Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

May 2026

Issue brief Information fires

Building C-C5ISRT advantage in competition

Martin Zuber, Caleb Eames, Daniel Minnocci, and Amy Cowley

Executive summary

Countering adversary command, control, communications, computers, cyber, intelligence, surveillance, reconnaissance, and targeting (C5ISRT) has emerged as a critical operational priority, underscored by Admiral Samuel Paparo's May 2025 congressional posture testimony and Admiral Daryl Caudle's 2026 US Navy Fighting Instructions. As the US military faces increasingly sophisticated adversaries who are constantly conducting hybrid warfare operations across all domains, countering C5ISRT (C-C5ISRT) during the competition phase (i.e., prior to engaging in conflict) is essential to gaining an advantage and deterring war.

The US military is at a critical tipping point. Success will depend on rapidly acquiring, integrating, training, and operationalizing C-C5ISRT capabilities before conflict begins. However, current doctrinal frameworks, organizational structures, and acquisition processes are not optimized for the requisite speed, integration, or scale to do so.

This paper offers a comprehensive set of recommendations for Congress, the Office of the Secretary of Defense, the Joint Staff, the military services, and the combatant commands. These recommendations focus on:

- Accelerating the transition to software-defined warfare.
- Aligning acquisition processes with operational timelines.
- Strengthening interagency and joint integration.
- Reforming training, doctrine, and organizational structures to enable the rapid deployment of C-C5ISRT capabilities.

Together, these recommendations will present a road map for the United States to deter adversaries in the competition phase, and to gain and retain a strategic advantage in information warfare.

Introduction

"Deterrence is our highest duty," Admiral Samuel Paparo, commander of US Indo-Pacific Command, declared in May 2025.[1] "Deterrence activities dominate the preponderance of what our forces do day-to-day around the world," Admiral Daryl Caudle, the thirty-fourth chief of naval operations, reaffirmed as he unveiled the US Navy Fighting Instructions at the AFCEA WEST 2026 in February.[2] This highest duty is challenged by an often-ambiguous era of competition that is no longer defined by military mass and capability overmatch, but rather by persistent "gray zone" actions by our adversaries: These are below the threshold of armed conflict, conducted through deniable C5ISRT activities that affect awareness, perceptions, will, and attitudes before a shot is fired.[3] Compounding this challenge is the fact that concepts like gray zone, C5ISRT, and information warfare remain poorly defined and debated.

1. "INDOPACOM Commander Underscores Importance of Land Forces, Deterrence, and AI in Indo-Pacific Security," US Army, May 14, 2025, https://www.army.mil/article/285494/indopacom_commander_underscores_importance_of_land_forces_deterrence_and_ai_in_indo_pacific_security.
2. "CNO Keynote Remarks at AFCEA WEST - as Prepared," US Navy, accessed April 17, 2026, https://www.navy.mil/Press-Office/Speeches/display-speech/Article/4406659/cno-keynote-remarks-at-afcea-west-as-prepared/. AFCEA is an information technology, communications, and electronics association for professionals in international government, industry, and academia worldwide; AFCEA West was held in San Diego, California.
3. C5ISRT stands for command, control, communications, computers, cyber, intelligence, surveillance, reconnaissance, and targeting.

On the one hand, due to US preeminence in conflict, our strategic adversaries have turned to asymmetric warfare in competition. The world is now marked by countless gray zone[4] operations such as VOLT TYPHOON, through which People's Republic of China (PRC) state-sponsored cyber actors are prepositioned on US networks to enable disruptive and destructive cyberattacks against US critical infrastructure, or Russia's continuous hybrid warfare campaign against Europe and the United States to sabotage critical infrastructure, sow disinformation, and probe NATO defenses.[5] Expansive internet accessibility, broad social media use, and the proliferation of camera-equipped smart devices have increased global interconnectedness, while the behaviors that constitute "warfare" in those connections have become less clear.

On the other hand, success in the West is often still measured as if we were in a kinetic conflict by measuring what we did, and not whether it produced the desired effect. The inability to measure the effectiveness of deterrence leads to ill-defined responses, costs taxpayer dollars through unoptimized force posture, and cedes information initiative to adversaries who operate on a wartime footing while we still treat competition as peacetime.

