Part I
Changes in the Strategic Environment in the Space Domain

Chapter 1
Winning the Fight for Sensing and Sensemaking

Bryan Clark

1. Introduction: Exploiting allied advantages in a post-dominance era

The US military has enjoyed broad superiority over potential and actual adversaries during the last half-century. Backed by a strong alliance network and the most robust defense research and development (R&D) base in the world, US forces routed opponents in Operations Desert Storm and Allied Force through the application of the then-new approach of networked precision strike warfare. And despite being frustrated by insurgencies in Iraq and Afghanistan, those largely strategic failures are not viewed as reflective of shortcomings in US military capabilities.

The era of US military dominance is now coming to a predictable end. The sensor, precision weapon, networking, and processing capabilities the Department of Defense (DoD) pioneered in the late Cold War are widely proliferated and being employed in combat by state and non-state groups across Ukraine, the Red Sea, and the Caucuses.[1] Moreover, as the underlying technologies associated with precision strike warfare—the global positioning system, satellite communications, and autonomous drones—were commercialized, adversaries such as Houthi rebels in Yemen can threaten US and allied forces at a fraction of the cost DoD spends in defense.

The erosion of US military dominance is most apparent with regard to the People's Republic of China (PRC). Through three decades of modernization, the PRC's People's Liberation Army (PLA) took the DoD's concept of precision strike warfare to new levels, fielding an extensive network comprising sensors across every domain and thousands of guided weapon launchers at sea, ashore, and in the air, as shown in Figure 1.

The asymmetry between the PLA and US military capacity in the Western Pacific derives in large part from the PRC's geostrategic advantages. Without significant mutual defense responsibilities, the PLA can concentrate its modernization and force posture on

---

[1] Defense Intelligence Agency (DIA), *Iran: Enabling Houthi Attacks Across the Middle East*, (Washington, DC: DIA, 2024), https://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/Iran_Houthi_Final2.pdf; David Barno and Nora Bensahel, "Learning From Real Wars: Gaza And Ukraine," War on the Rocks, December 6, 2023, https://warontherocks.com/2023/12/learning-from-real-wars-gaza-and-ukraine/.

pursuing a narrow set of core interests such as control over Taiwan or the South China Sea and preventing US or allied intervention.[2] In contrast, the US military is expected to address direct nation-state challengers like the PRC or Russia as well as opponents that are mainly threats to US allies, such as Iran or North Korea and their non-state proxies.

The PLA's structure and organization emphasizes defense of China's "near seas." Rather than build a globally deployed multi-mission military, the PLA Air Force (PLAAF) and Navy (PLAN) have not fielded substantial refueling and logistics capacity as part of their modernization and are still comprised predominantly of platforms that lack the capacity to both protect themselves and conduct attacks away from the PLA's mainland-based defenses.[3] But the most important enablers of China's counter-intervention strategy are the world's largest rocket force and the new Aerospace Force, which will pursue space-based sensing and counter-space capabilities and replaces part of the now-defunct Strategic Support Force.[4]

---

[2] Timothy Heath and Andrew S. Erickson, "Is China Pursuing Counter-Intervention?," The Washington Quarterly, Volume 38, Issue 3, Pages 143-156, DOI: 10.1080/0163660X.2015.1099029.

[3] For example, the PLAAF operates only about 2 dozen aerial refueling aircraft, compared to more than 500 US refueling aircraft; see Caleb Egli, "Fueling a Superpower: Reprioritizing the US Air Refueling Fleet for Great-Power Conflict," Air University, May 8, 2024, https://www.airuniversity.af.edu/JIPA/Display/Article/3768313/fueling-a-superpower-reprioritizing-the-us-air-refueling-fleet-for-great-power/; Mike Yeo, "Satellite Images Suggest China's New Tanker Aircraft Is under Production," Defense News, February 18, 2021, https://www.defensenews.com/global/asia-pacific/2021/02/18/satellite-images-suggest-chinas-new-tanker-aircraft-is-under-production/.

The PLAN has the following major combatants that can conduct offense and defense:
- 3 small carriers (on par with European CVs) vs. 11 larger US nuclear carriers
- 3 amphibious assault ships vs. 10 US amphibious assault ships
- 8 amphibious transport docks vs. 23 US amphibious transport docks
- 8 cruisers vs. 10 US cruisers
- 6 nuclear attack submarines vs. 50 US nuclear attack submarines
- 25 destroyers vs. 70 US Burke-class destroyers that carry 50% more weapons capacity

For smaller combatants, the PLAN has:
- 30 PLAN frigates vs. 32 comparable US littoral combat ships
- 24 quiet Yuan conventional subs that cannot operate quietly outside 2nd island chain
- About two dozen older conventional subs
- About two dozen older frigates and destroyers that only have enough weapon capacity to protect themselves in moderately contested environments: The US has retired equivalent ships

See Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China*, (Washington DC: US DoD, 2023), https://media.defense.gov/2023/Oct/19/2003323409/-1/-1/1/2023-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF.

