.2105/AJPH.2018.304567.

27. Alina Polyakova and Spencer P. Boyer, *The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition* (Brookings Institution, 2018), https://www.brookings.edu/articles/the-future-of-political-warfare-russia-the-west-and-the-coming-age-of-global-digital-competition/.

28. Waltzman, testimony on *The Weaponization of Information*.

29. Paul and Matthews, The Russian "Firehose of Falsehood" Propaganda Model.

30. Robert Chesney and Danielle Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," *California Law Review* 107 (2019): 1753–1819, https://www.californialawreview.org/print/deep-fakes-a-looming-challenge-for-privacy-democracy-and-national-security; Ullrich Ecker et al., "The Psychological Drivers of Misinformation Belief and Its Resistance to Correction," *Nature Reviews Psychology* 1 (2022): 13–29, https://doi.org/10.1038/s44159-021-00006-y.

31. Rid, Active Measures.

32. Polyakova and Boyer, The Future of Political Warfare; Waltzman, testimony on *The Weaponization of Information*.

33. Zuboff, The Age of Surveillance Capitalism.

34. U.S. Deputy Secretary of Defense, "Geolocation Policy;" Hern, "Strava Fitness App Reveals Military Bases."

35. Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press, 2009); Federal Trade Commission, *Data Brokers*.

36. Office of the Director of National Intelligence, *Intelligence Community Policy Framework for Commercially Available Information*.

37. Brill, "Demanding Transparency from Data Brokers."

38. de Montjoye et al., "Unique in the Crowd: The Privacy Bounds of Human Mobility."

39. Justin Sherman, *Data Brokers and Sensitive Data on U.S. Individuals: Threats to American Civil Rights, National Security, and Democracy* (Duke University Sanford School of Public Policy), https://techpolicy.sanford.duke.edu/wp-content/uploads/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf.

40. American Civil Liberties Union, "New Records Detail DHS Purchase and Use of Vast Quantities of Cell Phone Location Data," July 18, 2022, https://www.aclu.org/press-releases/new-records-detail-dhs-purchase-and-use-vast-quantities-cell-phone-location-data-0; Joseph Cox, "How the U.S. Military

Buys Location Data from Ordinary Apps," *VICE*, November 16, 2020, https://www.vice.com/en/article/us-military-location-data-xmode-locate-x/.

41. Kaitlin Boeckl et al., *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*, NIST IR 8228 (National Institute of Standards and Technology - Computer Security Resource Center, 2019), https://doi.org/10.6028/NIST.IR.8228.

42. Office of the Director of National Intelligence, *Intelligence Community Policy Framework for Commercially Available Information.*

43. Stuart A. Thompson and Charlie Warzel, "One Nation, Tracked: An Investigation Into the Smartphone Tracking Industry from Times Opinion," *The New York Times,* December 19–21, 2019, https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html.

44. "Home," DISARM Foundation, n.d., https://www.disarm.foundation/; "Home," MITRE, n.d., https://www.mitre.org/.

45. Center for Development of Security Excellence (CDSE), *OPSEC Fundamentals for OPSEC Practitioners Course Student Guide* (Center for Development of Security Excellence, 2025), https://www.cdse.edu/Portals/124/Documents/student-guides/OP110-guide.pdf; National Security Agency (NSA), *Keeping Safe on Social Media* (U.S. Department of War, 2020), https://media.defense.gov/2021/Feb/04/2002576239/-1/-1/0/KEEPING%20SAFE%20ON%20SOCIAL%20MEDIA%20UOO152077-20.PDF.

46. U.S. Army, "Think. Type. Post." n.d, https://www.army.mil/socialmedia/personal/.

47. U.S. Department of the Navy, *Operations Security, NTTP 3-13.3* (Department of the Navy, 2022), https://www.navifor.usff.navy.mil/Portals/48/OPSEC/May%202023%20uploads/NTTP%203-13.3%20OPSEC%20(DEC%202022).pdf; U.S. Department of the Army, *Communication Strategy and Public Affairs Operations*, FM 3-61 (Department of the Army, 2022), https://www.iowanationalguard.com/wp-content/uploads/2022/04/FM_3-61-Communications-Strategy-and-Public-Affairs-Operations.pdf; U.S. Department of the Air Force, *Public Affairs*, AFDP 3-61 (Department of the Air Force, 2024), https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-61/3-61-AFDP-PUBLIC-AFFAIRS.pdf.

48. Center for Development of Security Excellence, *OPSEC Fundamentals for OPSEC Practitioners Course Student Guide.*

49. Sander van der Linden et al., "Prebunking Misinformation Techniques in Social Media Feeds: Results from an Instagram Field Study," *Harvard Kennedy School Misinformation Review,* January 22, 2026, https://misinforeview.hks.harvard.edu/article/prebunking-misinformation-techniques-in-social-media-feeds-results-from-an-instagram-field-study/.

50. Paul et al., *The Information Warfighter Exercise Wargame Rulebook* (RAND Corporation, 2021), https://www.rand.org/pubs/tools/TLA495-1.html.

51. "Home," DISARM Foundation, n.d., https://www.disarm.foundation/; "Home," MITRE, n.d., https://www.mitre.org/.

52. Joint Chiefs of Staff, *Public Affairs*, JP 36-1 (Joint Chiefs of Staff, 2016); Whiteside, "Narrative Manipulation, Malinfluence Operations, and Cognitive Warfare Through Large Language Model Poisoning with Adversarial Noise."

53. U.S. Air Force, *Information Warfare Doctrine*, 2023; van der Linden et al., "Prebunking Misinformation Techniques in Social Media Feeds."

54. Boeckl et al., *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*.

55. National Security Agency, *Limiting Location Data Exposure* (Department of War, 2020).

56. National Security Agency, *Keeping Safe on Social Media*.

57. Deputy Secretary of Defense to Chief Management Officer of the Department of Defense Secretaries of the Military Departments, Chairman of the Joint Chiefs of Staff, Under Secretaries of Defense, Chief of the National Guard Bureau, Commanders of the Combatant Commands, General Counsel of the Department of Defense, Director of Cost Assessment and Program Evaluation, Inspector General of the Department of Defense, Director of Operational Test and Evaluation, Chief Information Officer of the Department of Defense, Assistant Secretary of Defense for Legislative Affairs, Assistant to the Secretary of Defense for Public Affairs, Director of Net Assessment, Directors of Defense Agencies, Directors of DoD Field Activities, *Use of Geolocation-Capable Devices, Applications, and Services* (memorandum of understanding), August 3, 2018, https://media.defense.gov/2018/Aug/06/2001951064/-1/-1/1/GEOLOCATION-DEVICES-APPLICATIONS-SERVICES.PDF.