This paper asserts that the US military's ability to optimize the operations of scarce capital forces[6], integrate information, and effectively message intent will play a decisive role in influencing adversary decision-making and deterring war. It argues the joint force is not optimized to counter adversary C5ISRT during the competition phase[7] due to our limited ability to measure effectiveness, inefficient force posturing and employment, and insufficient technological integration, resulting in suboptimal use of resources and reduced influence over adversary decision-making. To be clear, much work has been done to enable our military to win kinetic conflict, and our adversaries should fear our ability to close with and destroy the enemy, but the cognitive and information battles of competition require different investments to counter C5ISRT. In Paparo's testimony before the House Armed Services Committee in April 2025, he recognized that "the Joint Force must build the link between desired information effects and physical Operations, Activities, and Investments (OAIs) to assure adversary cognition of US capability and will."[8] This paper examines how the joint force, with particular emphasis on the US Navy, can optimize C-C5ISRT capabilities *in the competition phase* to affect adversary will, awareness, perceptions, attitudes, emotions, and cognition to create and sustain a joint, allied, and partner advantage and freedom of action in and through the information environment.

The adversary: PLA information warfare

Understanding the urgency behind optimizing C-C5ISRT capabilities requires examining how the People's Liberation Army (PLA), among other adversaries, approaches information warfare not as a supporting function but the decisive precondition for *all* military action. The PLA categorizes the current stage of warfare as informatization, with the previous stage being mechanization, and the next one being intelligentization, where artificial intelligence (AI) will be the defining component.[9] According to the PLA's Academy of Military Sciences—which reports directly to the Central Military Commission—informatized warfare is characterized by "digital networks that enable modern precision-guided munitions, platforms, and Information Related Capabilities (IRCs) such as electronic and cyber warfare."[10] A RAND report indicates this form of warfare

4. Forward Defense Experts, "Today's Wars Are Fought in the 'Gray Zone.' Here's Everything You Need to Know About It.," Atlantic Council, December 22, 2022, https://www.atlanticcouncil.org/blogs/new-atlanticist/todays-wars-are-fought-in-the-gray-zone-heres-everything-you-need-to-know-about-it/.
5. "PRC State-sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," Cybersecurity and Infrastructure Security Agency, accessed April 17, 2026, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a; and Peter Dickinson, "Putin's Hybrid War against Europe Continues to Escalate," Atlantic Council, August 25, 2025, https://www.atlanticcouncil.org/blogs/ukrainealert/putins-hybrid-war-against-europe-continues-to-escalate/.
6. Capital forces in military assets refer to the accumulated, durable, and productive capacity of a defense establishment, including weapons, infrastructure, and technology that require strategic investment
7. Air Force, *Air Force Doctrine Publication 3-0, Operations*, January 22, 2025, https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-0/AFDP3-0Operations.pdf.
8. "Statement of Admiral Samuel J. Paparo, Commander, U.S. Indo-Pacific Command on U.S. Indo-Pacific Command Posture," 2025.
9. Josh Baughman, "The Path to China's Intelligentized Warfare: Converging on the Metaverse Battlefield," *Cyber Defense Review*, December 19, 2024, https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/4012231/the-path-to-chinas-intelligentized-warfare-converging-on-the-metaverse-battlefi/.
10. B. A. Friedman, "Finding the Right Model: The Joint Force, the People's Liberation Army, and Information Warfare," *Journal of Indo-Pacific Affairs* 6, no. 3 (March–April 2023): 1–17; and Andrew W. Marshall, "Finding the Right Model: The Joint Force, the People's Liberation Army, and Information Warfare," Air University (AU) website, accessed April 17, 2026, https://www.airuniversity.af.edu/JIPA/Display/Article/3371164/finding-the-right-model-the-joint-force-the-peoples-liberation-army-and-informa/.

"places a central and critical emphasis on information superiority."[11] The Academy of Military Sciences has asserted that winning the information war is "the fundamental function of our military, and it is also the basis for the ability to accomplish diversified military tasks."[12] For the PLA, the information war is not something that will begin when crisis or conflict eventually erupts. It is already underway and every military task, activity, and employment serves to advance the narrative of the Chinese Communist Party (CCP).

So how has this occurred in practice? Many insights can be drawn from the PLA's May and October 2024 military exercises around Taiwan.[13] These PLA drills were timed to occur with the inauguration and National Day speech of President Lai Ching-te. Additionally, a 2025 US Department of Defense (DOD) Annual Report to Congress on the Military and Security Development's Involving the PRC, highlighted the fact that the exercises coincided with a surge of "official accounts and proxy accounts impersonating Taiwan citizens to exaggerate the PLA's capabilities and spread disinformation narratives about US-Japan unwillingness to aid Taiwan's defense,"[14] which were disseminated across social media platforms. The military drills were not simply training and rehearsal, but a synchronized demonstration across all instruments of national power to flood the information space and to seed malign public sentiment against the United States and its allies.

The PRC is not alone in this approach. Russia also conducts a persistent campaign of malign information operations, cyber intrusions,[15] critical infrastructure sabotage, and territorial incursions across Europe and NATO territories.[16] Western militaries and governments discretely maintain traditional delineations of warfare as either conventional or unconventional, while adversaries have evolved to an inextricably "information-led"[17] hybrid and asymmetric view of modern warfare.