[4] Namrata Goswami, "The Reorganization of China's Space Force: Strategic and Organizational Implications," *The Diplomat*, May 3, 2024, https://thediplomat.com/2024/05/the-reorganization-of-chinas-space-force-strategic-and-organizational-implications/; Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China*, (Washington DC: US DoD, 2023), https://media.defense.gov/2023/Oct/19/2003323409/-1/-1/1/2023-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF.

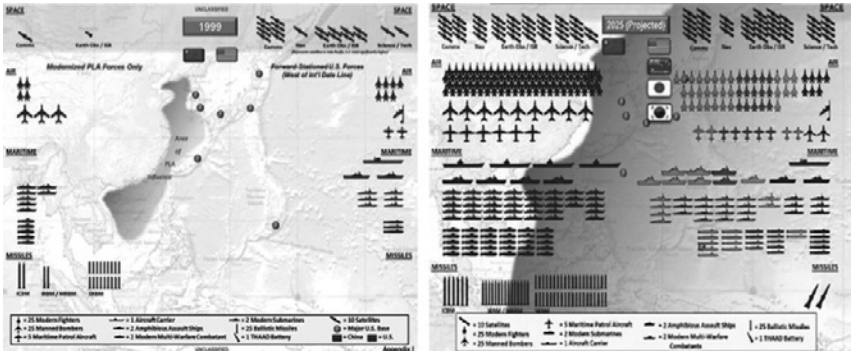


Figure 1: PLA posture in the Western Pacific compared to regionally-based US and allied forces[5]

Being the likely "home team" in future confrontations also affords PLA leaders the luxury to focus their concepts and capability development on countering the US military. As shown in Figure 1, the PLA could confront forces from Japan, Taiwan, Australia, or South Korea, but these US allies draw heavily upon US systems and emulate US tactics to enhance interoperability. And in conflict, the PLA could further undermine allies' contributions by attacking their home territory, compelling allied leaders to withdraw their relatively small forces to focus on homeland defense.

Degrading sensing and sensemaking to deter conflict

The US military will need to adopt a sustainable and survivable force posture in the Western Pacific to deter PRC aggression. In a rapid, large-scale conflict such as an invasion, the PLA's strike capacity would be diluted as it sought to engage many US and allied targets simultaneously. During a protracted, lower-intensity scenario like a blockade the PLA could devote more of its weapons to individual targets. And unlike the Taiwan scenario, US forces may not be able to counter-attack China's mainland unless an exchange escalates to theater-wide levels.

The DoD is unlikely to gain the upper hand in a symmetric missile vs. air defense competition with the PLA in the Western Pacific. Instead, it should take an asymmetric approach and degrade the PLA's ability to understand and anticipate allied operations or

[5] Brian Everstine's post on X, September 14, 2020, https://x.com/beverstine/status/1305512270571745282.

accurately target US forces. Attacking adversary command, control, communications, intelligence, surveillance, and reconnaissance (C3ISR) capabilities is already a stated objective of US Indo-Pacific Command leaders.[6] However, counter-C3ISR operations are historically focused on defeating enemy attacks during combat, when the PLA's capacity advantages may obviate US and allied electromagnetic warfare (EW) or cyber operations. Instead, US and allied counter-C3ISR operations will need to center on preventing conflict. PLA commanders may still see US and allied units operating in the region, but may be dissuaded from attacking if they cannot obtain precise location data, predict which US or allied forces are most important to planned operations, or expect their weapons to accurately hit intended targets.

This approach to attacking PLA sensing and sensemaking exploits US strengths in its own C3ISR capabilities and cyber or EW effects while exploiting inherent vulnerabilities in the PLA's operational concept of Systems Warfare. Depicted by Figure 2 in simplified form, Systems Warfare combines operations by reconnaissance-intelligence systems, firepower-strike systems, command systems, support systems, and information-confrontation systems to attack what PLA planners assess as key vulnerabilities in the US military's system of systems.[7]

The PLA's adoption of Systems Warfare is in part an effort to duplicate the successful US approach of precision strike warfare but with Chinese characteristics. Whereas US operations are fundamentally expeditionary, PLA operations are predominantly local. Given the difficulty of maintaining communications during combat, senior US officers and political leaders often rely on field commanders to manage operations, including sequencing fires, orchestrating maneuvers, and taking advantage of emergent openings. In contrast, top PLA commanders and the Central Military Commission (CMC) can easily communicate with PLA units, nearly all of which—such as those of the PLA Rocket Force (PLARF) and PLAAF—are based on Chinese soil. This allows senior leaders to directly control operations and not depend on field commanders, which senior

---

6 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/.