58. Office of the Director of National Intelligence, *Intelligence Community Policy Framework for Commercially Available Information*; "Privacy Framework," National Institute of Standards and Technology, accessed October 5, 2025, https://www.nist.gov/privacy-framework.

59. National Security Agency, *Limiting Location Data Exposure*; Office of the Director of National Intelligence, *Intelligence Community Policy Framework for Commercially Available Information.*

60. Huguet et al., *Media Literacy Standards to Counter Truth Decay,* RR-A112-12 (RAND, 2021), https://www.rand.org/pubs/research_reports/RRA112-12.html; Jennifer Kavanagh and Michael D. Rich, *Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life,* RR-2314-RC (RAND, 2018), https://www.rand.org/pubs/research_reports/RR2314.html.

61. Department of the Army, *FM 3-24*, 2014; John Boyd, "*Patterns of Conflict*," (PowerPoint presentation, Marine Corps University Amphibious Warfare School, Quantico, VA, January 1980), https://www.pogo.org/analyses/colonel-john-boyds-patterns-of-conflict-online.

62. Joint Chiefs of Staff, *Public Affairs*; U.S. Department of the Army, *Communication Strategy and Public Affairs Operations*; U.S. Department of the Air Force, *Public Affairs*.

63. *2024 SOLIC-SOCOM Joint Posture Statement*, 118th Cong. (2024) (statement of Christopher P. Maier, Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict and General Bryan P. Fenton, Commander of U.S. Special Operations Command); Joint Chiefs of Staff, *Military Intelligence Support Operations,* Joint Publication 3-13.2 (Joint Chiefs of Staff, 2014).

64. Kavanagh and Rich, *Truth Decay*; U.S. Department of the Air Force, *Public Affairs*.

65. Richards J. Heuer and Randolph H. Pherson, *Structured Analytic Techniques for Intelligence Analysis*, 2nd edition (CQ Press, 2014).

66. Office of the Director of National Intelligence, *Intelligence Community Policy Framework for Commercially Available Information.*

67. Joint Chiefs of Staff, *Joint Concept for Operating in the Information Environment (*Joint Chiefs of Staff, 2018).

68. Joint Chiefs of Staff, *Special Operations*, JP 3-05 (Joint Chiefs of Staff, 2018).

69. U.S. Department of the Air Force, *Information Operations*, AFDP 3-13 (Department of the Air Force, 2026), https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-13/3-13-AFDP-INFO-OPS.pdf.

70. U.S. Government Accountability Office, *Information Environment: DOD Operations Need Enhanced Leadership and Integration of Capabilities* (GAO-21-525T, 2021), https://www.gao.gov/products/gao-21-525t.

71. U.S. Department of Defense, *Counterintelligence Activities*, DoD Directive 5240.02 *(*Department of Defense, 2018), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/524002p.pdf;
U.S. Department of Defense, *Counterintelligence Awareness and Reporting (CIAR)*, DoD Directive 5240.06 *(*Department of Defense, 2011), https://www.scribd.com/document/73411112/DODD-5240-06-Counterintelligence-Awareness-and-Reporting-CIAR.

72. Maier and Fenton, *2024 SOLIC-SOCOM Joint Posture Statement;* U.S. Government Accountability Office, *Information Environment: DOD Needs to Address Security Risks of Publicly Accessible Information* (GAO-26-107492, 2025), https://www.gao.gov/products/gao-26-107492.

73. U.S. Department of the Air Force, *Information Operations*; Joint Chiefs of Staff, *Joint Concept for Operating in the Information Environment.*

74. Office of the Director of National Intelligence, *Intelligence Community Policy Framework for Commercially Available Information.*

75. Joint Chiefs of Staff, *Joint Concept for Operating in the Informative Environment,* (Joint Chiefs of Staff, 2018), https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf.

76. U.S. Government Accountability Office, *Information Environment.*

77. Gundars Bergmanis-Korats, Tetiana Haiduchyk, and Artur Shevtsov, *AI in Precision Persuasion. Unveiling Tactics and Risks on Social Media* (NATO Strategic Communications Centre of Excellence, 2024), https://stratcomcoe.org/publications/ai-in-precision-persuasion-unveiling-tactics-and-risks-on-social-media/309.

78. Boyd, It's Complicated; Zuboff, The Age of Surveillance Capitalism.

79. Rid, Active Measures; Whiteside, "Narrative Manipulation, Malinfluence Operations, and Cognitive Warfare Through Large Language Model Poisoning with Adversarial Noise."

80. Office of the Director of National Intelligence, *Intelligence Community Policy Framework for Commercially Available Information*; Gundars Bergmanis-Korats, Tetiana Haiduchyk, and Artur Shevtsov, *AI in Precision Persuasion. Unveiling Tactics and Risks on Social Media*.

81. Office of the Director of National Intelligence, *Intelligence Community Policy Framework for Commercially Available Information.*

82. Robert Chesney and Danielle Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security;" Federal Trade Commission, *Data Brokers*; Brill, "Demanding Transparency from Data Brokers;" Jon Roozenbeek et al., "Psychological Inoculation Improves Resilience Against Misinformation Across Cultures," *Science Advances* 8, no. 34 (2022), https://doi.org/10.1126/sciadv.abo6254.

83. Maier and Fenton, *2024 SOLIC-SOCOM Joint Posture Statement*; Office of the Director of National Intelligence, *Intelligence Community Policy Framework for Commercially Available Information.*

Chapter 5

Next Generation Intelligence, Surveillance, and Reconnaissance

AI and machine learning (ML) are rapidly transforming how organizations understand complex environments, make decisions, and generate operational advantage. For SOF, the ability to analyze vast volumes of data, identify hidden relationships, and anticipate emerging trends offers the potential to accelerate decision-making and improve mission effectiveness.

The paper in this section examines how SOF can leverage AI and machine learning to process large and diverse datasets, uncover meaningful patterns, and support predictive analysis for operational and strategic decision-making. Particular attention is given to the ways AI may redefine civil affairs by enhancing stakeholder engagement; improving understanding of human and social dynamics; and enabling more targeted and adaptive approaches to influence, governance, and stability operations.

Digital Shadows in the Human Domain: How Augmented Reality and AI Could Redefine Civil Affairs

By 1st Sgt. Nathan Greene

The Fog That Thinks Back

Kaohsiung, Taiwan. The air smells of diesel and static. Sirens echo down the narrow streets as columns of smoke twist skyward from the port district. A civil affairs (CA) team crouches on the second floor of a school repurposed as a humanitarian coordination node. The operator's lens projects a translucent overlay, evacuation routes highlighted in blue, civilian clusters in orange, and partner force checkpoints pulsing faintly on the periphery. AI summaries scroll across the display: Power grid damage, 43 percent. Casualties unverified. Disinformation trending: "U.S. forces abandoned southern Taiwan."