C-C5ISRT capabilities can enable the US military and its allies to combat this evolution throughout the competition continuum.[18] These capabilities target the web of networks adversaries depend upon most, from the sensors that detect US forces, the communications nodes and pathways that relay targeting data, the command posts that authorize operations, the sources of information adversary leaders rely on to make assessments, and perhaps most importantly, the cognitive processes that drive decision-making. For generations, every young US Marine has been taught that "fire without movement is a waste of ammo, and movement without fire is suicide." This combat truism must be updated for this new age of informatized warfare: Conventional fires without information maneuver are a waste of taxpayer dollars, and conventional maneuver without information fires is suicide.

The measurement challenge: Deterrence in competition

Measuring a kinetic effect in conflict is straightforward. Yet, unlike battle damage assessments, the ability to qualitatively measure the informational and cognitive effects that underpin deterrence remains elusive. Currently, deterrence is often evaluated through simple quantitative measures of performance, such as whether specific transit routes were navigated by US or allied ships in adversary-influenced littorals, or the number of exercises completed in a year near adversary-contested terrain. Consider a US ship transit of the Taiwan

11. Edmund J. Burke et al., *People's Liberation Army Operational Concepts*, Report, RAND Corporation, 2020, https://www.rand.org/pubs/research_reports/RRA394-1.html.
12. *In Their Own Words: Science of Military Strategy 2020*, trans. China Aerospace Studies Institute (Montgomery, Alabama: Air University, January 26, 2022), 337, https://www.airuniversity.af.edu/CASI/Display/Article/2913216/in-their-own-words-2020-science-of-military-strategy/; the *In Their Own Words* series provides translations of Chinese documents.
13. Amrita Jash, "China's Military Exercises around Taiwan: Trends and Patterns," Global Taiwan Institute, October 2, 2024, https://globaltaiwan.org/2024/10/chinas-military-exercises-around-taiwan-trends-and-patterns/.
14. "2025 Annual Report to Congress: Military and Security Developments Involving the People's Republic of China," Department of Defense, 2025, https://media.defense.gov/2025/Dec/23/2003849070/-1/-1/1/annual-report-to-congress-military-and-security-developments-involving-the-peoples-republic-of-china-2025.pdf.
15. Greg Otto, "Is the US Adopting the Gray Zone Cyber Playbook?," CyberScoop, January 12, 2026, https://cyberscoop.com/gray-zone-cyber-operations-state-power-below-threshold-conflict-op-ed/.
16. "Statement of Condemnation by the North Atlantic Council Concerning Russian Malicious Cyber Activities," NATO, July 18, 2025, https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/07/18/statement-of-condemnation-by-the-north-atlantic-council-concerning-russian-malicious-cyber-activities#:~:text=We%20strongly%20condemn%20Russia%27s%20malicious,which%20Russia%20claims%20to%20uphold.
17. Friedman, "Finding the Right Model," AU, April 24, 2023, https://www.airuniversity.af.edu/JIPA/Display/Article/3371164/finding-the-right-model-the-joint-force-the-peoples-liberation-army-and-informa/.
18. Air Force, *Air Force Doctrine Publication 3-0, Operations.*

Strait.[19] Does conducting this transit actually deter China from seeking reunification with Taiwan by force? Is this worth the real cost; measured in US dollars, Sailor Operational Tempo, and ship maintenance? Does the same operation encourage the average Filipino citizen to believe that the United States stands ready to ensure freedom of navigation in the South China Sea? Should this operation be timed to coincide with the annual CCP Plenum for greatest impact? Some research even suggests that US operations in and around Taiwan are inadvertently reinforcing Beijing's narrative of American encirclement, providing rationalization for PLA modernization and aggressive posturing.[20]

The gap between measuring performance and effectiveness manifests across the information enterprise. Public affairs teams can quickly quantify media production and interactions, such as views or likes, but rarely do those teams possess the tools to attribute that interaction to specific audiences or to gauge positive or negative shifts in response to it. Assessments to evaluate the reactions, sentiments, and behavioral changes surrounding those activities are often slow, fragmented across federal agencies, and compartmentalized. This leaves uncertainty about whether the joint force's action or message was perceived as intended by its target audience.

If success in competition means an adversary wakes up each morning and decides "today is not the day," warfighters must be able to assess whether yesterday's operations contributed to that decision. Commanders need analytical C-C5ISRT tools that provide a timely qualitative pulse of deterrence effectiveness to inform tomorrow's resourcing and force-posturing decisions. *Those tools already exist and are available today*. The United States' innovative technology sector and broad network of allies have produced digital capabilities that can better measure effectiveness, counter malign influence, and optimize operations in near real time. While authoritarian regimes are constrained by centralized decision-making and strict information control, open-market entrepreneurial innovation remains a systemic advantage, but only if the United States moves now to capitalize on it.