7 Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare* (Santa Monica, CA: RAND, 2018), https://www.rand.org/pubs/research_reports/RR1708.html.

PRC officials may not trust to be effective or loyal.[8]

The hierarchical nature of PLA command and control (C2) makes the reconnaissance-intelligence system and firepower strike system the most important elements of PLA Systems Warfare.[9] Senior PLA leaders depend on the reconnaissance-intelligence system to synthesize sensor data from widely-dispersed space, land, air, and sea-based systems, which is then provided to missile launchers on or near PRC territory for long-range precision strikes.

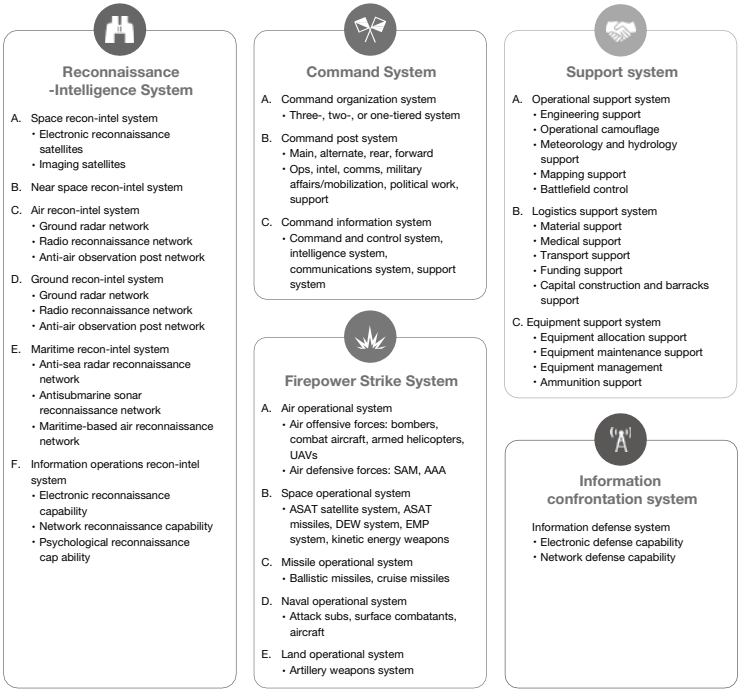


Figure 2: Simplified depiction of PLA Systems Warfare concept

---

[8] Jackson, Kimberly, Andrew Scobell, Stephen Webber, and Logan Ma, *Command and Control in U.S. Naval Competition with China*, (Santa Monica, CA: RAND Corporation, 2020), Pages 23-49. https://www.rand.org/pubs/research_reports/RRA127-1.html; Larry Wortzel, "The PLA and Mission Command: Is the Party Control System Too Rigid for Its Adaptation by China?," Association of the US Army, March 2024, https://www.ausa.org/sites/default/files/publications/LWP-159-The-PLA-and-Mission-Command-Is-the-Party-Conrol-System-Too-Rigid-for-Its-Adaptation-by-China.pdf.

[9] Joel Wuthnow, "System Destruction Warfare and the PLA," Institute for National Strategic Studies, June 2024, https://keystone.ndu.edu/Portals/86/PLA%20Systems%20Attack%20-%20JW%20update%20June%2024.pdf.

This centralized structure creates opportunities for US and allied forces to gain an advantage by undermining PLA sensing and sensemaking. Information from PLA aircraft and ships would be transmitted via a multiplicity of datalinks, which will increase their latency and reduce their reliability. Ground- and space-based sensor data would largely be conveyed via hard-wired connections from the sensor or ground station to a command center, offering greater timeliness and resilience compared to underway ships and aircraft. However, both categories of sensors are vulnerable to jamming, deception, and communications interdiction that could confuse the PLA's operational picture and decision-making.

Confusing and degrading sensing

US and allied forces could exploit their decades of experience in EW and cyber operations against PLA sensors on or above the earth's surface. These sensors all depend on radiofrequency (RF), visual, or infrared (IR) emissions, making them vulnerable to the injection of false or obscuring signals and malicious computer code. Undersea sensors like sonar depend on acoustic emissions which could be similarly manipulated to disrupt the PLA's undersea operational picture, as described in a previous Hudson Institute report.[10]

Well-orchestrated allied efforts to deceive or jam PLA sensors could confuse PLA operational pictures and planning. However, these efforts will only succeed for a limited time. Effective counter-sensing operations would need to address the likelihood that the Reconnaissance-Intelligence System could combine in real time the outputs of multiple sensors examining the same geographic position or target. Using sensor fusion, human operators, aided by artificial intelligence-enabled algorithms, would eventually determine the true position and activities of allied forces.