The team Leader steadies his breathing, toggling between English, Mandarin, and map symbols. Communications with the joint task force (JTF) pulse intermittently through a low-bandwidth mesh network, each packet of information competing with jamming and interference. Behind the augmented layer of data are frightened families, Taiwanese emergency volunteers, and local officials trying to hold together civil order as People's Liberation Army amphibious landings intensify along the western shore. Every decision made by the CA team will have a ripple effect on the information environment, shaping perceptions and survival.

This is not science fiction. It is a projection of where tomorrow's human domain fights will occur, where information, trust, and legitimacy move as fast as data. CA operators, once focused on face-to-face engagement and reconstruction, now stand at the intersection of influence and technology. Their ability to synchronize humanitarian aid, counter disinformation, and preserve partner trust will depend on mastering a battlespace where visibility and veracity collapse under pressure.[1]

Augmented reality (AR) and AI offer tools to bring order to that chaos. Yet these technologies also carry risk: cognitive overload,



Civil affairs team leader using AR interface during urban humanitarian operations in Southeast Asia. Source: Author-generated image using GPT 5.1

overreliance on automation, and the erosion of human judgment that defines effective CA work. Understanding how AR and AI could enhance or distort CA operations is no longer theoretical; it is essential preparation for the next war in the Indo-Pacific and beyond.

The New Front Line: The Human Domain Under Fire

The first salvos of a modern conflict will not be artillery or missiles. They will be information, confusion, and disbelief. In the opening hours of an invasion of Taiwan, satellite images and social media posts will flood the digital space with contradictory narratives. False reports will claim entire units have surrendered, while deepfake videos will show Taiwanese officials announcing capitulation. Within minutes, the CA team in Kaohsiung will become both operator and observer, caught in the turbulence of a human domain under direct assault.[2]

CA professionals have continuously operated at the intersection of the military, government, and population. In past decades, that line was physical: a village chief, a mayor, or a local reconstruction council. Today, it is digital, persistent, and contested. Every engagement, message, and aid delivery competes with automated disinformation networks and adversary psychological campaigns designed to fracture trust. In this environment, the human domain is no longer a backdrop to conflict; it is the decisive terrain.[3]

AR and AI hold the potential to reshape this landscape by enhancing awareness and speeding coordination. A properly configured AR display could provide operators with real-time overlays of population movements, key infrastructure status, and the emotional tone of crowds based on aggregated reporting. AI-driven systems can flag anomalies, detect influence campaigns, and highlight emerging needs before they escalate into crises. These technologies, when grounded in ethical design and doctrine, could help CA teams maintain order amid chaos, ensuring the correct information reaches the right hands in time to make a difference.

However, technology alone cannot secure legitimacy. CA operations rely on human relationships that can take months or years to develop. Trust cannot be automated. If AR and AI are to enhance the effectiveness of CA, they must serve as aids to empathy and precision, not replacements for them. The risk lies in believing that data alone captures the complexity of a community's will, fear, and resilience. Operators must remember that the essence of CA remains human connection, even when mediated through digital lenses.[4]

The Taiwan scenario reveals that success in the next conflict will not hinge solely on superior firepower but on superior understanding of people, networks, and perceptions. CA teams that can harness technology without losing their human touch will become the

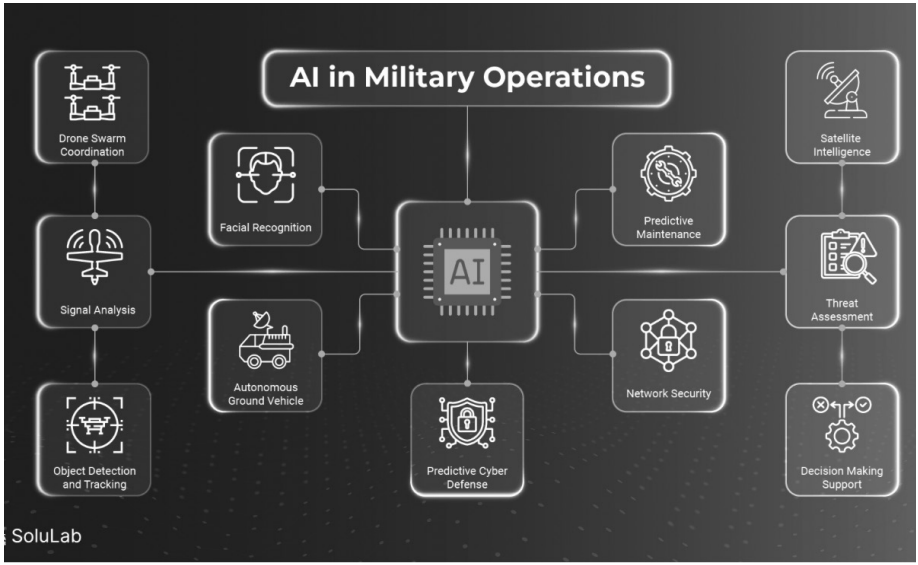


Figure 1. Diagram showing AI's potential in military operations. Source: SoluLab

connective tissue of the joint force. Their actions will bridge combat and stabilization, synchronize influence with humanitarian response, and help turn tactical engagements into strategic legitimacy.

Digital Shadows: Augmented Reality, AI, and Decision Superiority

Doctrine recognizes that information and understanding are decisive elements of modern warfare. Joint Publication (JP) 3-0 defines information as a warfighting function that directly influences decision superiority, while the U.S. Department of the Army Field Manual (FM) 3-05 *Special Operations* emphasizes the human domain as the decisive space where influence, legitimacy, and perception intersect. Within that framework, CA is uniquely positioned to translate tactical presence into strategic advantage.[5]

In a high-intensity environment such as Taiwan, the speed and precision of CA reporting can determine whether commanders act on fact or misinformation. U.S. Department of the Army Field Manual (FM) 3-57 *Civil Affairs Operations* (2021) current doctrine describes CA as the integrator of civil information, responsible for collecting, analyzing, and disseminating data that enables both lethal and non-lethal effects.[6] AR and AI directly support this mandate by improving how that information is gathered, visualized, and shared.