Tools providing timely qualitative deterrence measurement utilize advanced computing technologies, most notably AI and machine learning (ML), and they are fundamentally altering the character of the competition continuum. Central to today's computing revolution is the scaling of neural networks, particularly large language models (LLMs) that aggregate and process vast amounts of data at speeds impossible by human analysts alone. AI will not replace humans, but it will make them more efficient and enable clearer insight into target perception, influence drivers, and decision-making to maximize operational effects. AI/ML models can provide tailored and contextualized assessments that have historically relied on teams of humans to synthesize language proficiency, regional expertise, cultural knowledge, and advanced psychological, sociological, or social interpretation of the cognitive and behavioral impacts of operations in the information environment (OIE). This enhanced understanding could enable earlier intervention in adversary decision cycles, which strengthens deterrence, reduces the likelihood of conflict, or shapes an advantage during escalation. The challenge lies in harnessing these capabilities faster and more effectively than our adversaries.

Doctrinal and organizational inefficiencies

Technology alone cannot solve the measurement challenge. Even the most sophisticated AI tools require the right organizational structures, trained personnel, and operational concepts to employ them effectively. Before examining where C-C5ISRT capabilities should reside organizationally, it's essential to define what C-C5ISRT encompasses, how it nests within OIE, and how the services have approached associated concepts to this point. At its core, deterrence is the combination of capability, credibility, and communication.[21] Understanding how external actors in a specific region perceive the joint force's action is essential. Linking information effects with physical OAIs is one part of a broad category of OIE, which are defined as "military action involving the integrated employment of multiple forces to affect drivers of behavior by informing audiences; influencing foreign relevant actors; attacking and exploiting relevant actor information, information networks, and information systems; and protecting friendly information, infor-

19. Aaron-Mathew Lariosa, "Updated: U.S. Destroyer, Survey Vessel Transit Taiwan Strait," USNI News, US Naval Institute, January 17, 2026, https://news.usni.org/2026/01/17/u-s-destroyer-survey-vessel-conduct-first-taiwan-strait-transit-of-2026-say-chinese-officials.
20. Scott Fisher et al., "China, Dime, and Innovative Deterrence Methodology: How Authoritarian States React to Deterrence Activities through Information," *European Journal of International Security*, Cambridge Core, November 25, 2025, https://www.cambridge.org/core/journals/european-journal-of-international-security/article/china-dime-and-innovative-deterrence-methodology-how-authoritarian-states-react-to-deterrence-activities-through-information/131F93C80CA72E9B926F1D5DB5B3947D.
21. Andrea Grillo, "Decoding Deterrence: The Essentials of the Art of Persuasion," Deep InSecurity, January 24, 2025, https://www.deepinsecurity.com/decoding-deterrence/.

An illustration of a US Navy watchfloor. Graphic by Petty Officer 2nd Class William Sykes/US Navy graphic by Oliver Elijah Wood.

mation networks, and information systems."[22] Such operations, according to Joint Publication (JP) 3-04: *Information in Joint Operations*, were formerly called "information operations."[23]

While the services have each made investments in the race to informational arms, there is not yet a joint understanding. The Air Force and Army each released service-level doctrine on OIE in February 2023[24] and November 2023,[25] respectively. The Marine Corps published its service-level doctrine, "Information in Marine Corps Operations," in February 2024.[26] The Navy has likewise promulgated an updated service-level definition of OIE and established a division for OIE within the Office of the Deputy Chief of Naval Operations (DCNO) for Information Warfare (OPNAV N2N6),[27] before later shifting it to the DCNO for Operations, Plans, Strategy, and Warfighting Development (OPNAV N3N5N7).

Many information warfare capabilities and concepts also fit neatly under OIE and are ubiquitous across combatant commands. Perhaps most prominent among them is the concept

22. US Army and Navy, *JP 3-04: Information in Joint Ops*, September 14, 2022, https://www.scribd.com/document/660170977/JP-3-04-Information-in-Joint-Operations.
23. US Army and Navy, *JP 3-04*.
24. US Air Force, *Air Force Doctrine Publication 3-13: Information in Air Force Operations*, February 1, 2023, https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-13/3-13-AFDP-INFO-OPS.pdf.
25. Randi Stenson, "Army Publishes First Doctrinal Manual Dedicated to Information," US Army, November 25, 2024, https://www.army.mil/article/271932/army_publishes_first_doctrinal_manual_dedicated_to_information.
26. Todd McCarthy , *MCWP 8-10: Information in Marine Corps Operations*, US Marine Corps, February 29, 2024, https://www.marines.mil/Portals/1/Publications/MCWP%208-10%20(SECURED).pdf?ver=c4OjkntxdXoXZ9RvGMaIlA%3D%3D.
27. "U.S. Navy Operations in the Information Environment (OIE) Defined," US Navy, December 10, 2024, https://www.navy.mil/Press-Office/News-Stories/display-news/Article/3992620/us-navy-operations-in-the-information-environment-oie-defined/.