Attacking adversary sensemaking

Allied forces will therefore need to complement their efforts to degrade PLA sensor fusion by attacking PLA sensemaking. One approach would be to disrupt the communication networks needed to simultaneously bring together the outputs of multiple sensors across domains. Jamming or interrupting these signals, such as the datalink from a synthetic aperture radar (SAR) aircraft, would clearly degrade the Reconnaissance-Intelligence

[10] Bryan Clark and Timothy A. Walton, *Fighting into the Bastions: Getting Noisier to Sustain the US Undersea Advantage*, (Washington, DC: Hudson Institute, 2023), https://www.hudson.org/fighting-bastions-getting-noisier-sustain-us-undersea-advantage-submarine-bryan-clark-timothy-walton.

System's sensor fusion capability. And more subtle techniques—such as injecting code into the datalink that changes its message format—could defeat sensor fusion by slowing the integration of sensor data or by making the data appear to be associated with a different location or target.

US and allied forces can also undermine PLA sensemaking by combining their counter-sensing operations with less predictable tactics and force compositions. AI-enabled algorithms in the Reconnaissance-Intelligence System will attempt to compare sensor data with historical US operations and doctrine to inform PLA course of action (COA) development. US and allied forces can exploit the PLA's reliance on AI and predictive planning processes by establishing the possibility that US and allied forces could pursue a wide range of force compositions and operational concepts, rather than just those the PLA has seen or studied.

The DoD's ongoing efforts in Combined Joint All-Domain Command and Control (CJADC2) can help enable a more recomposable force that would give commanders more options for organizing and orchestrating their operations. Experiments such as those being pursued under the Army's Project Convergence and Navy's Project Overmatch are increasing the diversity of kill chains available to US forces through communications interoperability improvements. At the combatant commander level, the CJADC2 initiative produced an initial instantiation of the Joint Fires Network (JFN), which will connect commanders, shooters, and sensors across an entire theater to provide an adaptable set of attack options.[11]

However, force design can be more impactful than communications interoperability in creating a wider range of COAs for commanders and, as a result, greater uncertainty for enemy sensemaking. As depicted in Figure 3 and described in the authors' research on Mosaic Warfare and Decision-Centric Warfare, the DoD will need a more disaggregated force with a larger number of less multifunctional—and probably uncrewed—forces to substantially degrade PLA sensemaking. A small force, represented by the top half of Figure 3, can only configure itself in a few different ways, which limits it to a narrow range of operational concepts and tactics. Even a small force of multimission ships or aircraft does not present substantial complexity to an opponent like the PLA because each platform often behaves as a self-contained kill chain that can be neutralized by attacking only one target.

---

[11] Mark Pomerleau, "Indo-Pacific Command to Test Prototype of Joint Fires Network This Year," DefenseScoop, March 21, 2024, https://defensescoop.com/2024/03/21/joint-fires-network-indo-pacific-command-test-prototype/.

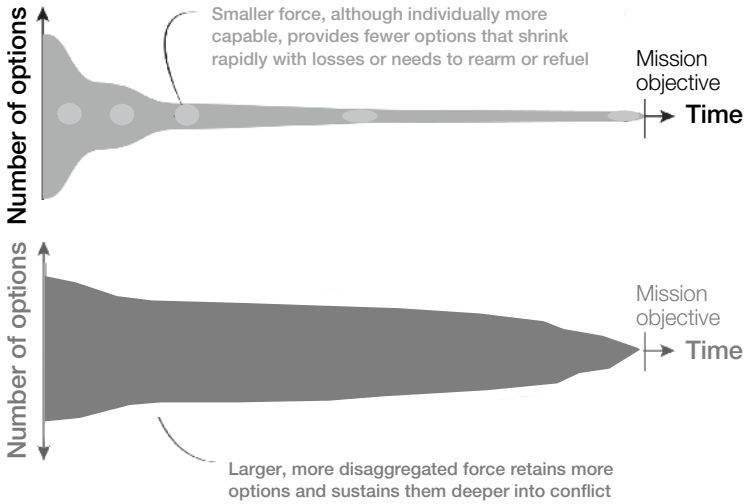


Figure 3: Options available to allied commanders

A larger force with more individual units, even if they are less sophisticated than those in a smaller force, would afford commanders more options for composing kill chains and therefore create more challenges for PLA sensemaking. And this disaggregation does not need to be of real weapons systems to be useful. Decoy or simulated platforms and vehicles can create the same complexity for enemy sensemaking as actual ones, compelling the adversary to either prepare for a wider range of US options or spend time and sensing resources to resolve ambiguity regarding the sensor information.