Augmented Reality as an Enabler of Situational Understanding

The U.S. Army's Integrated Visual Augmentation System (IVAS) has already demonstrated that heads-up displays can fuse navigation, communication, and sensor data into a single operational picture. Although IVAS was designed for close-combat forces, its architecture provides a model for CA applications. A lightweight variant could allow operators to see live overlays of essential services, population density, and partner assets. In doctrine, this aligns with the Civil Knowledge Integration (CKI) process: collect, analyze, and distribute. The difference is speed. What once took hours of manual plotting could occur instantly, reducing cognitive load and improving coordination with maneuver elements.[7]

Case studies from the IVAS program's campaign of learning show measurable improvements in reaction time and accuracy when soldiers operated with fused visual data. CA could leverage those same benefits for humanitarian coordination, using AR to identify evacuation corridors, medical aid points, or critical infrastructure under strain. The capability would allow CA teams to synchronize efforts with host-nation ministries and nongovernmental partners even when communications are degraded.[8]

AI as the Engine of Decision Superiority

AI complements AR by turning raw data into actionable insight. During humanitarian crises or stability operations, AI can classify damage imagery, flag anomalies in population behavior, or detect disinformation narratives spreading through local networks. This supports the Special Operations Hard Problem of Mission Assured Communications by ensuring that critical information reaches decision-makers even when human analysts are overwhelmed (see Fig 1).[9]

The Assessing Revolutionary and Insurgent Strategies (ARIS) series provides historical context for why this matters. ARIS research highlights that insurgent and resistance movements often exploit informational asymmetry rather than material superiority. In Taiwan, the People's Republic of China (PRC) would likely attempt to saturate the information environment with contradictory messaging.[10] An AI-assisted system trained on local language patterns could help CA identify emerging narratives and coordinate counter-messaging with PSYOP counterparts before misinformation undermines public trust.

Ethical and Operational Integration

Doctrine warns against overreliance on automation. U.S. Department of the Army Field Manual 6-22 on leadership underscores that technology cannot replace judgment, empathy, or moral reasoning. The integration of AR and AI into CA must therefore be governed by clear policy. Operators should utilize technology to enhance situational understanding, rather than making determinations about human intent or allegiance. Ethical oversight, data classification controls, and partner nation consent remain essential to preserving legitimacy.[11]

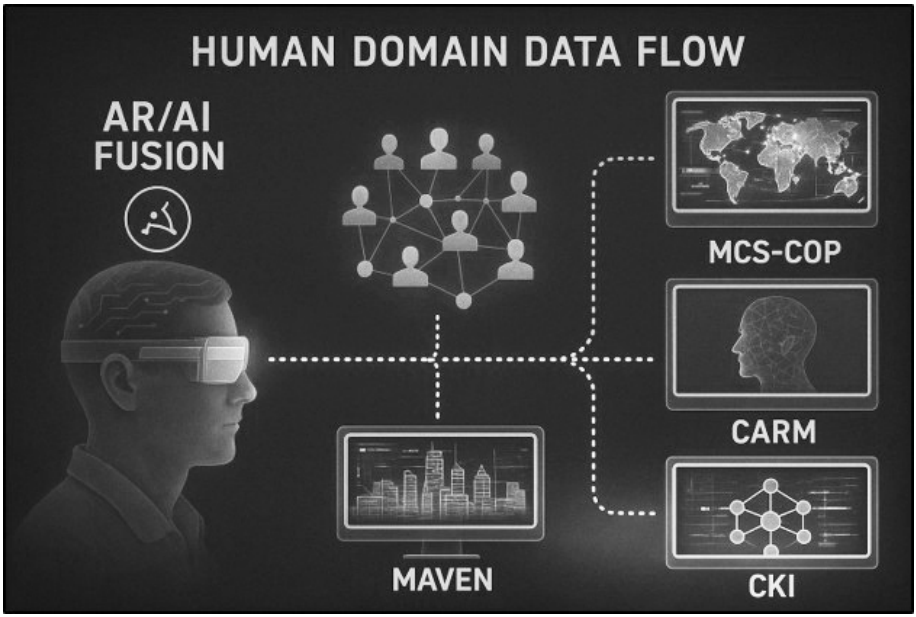


Figure 2. Conceptual illustration of "Human Domain Data Flow," showing augmented reality-AI fusion supporting CARM and Civil Knowledge Integration, while feeding MCS-COP, and Maven. Source: Author-supplied image generated by GPT 5.1

Special operations initiatives on small-unit dominance emphasize adaptability at the team level.[12] CA teams equipped with AR-AI tools could achieve this dominance not through firepower but through clarity, seeing patterns in chaos, and acting faster than adversaries can adapt. By institutionalizing digital literacy and human-machine teaming in doctrine and training, the force can ensure these tools remain servants of strategy rather than its drivers.

Civil Affairs at the Edge of Technology and Trust

CA operators have long worked in the gray space between stability and chaos, where decisions made in minutes shape perceptions for years. The rise of great power competition, especially in the Indo-Pacific, has exposed a recurring vulnerability in

that region: the inability to collect, share, and act on civil information quickly enough. Across real-world missions and training exercises, CA teams have demonstrated exceptional adaptability; however, their tools and networks have not kept pace with the environment in which they operate.

Operation Tomodachi: When Speed Meets Friction

In 2011, U.S. forces responded to Japan's catastrophic earthquake and tsunami in Operation Tomodachi. CA elements quickly established partnerships with the Japan Self-Defense Forces and local leaders; however, the operation revealed a critical problem: a fragmented information flow. Digital mapping systems, assessment spreadsheets, and reporting channels varied across agencies, forcing teams to spend hours reconciling data before taking action.[13]

An augmented overlay that displayed verified infrastructure damage, population displacement, and logistics status could have accelerated the response by visualizing what every stakeholder saw differently. AI could have filtered redundant reports and prioritized high-need areas, allowing teams to allocate engineers and medical support in near real-time. The gap was not in capability but in integration. CA teams needed a shared picture that could evolve as fast as the crisis.

Exercise Balikatan: Coalition Barriers in the Human Domain

During recent iterations of Exercise Balikatan in the Philippines, U.S. and partner-nation CA operators rehearsed disaster-relief and security cooperation missions in contested communications environments. Despite high proficiency and trust between forces, interoperability remained a persistent barrier. Each nation used different software for mapping and logistics. Even when data could

be shared, differences in language, classification, and network access created friction.[14]

AR systems designed for multinational use could overcome this by projecting coalition-releasable overlays that synchronize routes, resource points, and communication windows without requiring a stable internet connection. AI-enabled translation could render key mission prompts in both English and Tagalog, reducing miscommunication. These are not futuristic solutions; they are extensions of existing technology adapted to the human domain.

Ukraine and the Contest for Legitimacy

The war in Ukraine offers another lesson in the limits of traditional situational awareness. Civilian infrastructure, humanitarian corridors, and public sentiment have become decisive factors in the conflict. Disinformation spreads faster than ground truth, creating both tactical and moral hazards. CA-like functions performed by local defense organizations have struggled to distinguish legitimate humanitarian activity from adversary manipulation.