and associated capabilities of C-C5ISRT, which Paparo has highlighted as his top priority.[28] While OIE focuses on shaping behavior through information effects, C-C5ISRT describes the kill web network of nodes and connective tissue that feeds targeting decisions and is about constraining/restraining (or at times enabling) the adversary's ability for decision and action. It includes the cognitive, technical, and organizational systems through which information is sensed, processed, protected, and translated into decisions and actions.

These C-C5ISRT capabilities must reside at the operational level of war under commands like Pacific Fleet (PACFLT), Pacific Air Forces (PACAF), and their respective maritime and air operations centers (i.e., MOCs and AOCs). These operations centers execute the seven joint functions (command and control, information, intelligence, fires, movement and maneuver, protection, sustainment), and C-C5ISRT sets the conditions for all seven.[29] This is where campaigns are planned, where theater-wide intelligence is fused, and is best positioned to link physical operations to desired information effects. Future technological advancement will undoubtedly spur new organizational shifts, but today, more tactical echelons lack access to theater-wide intelligence and the authority or capability to synchronize effects across domains and services. Strategic echelons are too far removed from execution to respond at the speed of modern gray-zone warfare. While certain capabilities and concepts of OIE can be, and are, executed at the tactical, operational, and strategic levels, C-C5ISRT must be executed from the operational level.

While the joint force currently has no specific structure for C-C5ISRT, the Navy's Fleet Information Warfare Center Pacific (FIWCPAC) model demonstrates what effective operational-level integration should look like.[30] As an operational Echelon III command, FIWCPAC can "synchronize, align, and integrate information related capabilities across the Joint Force, to include U.S. Space Command (SPACECOM), U.S. Cyber Command (CYBERCOM), the U.S. Indo-Pacific Command (INDOPACOM) service components, and others, to enable Joint Force speed, action, and maneuver across the competition continuum."[31] This unit that can synchronize at the operational level of war, directly for and with the service component's operational centers, ensures that C-C5ISRT and information warfare is a core planning consideration from the outset. INDOPACOM has already seen success with this model and begun to proliferate it across service component commanders.[32] The joint force should next expand this construct to other geographic combatant commands as an immediately scalable approach to fielding C-C5ISRT capabilities.

Authorities, misperceptions, and cultural barriers

Misunderstandings surround the authorities to both acquire capabilities and operate in the information domain. At the tactical level, a common misperception is that nonspecialized units are not authorized to acquire or operate systems that could create a cognitive advantage. Many believe those capabilities are retained by and conducted at a higher echelon. However, acquisition and operational experts conclude many authorities are already available to warfighters, they are simply not used or well known. It is not a question of having the authority to either acquire or employ, but rather a mix of misperceptions and the services' cultural issues that stifle or restrict their use.

The DOD is making significant reform to its antiquated acquisition process to streamline the delivery of materiel and technology to its warfighters.[33] So far, this has demonstrated a willingness to accept more risk in the acquisition processes to ultimately reduce risk in fielding capabilities. While the reforms are primarily focused on materiel, they must also include software acquisitions which can create effects. Unlike materiel

28. Jon Harper, "Counter-C5isrt Is Top Priority for Nominee to Lead Indo-Pacific Command," DefenseScoop, February 1, 2024, https://defensescoop.com/2024/02/01/counter-c5isrt-samuel-paparo-indo-pacific-command-nomination/.
29. Matthew J. Tackett, "The Joint Functions: Theory, Doctrine, and Practice," National Defense University Press, October 22, 2024, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/4285985/the-joint-functions-theory-doctrine-and-practice/.
30. Daniel Marciniak, "Fleet Information Warfare Command Pacific Needs the Warfighters of the Future Today," US Pacific Fleet, April 26, 2024, https://www.cpf.navy.mil/Newsroom/News/Article/3758149/fleet-information-warfare-command-pacific-needs-the-warfighters-of-the-future-t/.
31. Mark Pomerleau, "Navy's Pacific Information Warfare Command Coordinating Vast Capability across Region," DefenseScoop, July 19, 2023, https://defensescoop.com/2023/07/19/navys-pacific-information-warfare-command-coordinating-vast-capability-across-region/.
32. Avery Smith, "Army's Information Vanguard: 1st Tiad Activation Signals Strategic Shift," US Army Pacific, November 19, 2025, https://www.usarpac.army.mil/Our-Story/Our-News/Article-Display/Article/4337704/armys-information-vanguard-1st-tiad-activation-signals-strategic-shift/#:~:text=FORT%20SHAFTER%2C%20Hawaii%20%E2%80%94%20On%20November,free%20and%20open%20Indo%2DPacific.
33. Exec. Order No. 14265, 90 Fed. Reg. 15621 (April 9, 2025).

acquisitions, software must also undergo the added scrutiny of the authority-to-operate (ATO) process, currently about twelve months long. This process must also be streamlined to focus on technical cybersecurity requirements and remove much of the archaic and unnecessary check-the-box coordination which creates unnecessary delays to fielding combat capability.