Prioritizing cross-domain non-kinetic effects

Compared to 20th century wars and 21st century counterterrorism, US and allied forces will need a more sophisticated EW and cyber approach to undermine a major power's comprehensive sensing and sensemaking architecture. In previous confrontations, non-kinetic capabilities were often employed within their respective domains and in different phases of conflict. Cyber exploits and malware were generated and delivered via wired networks, often as part of peacetime intelligence or counterterrorism operations. EW jamming and false targets were transmitted to enemy radars and radios through the RF spectrum during combat. For example, the PLA's reconnaissance-intelligence system is largely built on stand-alone networks inaccessible from outside China and incorporates large numbers of redundant RF sensors.

Adversaries' incorporation of digital technology into communications and sensing creates opportunities for allied forces to circumvent adversary efforts to create resilient sensing and sensemaking networks. Computerized military sensors can be better at detecting and countering EW attacks through signal processing but also include security weaknesses common to digital systems. And although potential opponents have shifted more of their military communications to stand-alone networks to protect against hacking, they still rely on RF apertures for sensing and to communicate with space, airborne, and sea-based platforms to enable sensor correlation and fusion.[12]

This suggests non-kinetic effects should increasingly be combined to overcome adversary sensor processing and fusion, as shown in Figure 4 and described in the 2020 Department of Defense Electromagnetic Spectrum Superiority Strategy.[13] For example, in addition to traditional "on-network" cyber effects being delivered via a wired connection, cyber effects will need to be delivered through RF apertures into stand-alone networks.[14] In addition to traditional EW effects that manipulate or obscure the RF signal reaching a sensor or radio, EW effects will depend on cyber exploits degrading the receiver's processing or verifying the EW effect succeeded.[15]

---

[12] Mark Pomerleau, "Services Working to Convergence EW, Cyber Warfare Capabilities," DefenseScoop, September 30, 2022, https://defensescoop.com/2022/09/30/services-working-to-convergence-ew-cyber-warfare-capabilities/.

[13] US DoD, 2020 *Department of Defense Electromagnetic Spectrum Superiority Strategy* (Washington, DC: US DoD, 2020), https://dodcio.defense.gov/Portals/0/Documents/Spectrum/2020DoD-EMS-SuperiorityStrategy.pdf.

[14] Director, Operational Test and Evaluation (DOT&E), *Cyber Assessment Program (CAP)* (Washington, DC: US DoD, 2023), https://www.dote.osd.mil/Portals/97/pub/reports/FY2023/dotemanaged/2023cap.pdf?ver=DrwfdCEmkKW0KX4UEQLFXg%3D%3D#:~:text=DoD's%20cyber%20posture%20remains%20at,systems%20that%20are%20essential%20to.

[15] Mark Pomerleau, "US Cyber Command Looking at How to Utilize Tactical On-the-ground Systems," DefenseScoop, January 16, 2024, https://defensescoop.com/2024/01/16/us-cyber-command-looking-at-how-to-utilize-tactical-on-the-ground-systems/.

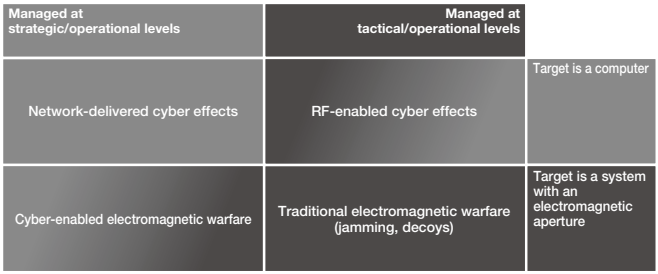


Figure 4: Emerging relationships between non-kinetic effects

Offensive cross-domain non-kinetic effects like cyber-enabled EW and RF-enabled cyber operations create new considerations for DoD C2. On-network US offensive cyber operations are generally authorized at the operational to strategic level by combatant commanders like US Cyber Command or the National Command Authority, which is either the president or secretary of defense. This reflects the permanent impact of releasing a cyber tool with the potential for immediate and recurring collateral damage. Offensive EW operations are usually controlled by field commanders or individual operators at the tactical to operational level because the effect is temporary and isolated to the aperture being targeted. Defensive effects in both cyber and EW operations are almost always controlled at a much lower level of authority and in many cases are automated.