For U.S. and partner CA teams, this underscores a critical capability gap: the need to visualize legitimacy as clearly as terrain. AR-enabled systems could mark verified humanitarian sites, displaced populations, and friendly aid convoys, helping commanders and partners make informed decisions without compromising civilian safety. AI could detect false reporting before it spreads, protecting both lives and narrative advantage.

Bridging the Gaps

Across these operations, the pattern is consistent. CA operators possess the cultural knowledge, leadership, and initiative to succeed, but they lack the digital infrastructure to keep pace with their mission tempo. Current systems are often fragmented,



Ukrainians crowd under a destroyed bridge as they try to flee crossing the Irpin river in the outskirts of Kyiv, Ukraine, Saturday, March 5, 2022. (Photo: Associated Press)

overly classified, or incompatible with partner networks. AR and AI integration could transform that landscape by providing a visual, adaptive, and shareable interface that aligns with CA doctrine to understand, engage, and influence.

The human domain cannot be reduced to code, but it can be clarified with better tools. The next evolution of CA is not about replacing human judgment; it is about giving operators a clearer picture of the world they already understand (see Fig. 2).

Joint SOF Integration in Crisis

No CA mission exists in isolation. Every engagement, assessment, or stability effort depends on the synchronization of the broader special operations enterprise. The modern battlefield demands unity of action among CA, PSYOP, and Special Forces (SF), supported by intelligence, logistics, and aviation elements. Each contributes a unique piece of the human domain puzzle, yet their effectiveness often hinges on how quickly and accurately they can share context.

The Fragmented Reality of the Joint Environment

Joint doctrine envisions seamless integration across SOF components, but in practice, information friction persists. CA teams may gather valuable local insights, PSYOP elements may monitor sentiment and narratives, and SF detachments may conduct security cooperation with host-nation units. However, these efforts frequently operate on separate systems with limited interoperability. Data from a CKI report might never reach a PSYOP planner who could use it to counter emerging propaganda or an SF team conducting key leader engagements in the same area.[15]

AR and AI integration could close these seams by creating a unified operational layer that allows all SOF elements to visualize the same environment through their respective lenses. A CA operator might see population sentiment and infrastructure overlays, a PSYOP planner might see trending narratives and information pathways, and a SF detachment might see security status and partner readiness, all connected through a single, synchronized data model.

Indo-Pacific Joint Operations: The Balikatan Example

Exercises across the Indo-Pacific, such as Balikatan in the Philippines, already demonstrate both the progress and the challenges of joint integration. During recent iterations, CA, PSYOP, and SF teams executed combined humanitarian response missions alongside the Armed Forces of the Philippines. Each component contributed critical capabilities: CA coordinated civilian relief, PSYOP managed public messaging, and SF ensured security and logistics. Yet, coordination still relied heavily on verbal updates and fragmented reporting tools.[16]

If AR-AI systems had been integrated, the JTF could have visualized all operations in real time. PSYOP could have overlaid narrative sentiment data on maps of humanitarian

distribution points, allowing CA to adapt outreach strategies before misinformation spread. SF could have accessed updated infrastructure overlays to secure key supply routes without waiting for radio confirmation. The result would have been a faster, more adaptive, and more credible joint effort.

Crisis Application: Taiwan as a Joint SOF Testbed

In a Taiwan contingency, these integration gaps could carry strategic consequences. A CA team might identify displaced populations and critical infrastructure under threat, PSYOP units might need to counter PRC disinformation claiming civilian casualties, and SF detachments might be coordinating local defense support. Without an integrated digital framework, these efforts risk duplication, contradiction, or delayed response.

An AR-AI-enabled environment could connect these threads. CA overlays could feed into PSYOP sentiment dashboards, which in turn inform SF route planning and engagement priorities. A shared platform would allow commanders to align influence, stability, and security effects within a single operational picture, thereby achieving decision superiority across the spectrum of operations.[17]

Toward the Future Force

Special operations modernization efforts highlight the need for convergence across functional areas. Hard Problems, such as Mission Assured Communications and Small Unit Dominance, are not just about equipment but about cognitive speed, the ability of teams to sense, decide, and act faster than the adversary. CA, PSYOP, and SF all depend on that speed. [18]

AR and AI integration can provide the connective tissue for this convergence. It can transform the joint special operations environment from a collection of capable but separate units

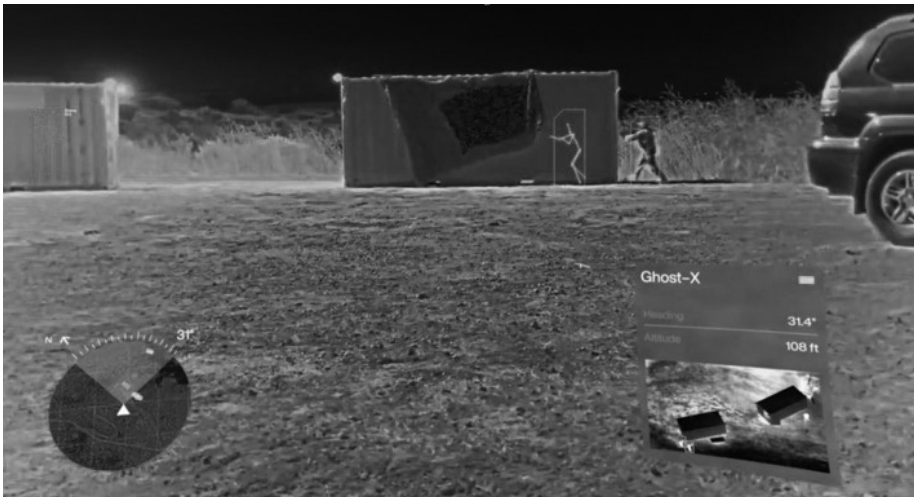


Figure 3. Real-world point-of-view using Anduril Eagle Eye in an online demonstration. Source: Anduril

into a digitally linked network that sees the human domain as one continuous battlespace (see Fig. 3). The future force will not be defined by who collects the most data but by who can interpret it first, act on it ethically, and share it across the enterprise without friction.[19]

Lessons for the Next Fight

Institutionalizing Human-Machine Teaming Through Doctrine

Special operations should codify the use of AR and AI within joint special operations doctrine, focusing on CKI information operations and interagency coordination. Future revisions of *Special Operations* FM 3-05 and *Civil Military Operations* JP 3-57 should define how AR-AI systems support CA, PSYOP, and SF at the tactical level while reinforcing human decision authority.[20]

Doctrine must emphasize that these technologies do not replace judgment or interpersonal engagement. Instead, they expand the operator's capacity to perceive, prioritize, and communicate in the human domain. Every new capability should include doctrinal language requiring ethical data handling, coalition-releasable frameworks, and adherence to host-nation consent.[21]

Training the Army Special Operations Forces Operator for Digital Fluency

Technology adoption fails when operators receive hardware without context. Special operations should integrate digital literacy and cognitive load management into the education pipeline to enhance operational effectiveness. Courses at the John F. Kennedy Special Warfare Center and School, including the PSYOP qualification course and SOF language and culture programs, should incorporate AR-AI familiarization, practical decision-making under augmented conditions, and ethical scenario training.[22]

CA operators in particular need immersive simulations that replicate the complexity of operating with digital overlays during humanitarian crises or partner engagements. Similar to marksmanship or medical lanes, units should conduct augmented lanes in which operators practice using visual data while maintaining rapport and situational awareness.