Even after acquiring and fielding capabilities, service culture barriers seemingly hinder the authority to conduct C-C5ISRT at echelon. While specific communities have unique authorities, such as intelligence and special operations, the larger conventional force remains less clear on the bounds, which results in a risk-averse approach to proactive C-C5ISRT. Today's global prevalence of social media and generative AI tools has created significant risk in the information domain. Especially in the competition phase, falling behind adversarial initiative and failing to minimize this risk puts the joint force at a significant disadvantage in shaping perceptions, legitimizing actions, strengthening alliances, changing behaviors, or altering decision-making. Ahead of conflict, the joint force and services must accept increased risk in employing cognitive effects and appropriately delegate authority to operate. This delegation of information authorities should coincide with like-delegation of kinetic authority; the two should be mutually complementary—and it should never be easier to unleash a bomb or missile than to send an official social media message. Promulgating higher headquarters guidance concerning information fires will assist in mitigating unintended or detrimental second- and third-order effects, similar to kinetic rules of engagement.

C-C5ISRT authorities and capabilities are not just for games and exercises; instead, the joint force must encourage their continual full-spectrum use by warfighters for all real-world operations. Ensuring inherently information-focused elements, including public affairs units or personnel, are "read-in" from the planning phase will enable better integration and synchronization of effects that contribute to an overall information advantage and mission success.

Operational employment and rapid implementation

The joint force must wholly shift from a reactive to proactive posture that prioritizes C-C5ISRT into all operations. Creating dilemmas for our adversaries through intentional surprise and uncertainty should be a part of every concept of operations. By creating an intentional dilemma for our adversary, we can force them to reveal their own tactics, techniques, and procedures in response. If we plan and conduct C-C5ISRT operations in competition correctly, we can force the adversary to burn their capabilities, sources, and methods. Conceal and reveal operations exemplify this model. The complex decision-making that determines controlled disclosure versus concealment of capabilities has been simplified through today's AI tools, which enhance our ability to weigh pros and cons, target messaging, and then evaluate effectiveness. Determining whether to withhold or reveal capabilities is never an easy decision, but in protracted long-term strategic competition, revealing can be a profitable decision for maintaining peace.[34]

Utilizing deception, decoys, and nontraditional methods of collecting data, feedback, and intelligence into our operational centers also remain insufficient. The joint force should leverage industry partnerships and new commercial capabilities such as advertising technologies, dark web scraping, and advanced social media analysis—all proliferated through AI—as new avenues to garner immediate messaging feedback and operational effectiveness. Combatant commands and operational-level commanders should share unclassified versions of their commander's critical information requirements (CCIRs) and priority information requirements (PIRs) with industry partners so commercial entities can tailor AI models and refine data collection to support operational needs. This collaboration, when paired with official intelligence assessments, would enable the joint force to understand adversary and allied populations' sentiment in near real time, better informing operations.

The scale of this challenge demands this integration. Data in the competition phase will be as defining as ammunition is during conflict; therefore, enabling our operational centers to collect and process data is essential to maintain decision advantage. The scale of our adversary also demands additional integration. The PRC can put significantly more personnel to task simply as a product of population. In the cyber realm, former FBI Director Christopher Wray called attention to this overmatch in 2023 by revealing that Chinese hackers outnumber FBI cyber personnel by at least fifty to one.[35] Closing this gap requires pushing data collection and analysis, along with intelligence capabilities, closer to the operational and tactical edge rather than retaining them at strategic echelons. This is not about replacing strategic intelligence but providing commanders real-time tools in order to speed and optimize operations. Integration of intelligence, public affairs, industry,

34. Brendan Rittenhouse Green and Austin Long, "Conceal or Reveal? Managing Clandestine Military Capabilities in Peacetime Competition," *International* Security 44, no. 3 (Winter 2019/20): 48–83, doi.org/10.1162/ISEC_a_00367.

35. Lauren Feiner, "Chinese Hackers Outnumber FBI Cyber Staff 50 to 1, Bureau Director Says," CNBC, April 28, 2023, https://www.cnbc.com/2023/04/28/chinese-hackers-outnumber-fbi-cyber-staff-50-to-1-director-wray-says.html.

data analytics, cyber operations, and traditional kinetic planning at the operational level enables the synchronized effects C-C5ISRT requires.