Reforming for cross-domain non-kinetic operations

Offensive cross-domain non-kinetic effects will demand new C2 approaches. Like other military operations, operators delivering non-kinetic effects need access to the target, which is often fleeting. For an on-network cyber effect, senior leaders can usually monitor the target in real time over transcontinental distances and authorize delivery when appropriate. In contrast, forces delivering cyber-enabled EW and RF-enabled cyber effects will often be in areas where communications are degraded far from a command center. Field commanders may be challenged to obtain senior leader authorization during a window when the target aperture is accessible.

Cross-domain non-kinetic effects also occur over a different time scale compared to traditional cyber or EW effects, complicating planning and execution. Once authorized, operators can deliver on-network cyber tools at the speed of light and the impacts occur over minutes or hours. EW operations such as jamming or decoying transpire over minutes or hours because the effect is transitory and generally dissipates once the EW

system is turned off. Like EW operations, cross-domain non-kinetic effects may take minutes or hours to deliver due to challenges gaining access to the appropriate apertures, but the impacts may be long-lived like cyber effects because they incorporate digital code.

Cyber-enabled EW and RF-enabled cyber effects will likely require a hybrid C2 approach similar to how other military capabilities are employed. Senior military and civilian leaders generally prefer to have control over on-network cyber effects because their presence on the internet can cause collateral damage or allow them to be released "into the wild." However, cross-domain non-kinetic effects are by definition being delivered into an isolated adversary and have less likelihood of impacting other military or civilian networks. To avoid missing opportunities to exploit US advantages in cyber and EW, senior leaders could approve types or categories of cross-domain effects and delegate to local commanders the authority to use them in accordance with prescribed rules of engagement.

Most relevant to this report, cross-domain non-kinetic effects also demand a new capability development approach. The US military services and US CYBERCOM develop new offensive cyber tools on government-owned ranges at a relatively slow tempo, given their infrequent employment in military operations. In contrast, the services each have a robust infrastructure for EW requirements development and reprogramming that, while slow, implements a substantial number of changes each year. The DoD will need an approach that can model both wired network and RF delivery mechanisms and allow for integration of activities across electromagnetic and cyber environments.

The DoD's non-kinetic capability development process will also need to deliver at greater scale than today. As described in Section 2, the US military will need to employ non-kinetic effects more frequently as part of peacetime competition and crisis. Historically, these operations were reserved for combat, where they protected allied forces and degraded the effectiveness of enemy attacks. However, given their geostrategic disadvantages US and allied militaries will need to disrupt enemy sensing and sensemaking as an element of dissuasion and deterrence. Section 3 of this report will detail an approach to counter-sensing and sensemaking campaigns against capabilities like those deployed by the PLA.

The DoD will need a deep magazine of non-kinetic effects to implement a counter-sensing and sensemaking campaign. This report concludes with recommendations for the DoD to adopt this new process and enable the US military to regain the advantage in a post-dominance era.

2. Using counter-sensing and sensemaking for deterrence and dissuasion

Allied forces should use their advantages in C3ISR and counter-C3ISR to support deterrence and dissuasion, rather than only relying on these capabilities in combat after deterrence has failed. Traditionally, the US military has pursued deterrence by threatening to deny success to an adversary's aggression and impose economic or military punishments that would outweigh the benefits of an attack. This approach is losing efficacy in the post-dominance era. Russian president Vladimir Putin chose to attack Ukraine in 2022 despite facing the most comprehensive economic and diplomatic punishments mounted since World War II and continued the invasion after Ukraine's initial denial of the assault.[16] Iranian-backed Houthi rebels regularly attack US ground and naval forces across the Middle East despite sanctions on Iran and counter-attacks by US and allied forces.[17] And the PRC's coast guard and maritime militia routinely harass and periodically collide with naval and constabulary forces from the Philippines, Taiwan, and Japan.[18]

The US and its allies will need to do more than threaten punishment or denial to dissuade PRC aggression. Incremental attacks like Russia's "gray-zone" operations in eastern Ukraine and annexation of Crimea can be difficult to counter with traditional military forces. More overt actions such as Russia's 2022 invasion of Ukraine are easier to recognize but difficult to interdict from long range and on short notice. A PRC blockade of Taiwan could look more like the former while an invasion would more closely resemble the latter.

US and allied militaries could exploit the PLA's dependence on its reconnaissance-intelligence system to address both types of challenges. For example, Chinese forces implementing a blockade will require an accurate and timely operational picture to understand where shipping is attempting to enter or leave the blockaded country and the position of potential escorts. During an invasion of Taiwan, attacking PRC forces will need an accurate target picture to avoid wasting weapons that may be needed later if a conflict becomes protracted, as happened in Ukraine.

---

16 Nadia Schadlow, "Why Deterrence Failed Against Russia," The Wall Street Journal, March 20, 2022, https://www.wsj.com/articles/why-u-s-deterrence-failed-ukraine-putin-military-defense-11647794454.