Leadership Development for Ethical and Cognitive Adaptation

Leaders must learn to interpret data without becoming dependent on it. Leadership courses should include modules on human-machine trust, algorithmic bias, and ethical command decisions. Commanders should understand when to rely on AR-AI recommendations and when to defer to human intuition. [23]

Special operations can draw from civilian models in medicine and aviation, where augmented decision aids are common, but ultimate accountability remains with the human professional. Embedding this mindset early will prevent future generations of operators from confusing technological clarity with certainty.

Experimentation and Rapid Prototyping Through SOF AT&L

SOF Acquisition, Technology, and Logistics already provides a mechanism for bottom-up innovation. The enterprise should expand its collaboration with the operator community through pilot programs that test AR-AI prototypes in live training environments such as Balikatan, Rim of the Pacific, and Freedom Shield.[24]

CA teams can serve as the ideal user base for experimentation because their missions span both combat and stability environments. Field data from these pilots can refine user interfaces, translation algorithms, and interoperability features before they are scaled enterprise wide. Each prototype cycle should include a joint user group, coalition participation, and ethics and legal oversight from the onset of the design process.[25]

Integration Into the SOF Hard Problems Framework

AR and AI integration directly address multiple Hard Problems: Mission Assured Communications by enabling low-bandwidth data visualization and messaging even in denied environments; Small Unit Dominance by enhancing perception, coordination, and decision speed without adding manpower; and Signature Management by reducing the need for large command posts or constant transmissions through visual tasking and store-and-forward systems. [26]

The enterprise should treat AR-AI adoption not as a stand-alone technology initiative but as a cross-cutting enabler that supports every modernization line of effort.[27]

The Human Domain as the End State

Ultimately, technology must reinforce what has always defined success: human connection, adaptability, and credibility. Training and doctrine should make clear that AR and AI are extensions of those values, not replacements for them. When properly integrated, they can enhance transparency with partners, improve civilian safety, and provide leaders with a faster, more precise picture of a complex world.[28]

The next conflict will not grant time for experimentation. The enterprise must act now to prepare its operators for a future in which information moves faster than intention can form. By building doctrine, training, and leadership around ethical human-machine collaboration, special operations can ensure that, in the most contested environments, the advantage remains with the people who understand them best (see Fig. 4).[29]

The Way Forward

The next fight will not begin with a clear line of battle. It will emerge in crowded cities, contested networks, and the blurred intersections of truth and perception. For CA and the broader special operations community, the first step toward dominance in that environment is not a new weapon but a new way of seeing.

AR and AI offer that vision. When integrated across CA, PSYOP, and SF, these tools can transform how the joint force perceives the human domain. They can shorten decision cycles, reveal hidden patterns, and give commanders and operators the clarity they need

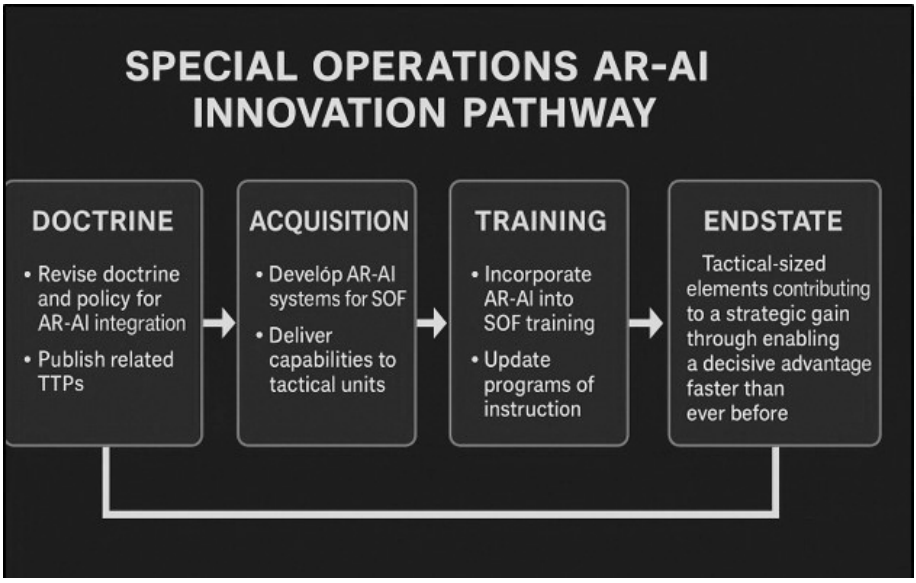


Figure 4. Special operations innovation pathway illustrating doctrinal, training, and acquisition integration for augmented-AI adoption within special operations forces. Source: Author-generated image using GPT 5.1

to act with precision and legitimacy. Yet, the value of these systems will depend entirely on how they are taught, led, and governed. [30]

Special operations' advantage has never been technological alone. It has always been human. The skill, empathy, and adaptability of its operators remain the decisive edge. AR and AI can enhance those qualities by filtering noise, improving coordination, and protecting relationships built on trust. The danger lies not in the technology itself but in failing to adapt to it before adversaries do.

CA stands at the center of this transition. The mission to understand, engage, and influence populations demands both data and discernment. With proper integration, AR and AI will not replace the CA operator; they will empower them to be faster, safer, and more effective in an increasingly complex world.

The way forward is disciplined innovation, guided by technology that is informed by ethics, doctrine, and human purpose. By institutionalizing digital fluency, cross-functional experimentation, and doctrinal clarity, special operations can ensure that, in the next conflict, its operators not only fight in the fog of war but also see through it.[31]

About the Author

First Sergeant Nathan Greene holds a bachelor of science in organizational leadership and is pursuing a master of business administration from the University of Charleston. Greene is a Joint Special Operations University graduate with honors in enterprise management and has completed multiple advanced SOF courses. His operational experience includes three deployments with CA teams and a partner force capacity-building deployment spanning five countries across the Indo-Pacific theater.