Time is not on our side. Adversaries are fielding capabilities faster, experimenting more aggressively, and operating proactively. The United States needs to put rapidly adaptable, easily iterable, software-defined products into warfighters' hands now and acknowledge that perfect is the enemy of good enough. The twenty-year-old on the battlefield will find novel uses for capabilities that planners never envisioned. Learning through experimentation, and ensuring that data is collected, processed, and acted upon is the only path to staying ahead of adversary adaptation.

Recommendations

Countering adversary C5ISRT is not a single capability challenge: It requires a system-wide approach including operational concepts, force structure, and supporting technology. As adversaries increasingly integrate emerging technologies into their C5ISRT systems, the US military must adapt how it detects, disrupts, and degrades these systems, particularly in the competition phase. The recommendations below identify near- to medium-term actions—by entity, offices, services, and commands—that can strengthen counter adversary C5ISRT operations.

Congress

- Aid the DOD's transition to software-defined warfare by enacting legislation to incentivize the rapid development, deployment, and continuous updating of software-enabled capabilities across the joint force. Recent DOD guidance on software acquisition highlights the need to rapidly adopt commercial software solutions, streamline the requirements processes, and enable consistent digital capabilities. Building on these efforts and echoing the recommendations of the Atlantic Council's Commission on Software-Defined Warfare,[36] Congress should also provide the DOD with greater flexibility in software funding across research, development, test, and evaluation (RDT&E), procurement, and operations and maintenance (O&M) accounts. These reforms would allow the DOD the required flexibility to deploy C-C5ISRT capabilities to scale quickly.
- Conduct a comprehensive review of the DOD Financial Management Regulation to align fiscal law with the Adaptive Acquisition Framework.[37] Congress should then establish a unified software-funding appropriation or provide clear statutory guidance on the application of existing appropriations to infrastructure as a service, platform as a service, and software as a service solutions that eliminate friction and accelerate delivery of C-C5ISRT capabilities to operational commanders.
- Direct the Defense, State, and Treasury departments to establish closer working ties at geographic combatant commands to ensure integrated operations and unity of effort.

Office of the Secretary of Defense (OSD)

- Develop, in collaboration with the Joint Staff and services, a departmental policy framework within the Office of the Under Secretary of Defense for Research and Engineering that guides salient C-C5ISRT capabilities and integration among the services, to include AI software selection and development.
- Expand the existing purview of the Joint Rapid Acquisition Cell within the Office of the Under Secretary of Defense for Acquisition and Sustainment to include nonmateriel solutions to urgent/emergent operational needs, such as AI software or program-user licenses.
- Direct a comprehensive review of the authorization requirements of the Federal Risk and Authorization Management Program (FedRAMP), as applied to DOD software acquisition, with the objective of reducing authorization timelines to ninety days or less for operationally relevant solutions. Where FedRAMP adds genuine security value, the process should be streamlined and incentivized. Where it functions primarily as an administrative gatekeeping mechanism that delays capable vendors, it should be reformed in favor of faster, operationally focused security-assessment pathways.

Joint Staff

- Formally adopt "C5ISRT" through the DOD Terminology Program and provide a standardized definition and common understanding among the joint force.
- Instill a common framework for planning, resourcing, and operationally executing C-C5ISRT across the joint

36. Whitney McNamara, Peter Modigliani, and Tate Nurkin, "Atlantic Council Commission on Software-Defined Warfare: Final Report," Atlantic Council, March 27, 2025, https://www.atlanticcouncil.org/in-depth-research-reports/report/atlantic-council-commission-on-software-defined-warfare/.
37. "Adaptive Acquisition Framework," Defense Acquisition University, accessed April 8, 2026, https://aaf.dau.edu/.

force through the Joint Warfighting Concept and updates to relevant Joint Publications, including an updated deterrence concept.