17 Oren Liebermann and Nikki Carvajal, "Biden Concedes Houthis Haven't Been Deterred from Carrying Out Attacks as US Launches Further Strikes," CNN, January 18, 2024, https://edition.cnn.com/2024/01/18/politics/biden-houthi-strikes/index.html.

18 Derek Grossman, "How to Respond to China's Tactics in the South China Sea," *Foreign Policy*, May 29, 2024, https://foreignpolicy.com/2024/05/29/philippines-us-south-china-sea-gray-zone-tactics-alliance-military-treaty/.

The 2022 US National Defense Strategy (NDS) offers a way to exploit the PLA's sensing and sensemaking vulnerabilities through its line of effort for "campaigning." The strategy directs the DoD to "operate forces, synchronize broader Department efforts, and align Department activities with other instruments of national power, to undermine acute forms of competitor coercion, complicate competitors' military preparations, and develop our own warfighting capabilities together with Allies and partners."[19]

In US Marine Corps doctrine, campaigning is a series of operations designed to achieve a particular objective in a specific time and space.[20] Campaigning recognizes that winning battles is no guarantee of achieving long-term objectives, as numerous historical cases can attest.[21] Often associated with large-scale combat operations like the Allied retaking of Europe during World War II, campaigns can also comprise a long series of less-intense actions during peacetime, such as the British counterinsurgency operation in Malaysia.[22] Although nonmilitary instruments have a substantial role in enabling these and other successful campaigns, this report will focus on the application of military activities.

The DoD could use a counter-sensing and sensemaking campaign to dissuade aggression by the PRC. Although less studied and discussed compared to deterrence, dissuasion offers a way to influence competitions or confrontations when conflict is not imminent. If combatants are hurtling toward war and key decisions have already been made, it is likely that only the certainty of failure or intolerable punishment will stop them; for every other situation, efforts to dissuade could steer the belligerents away from destructive action.[23]

---

[19] Lloyd Austin, *2022 National Defense Strategy of the United States of America*, (Washington, DC: US DoD, 2022), 1, https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF.

[20] US Marine Corps, "Campaigning," in *Marine Corps Doctrinal Publication 1-2*, August 1, 1997, https://www.marines.mil/Portals/1/Publications/MCDP%201-2%20Campaigning.pdf.

[21] Perhaps the best recent example of this is William Westmoreland, who proudly claimed that the US won every battle it fought though many people regard the Vietnam War as unsuccessful in achieving US aims. See Neil Sheehan, *A Bright Shining Lie: John Paul Vann and America in Vietnam* (New York: Random House, 1988).

[22] Robert W. Komer, *The Malayan Emergency in Retrospect: Organization of a Successful Counterinsurgency Effort* (Santa Monica, CA: RAND, 1972), https://www.rand.org/pubs/reports/R957.html.

[23] For more details on this approach, see Bryan Clark and Dan Patt, *Campaigning to Dissuade: Applying Emerging Technologies to Engage and Succeed in the Information Age Security Competition*, (Washington, DC: Hudson Institute, 2023), https://www.hudson.org/defense-strategy/campaigning-dissuade-applying-emerging-technologies-engage-succeed-information-age-bryan-clark-dan-patt.

Restoring escalation advantage

PRC military and paramilitary forces would need to mount an intense, large-scale fires campaign to support an invasion of Taiwan. History shows amphibious assaults are high-risk operations that leave large numbers of troops exposed and vulnerable for extended periods.[24] To prevent Taiwan and its allies from interdicting its invasion force, the PLA will need to neutralize ships, air bases, and aircraft carriers across the East and South China Seas and Philippine Sea. US and allied forces could use counter-sensing and sensemaking operations to increase the likelihood an invasion could fail by degrading PLA fires.

The PLA would normally have a substantial escalation advantage over Taiwan and its allies. As shown in Figure 5, the reconnaissance-intelligence system and firepower strike system enable the PLA to mass fires at various scales in its near-abroad, including in defense of its gray-zone operations. Allied forces lack the defensive capacity to protect themselves from PLA attacks unless they aggregate in large formations that may only be practical in the context of major conflict. Moreover, US allies in the region could consider large formations to be overly provocative or escalatory if mobilized in response to a gray-zone confrontation.