Notes

1. Joint Chiefs of Staff, *Joint Operations*, Joint Publication (JP) 3-0 (Department of Defense, 2024); U.S. Department of the Army, https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series/; *Special Operations*, Field Manual (FM) 3-05 (Department of the Army, 2025).
2. Joint Chiefs of Staff, *Joint Operations*; U.S. Department of the Army, *Special Operations*.
3. U.S. Department of the Army, *Developing Leaders*, Field Manual (FM) 6-22 (Department of the Army, 2020).
4. U.S. Department of the Army "Army Accepts Prototypes of the Most Advanced Version of IVAS," Army.mil, August 1, 2023, https://www.army.mil/article/268759/army_accepts_prototypes_of_the_most_advanced_version_of_ivas.
5. Joint Chiefs of Staff, *Joint Operations*; Department of the Army, *Special Operations*.
6. Joint Chiefs of Staff, *Civil-Military Operations*, Joint Publication (JP) 3-57 (Department of Defense, 2018); U.S. Department of the Army, *Special Operations*.
7. Congressional Research Service, *The Army's Integrated Visual Augmentation System (IVAS): Background and Issues for Congress*, CRS Report (Library of Congress, CRS, September 11, 2025), https://www.congress.gov/crs_external_products/IF/PDF/IF13022/IF13022.2.pdf.
8. Assessing Revolutionary and Insurgent Strategies (ARIS) Project, *Undergrounds in Insurgent, Revolutionary, and Resistance Warfare*, 2nd ed. (U.S. Army Special Operations Command, 2013), https://info.publicintelligence.net/USASOC-ARIS-Undergrounds.pdf.
9. Takeshi Ise et al., "Information Linkage by SIP4D: Real-Time Data Sharing During Disaster Response," *Journal of Disaster Research* 17, no. 6 (2022): 755–68, https://doi.org/10.20965/jdr.2022.p0755; U.S. Special Operations Command, *SOF Hard Problems Framework* (U.S. Special Operations Command, 2025).
10. ARIS Project, *Undergrounds in Insurgent, Revolutionary, and Resistance Warfare*; U.S. Special Operations Command, *SOF Hard Problems Framework*.
11. U.S. Department of the Army, *Developing Leaders*.
12. U.S. Special Operations Command, *SOF Areas of Interest* (Office of Acquisition, Technology, and Logistics, U.S. Special Operations Command, 2025).
13. U.S. Agency for International Development (USAID), *Operation Tomodachi: Lessons from Japan's Earthquake and Tsunami Response* (USAID, 2012).
14. U.S. Indo-Pacific Command, *Exercise Balikatan 2023 After-Action Summary* (U.S. Indo-Pacific Command, 2023); U.S. Special Operations Command, *USSOCOM Strategy 2030: Empowering People, Sustaining Advantage* (U.S. Special Operations Command, 2023).
15. Hiroshi Nishiyama, "Disaster Relief Activities of the Japan Self-Defense Force," *Journal of Disaster Medicine* 28, no. 4 (2014): 194–98. https://doi.org/10.1017/dmp.2014.46

16. U.S. Indo-Pacific Command, *Exercise Balikatan 2023*; United States Special Operations Command, *USSOCOM Strategy 2030*.
17. Nishiyama, "Disaster Relief Activities."
18. U.S. Special Operations Command, *SOF Hard Problems Framework*.
19. Nishiyama, "Disaster Relief Activities."
20. U.S. Department of the Army, *Special Operations*; Joint Chiefs of Staff, *Civil-Military Operations*.
21. U.S. Department of the Army, *Developing Leaders*.
22. U.S. Army John F. Kennedy Special Warfare Center and School, *Civil Affairs Operations Course Handbook* (U.S. Army John F. Kennedy Special Warfare Center and School, 2024).
23. U.S. Department of the Army, *Developing Leaders*.
24. U.S. Special Operations Command, *SOF Hard Problems Framework*.
25. U.S. Special Operations Command, Office of SOF Acquisition, Technology & Logistics, "Rapid Prototyping for SOF Operators" (fact sheet, United States Special Operations Command, 2025).
26. U.S. Special Operations Command, Office of SOF Acquisition, Technology & Logistics, "Rapid Prototyping."
27. U.S. Special Operations Command Office of SOF Acquisition, Technology & Logistics, "Rapid Prototyping for SOF Operators"; U.S. Special Operations Command, *SOF Areas of Interest*.
28. U.S. Special Operations Command, Office of SOF Acquisition, Technology & Logistics, "Rapid Prototyping."
29. U.S. Special Operations Command, Office of SOF Acquisition, Technology & Logistics,"Rapid Prototyping."
30. ARIS Project, *Undergrounds in Insurgent, Revolutionary, and Resistance Warfare*.
31. Nishiyama, "Disaster Relief Activities."

2027 CALL FOR SPECIAL OPERATIONS PAPERS

MODERN WARFARE

JSOU's Call for Special Operations Papers program encourages those in the SOF enterprise to research and write short, impactful papers that promote discourse, spark idea generation, and offer innovative solutions for SOF leaders and decision-makers. As the program evolves, so, too, do the topics.

The AY27 effort is focused on modern warfare and seeks submissions that examine ways SOF can integrate with the joint force to modernize for the future fight. Topics were derived from Commander's Decision Round Table after-action reviews and senior leader discussions, in coordination with the USSOCOM Doctrine and Lessons Learned team, to ensure relevance and alignment with the USSOCOM priorities of WIN, PEOPLE, and TRANSFORM.

This year, categories are not based on author type (active-duty, allies and partners, or academics); rather, the categories are the topics themselves. Papers will be judged against papers of the same topic, no matter the author's affiliation. Also new this year: Submissions can be written up to the SECRET level, allowing for broader depth of discussion and more targeted recommendations.

Categories and Questions

Category 1 *Targeting: The Role of SOF in Dynamic Targeting Networks*

1. What unique capabilities and advantages does SOF bring to the joint find, fix, track, target, engage, and assess (F2T2EA) cycle, and how can SOF maximize its contribution to deliberate and dynamic targeting in contested environments?

2. How can SOF develop resilient decentralized command, control, communications, computers, cyber, intelligence, surveillance, reconnaissance, and targeting (C5ISRT) architectures that enable sensing, targeting, and decision-making when communications and networks are denied, degraded, intermittent, or disrupted?

3. How can SOF balance the increasing power, connectivity, and signature requirements of advanced technologies with the need for low-signature, self-sustaining operations in anti-access/anti-denial (A2/AD) environments?

4. How should SOF integrate with and influence joint all-domain targeting networks to accelerate the transition from sensing to decision and action?

Category 2 *Joint Warfighting: SOF as Stand-in Forces: Advancing the Joint Warfighting Concept in Contested Environments*

1. How can joint SOF task forces best operationalize the integration of space, cyberspace, and electromagnetic spectrum (EMS) capabilities at the tactical edge to achieve decision advantage against peer adversaries?