Military services

- Identify the organizations or units which perform OIE functions aligned with C-C5ISRT and assign the appropriate operational and tactical universal joint tasks and associated measures related to the coordination, integration, or employment of OIE to align planning, readiness reporting, training, exercises, and requirements.
- Structurally reform the ATO process and accelerate its existing compliance architecture. Publish Risk Management Framework (RMF) authorizing official (AO) chains of review, expand the pool of cleared agreements officers authorized to conduct ATO work on classified networks, establish reciprocal ATO recognition across services, and institute provisional ATOs for operationally urgent C-C5ISRT tools. Reform efforts should shift the RMF from a compliance-checklist orientation to a risk-based, operationally focused outcome-driven assessment model with a target authorization timeline of sixty days or less, with incentive structures that reward AOs for timely, well-reasoned decisions rather than defaulting to delay.
- Rapidly fund and field C-C5ISRT tools, software, and decision aids that utilize AI/ML for key operational centers. Prioritize speed and agility to rapidly deliver C-C5ISRT capabilities to warfighters. Implement a bottom-up training approach that enables operators to collect data and refine capabilities.
- Prioritize upgrades to operational centers to accommodate requisite people, equipment, and physical spaces including a collocated and accredited sensitive compartmented information facility (SCIF) space that accommodates special access programs (SAP) and compartmented access programs (CAP). Operational centers must be accredited to the classification of future competition and conflict.
- Prioritize the funding and outfit of live virtual and constructive (LVC) training environments, accredited up to SAP/CAP, at key operational centers. Soldiers, sailors, airmen, marines, and guardians should be able to train from the same watchfloors where they stand watch. These watchfloors are warfighting units in their own right and should be resourced as such.
- Ensure that individuals assigned to write requirements for software contracts are trained, retained, and promoted in accordance with their expertise. Consider utilizing reservists with public-sector software experience on long-term orders to develop expertise in the near term.
- Integrate public affairs and intelligence early and often in junior officer career paths. Mandate early involvement and integration at the operational level.

Combatant commands

- Apply the FIWCPAC model from INDOPACOM PACFLT to service component commanders across the globe, where appropriate.
- Craft a deterrence framework for respective areas of responsibility that nests within the Joint Concept with specificity on how C-C5ISRT capabilities enable deterrence and should be utilized.
- Craft unclassified CCIRs and/or PIRs to share with industry partners so that they can design tools to assist (e.g., tailor AI models, refine data scrapes).
- Capture relevant sentiment data from every joint operation and incorporate feedback to refine future joint force operations, activities, and investments.

Conclusion

If addressed effectively during the competition phase, C-C5ISRT operations will provide the United States with a decisive operational advantage. Reforming DOD processes to better enable the rapid acquisition, training, and deployment of C-C5ISRT capabilities will allow the US military to sense, target, and disrupt adversary systems before conflict begins. Achieving this outcome requires urgency and coordination throughout the national security enterprise, including Congress, the Office of the Secretary of Defense, the Joint Staff, the military services, the combatant commands, and private industry. These reforms would position the joint force to disrupt adversary C5ISRT systems, impose operational dilemmas, and create favorable conditions for deterrence and broader strategic influence.

The opinions expressed are those of the authors and do not reflect the views or policies of the US Department of Defense, Department of the Navy, Department of the Air Force, or the US government. No federal endorsement is implied or intended.

About the authors

Lieutenant Commander Martin Zuber is the 2025-2026 senior US Navy fellow at the Atlantic Council's Scowcroft Center for Strategy and Security. A surface warfare officer turned cryptologic and maritime cyber warfare officer, he has served in operational and staff roles across the Indo-Pacific, Middle East, and European theaters. He holds degrees in computer science and business analytics, with expertise in cyber warfare and artificial intelligence.

Lieutenant Colonel Caleb Eames is the 2025-2026 senior US Marine Corps fellow at the Atlantic Council's Scowcroft Center for Strategy and Security. His career spans enlisted and commissioned service in nuclear, biological, and chemical defense, embassy security, and public affairs, with operational experience in Iraq and across the Indo-Pacific. He currently serves as a communications strategy officer in the US Marine Corps and holds degrees in criminal justice, government administration, and communications.

Lieutenant Colonel Daniel Minnocci is the 2025-2026 senior US Air Force fellow at the Atlantic Council's Scowcroft Center for Strategy and Security. Most recently, he served as policy branch chief at Headquarters Air Force, where he led the development and coordination of Air Force protection policy. A career Security Forces officer, he has held command and staff roles across Air Force, joint, and multinational organizations, with extensive deployment experience.

Amy Cowley is an assistant director in the Forward Defense program at the Atlantic Council's Scowcroft Center for Strategy and Security. She holds degrees in international affairs and political science.

Acknowledgments

Forward Defense is grateful to Vannevar Labs for its support of this publication. This publication was written and published in accordance with the Atlantic Council's Intellectual Independence Policy, which requires all donors to agree to the Council maintaining independent control of the content and conclusions of its work. The authors are solely responsible for the publication's analysis and recommendations.

About the center

The **Scowcroft Center for Strategy and Security** works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.

Within the Scowcroft Center for Strategy and Security, *Forward* Defense leads the Atlantic Council's US and global defense programming, developing actionable recommendations for the United States and its allies and partners to compete, innovate, and navigate the rapidly evolving character of warfare. Through its work on US defense policy and force design, military applications of advanced technology, space security, strategic deterrence, and defense industrial revitalization, it informs the strategies, policies, and capabilities that the United States will need to deter, and, if necessary, prevail in major-power conflict.