2. How can SOF adapt its operational approaches across all core activities to effectively increase allied and partner defense burden-sharing in support of mutual security objectives?

3. How can SOF integrate with conventional maritime, air, land, and cyber forces?

4. What unique risks and opportunities does the SIF concept create for SOF, and what must change in SOF force design, training, education, authorities, and sustainment to make the concept viable?

Category 3 *Recruiting and Retention: Evaluating Recruitment Models for SOF*

1. How can the SOF enterprise recruit, develop, and retain personnel with the specialized technical expertise required to rapidly integrate, operate, and maintain transformative technologies in denied environments?

2. As SOF prioritizes the new competencies required for globally integrated, multi-domain joint force operations, what traditional training and education requirements or legacy skill sets should be de-prioritized or divested to optimize the force generation pipeline and preserve unit readiness?

3. How do different recruiting models affect attrition rates during selection and training and what lessons can be drawn from U.S. Army Special Forces, Navy SEALs, Marine Raiders, Air Force Special Warfare, and allied SOF organizations?

4. What attributes—not merely skills—will the future SOF operator require, and how should SOF selection, education, training, and career development evolve to develop them?

Category 4 *Autonomous Warfare: Autonomous Warfare and the Future of Special Operations*

1. How can SOF better leverage AI/machine learning, quantum computing, and autonomous systems in tactical, operational, strategic, and contested environments?

2. How can autonomous systems support stand-in forces, distributed operations, and joint warfighting concept objectives?

3. What lessons from current conflicts inform the future employment of autonomous systems?

4. How will SOF adjust its training and education to ensure its operators exploit technology rather than depend on it? How can we ensure human agility is enhanced by, rather than reliant on, technological superiority?

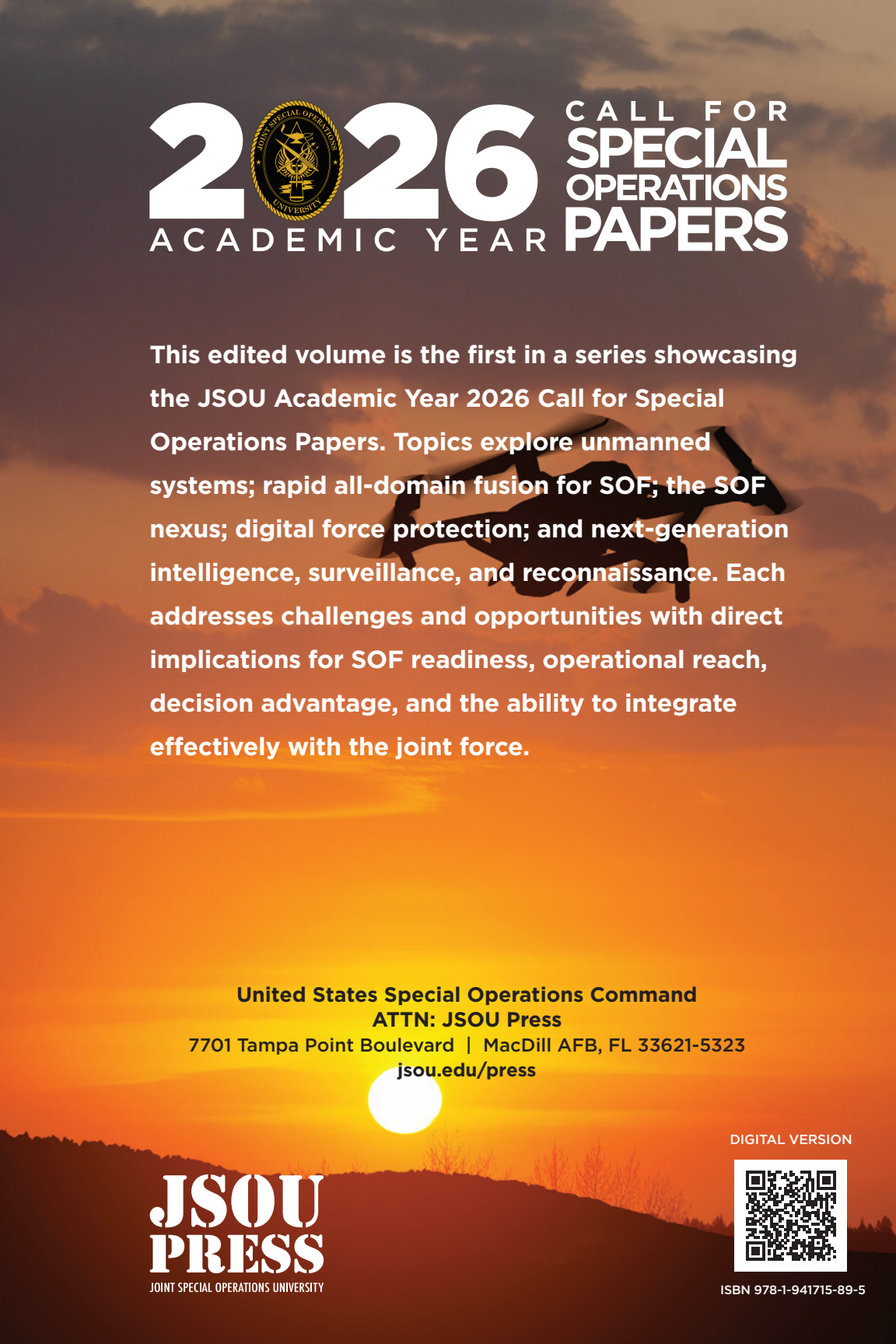
5. How can unconventional warfare models be adapted and applied to the modern battlefield?

Submissions are limited to 3,500 words or fewer. Papers will be evaluated by a panel of subject matter experts, and winning submissions will be recognized by the USSOCOM Commander and JSOU Press.

Submission deadline is March 1, 2027

Visit
https://www.jsou.edu/press/callforpapers
to learn more and submit.

2026 ACADEMIC YEAR CALL FOR SPECIAL OPERATIONS PAPERS



This edited volume is the first in a series showcasing the JSOU Academic Year 2026 Call for Special Operations Papers. Topics explore unmanned systems; rapid all-domain fusion for SOF; the SOF nexus; digital force protection; and next-generation intelligence, surveillance, and reconnaissance. Each addresses challenges and opportunities with direct implications for SOF readiness, operational reach, decision advantage, and the ability to integrate effectively with the joint force.

United States Special Operations Command
ATTN: JSOU Press
7701 Tampa Point Boulevard | MacDill AFB, FL 33621-5323
jsou.edu/press

JSOU PRESS
JOINT SPECIAL OPERATIONS UNIVERSITY

DIGITAL VERSION

ISBN 978-1-941715-89-5