The asymmetry depicted in Figure 5 leaves US and allied forces at an escalation disadvantage to China. For example, People's Maritime Militia and China Coast Guard ships can harass and ram Philippine fishing and coast guard vessels under the protection of mainland-based ships, aircraft, air defenses, and surface-to-surface missiles. Allies confronting the aggression will either need to do so at elevated risk or bring substantial offensive and defensive firepower to survive and threaten counterattacks in a highly contested environment close to China. However, such a robust force posture could prove counterproductive by portraying US and allied militaries as aggressors rather than the PRC.[25]

---

[24] Carter Malkasian, *Charting the Pathway to OMFTS: A Historical Assessment of Amphibious Operations from 1941 to the Present*, (Alexandria, VA: CNA, 2002), https://www.cna.org/reports/2002/D0006297.A2.pdf.

[25] These dynamic and potential solutions are addressed in Bryan Clark, Mark Gunzinger, and Jesse Sloman, *Winning in the Gray Zone: Using Electromagnetic Warfare to Regain Escalation Dominance*, (Washington, DC: CSBA, 2017), https://csbaonline.org/research/publications/winning-in-the-gray-zone-using-electromagnetic-warfare-to-regain-escalation.

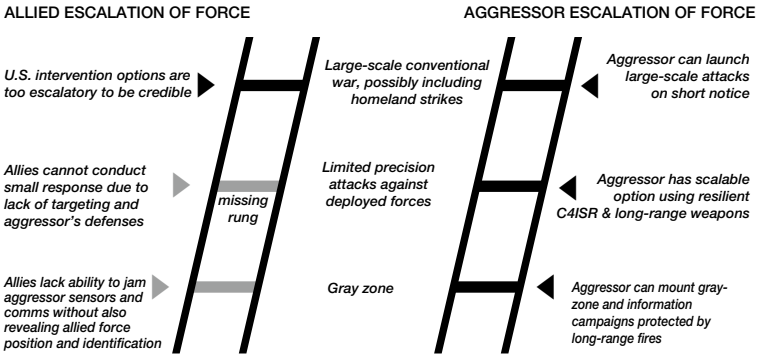


Figure 5: Escalation ladder comparing allied forces and PLA forces

If equipped with appropriate delivery systems and effects, US and allied forces could use non-kinetic operations to restore lower-level rungs on the escalation ladder and switch this asymmetry as shown in Figure 6. For example, US and allied forces could degrade adversary sensors through electronic jamming and deploy persistent decoys across multiple regions of the EMS. They could enhance the impact of counter-sensing operations through actions to complicate sensemaking, such as deploying in distributed and recomposable formations that deny adversary operators an opportunity to determine which targets are real or most valuable based on historical patterns. In addition to creating uncertainty for opposing commanders' plans, these activities could elicit responses that reveal adversary concerns regarding reconnaissance-intelligence system effectiveness.

Non-kinetic effects would also drive the potential aggressor to higher levels of escalation. To ensure they engage intended targets in the face of US and allied counter-sensing and sensemaking operations, aggressors may need to expend more weapons to attack all the potential targets simultaneously. Alternatively, enemy commanders could attempt to clarify the target picture and enable more efficient strikes, but these actions can also be escalatory. PLA sensor platforms may need to closely approach US and allied forces to obtain accurate classification and identification information or illuminate them with fire control radars, which could be perceived as provocative. In either case, counter-sensing and sensemaking removes lower rungs from China's escalation ladder.[26]

---

[26] Bryan Clark and Dan Patt, *Campaigning to Dissuade: Applying Emerging Technologies to Engage and Succeed in the Information Age Security Competition*, (Washington, DC: Hudson Institute, 2023), https://www.hudson.org/defense-strategy/campaigning-dissuade-applying-emerging-technologies-engage-succeed-information-age-bryan-clark-dan-patt.

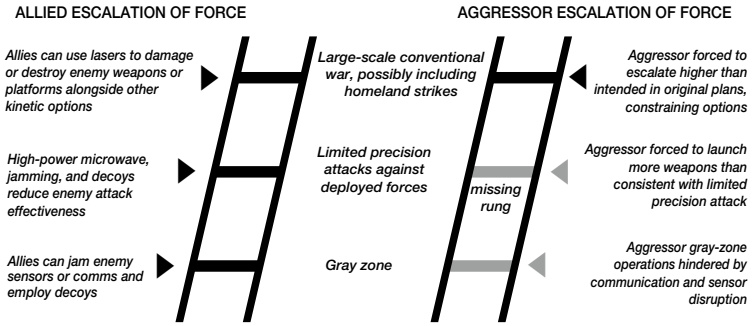


Figure 6: Revised escalation ladder with effective counter-sensing and sensemaking of allied forces

In addition to being escalation options in their own right, counter-sensing and sensemaking would also restore the ability to conduct small-scale allied physical attacks. Under the current escalation paradigm of Figure 6, small attacks such as disabling a maritime militia ship or forcing down an intruding bomber can only be undertaken at great risk in the region around China. However, if complemented by counter-sensing and sensemaking operations, these small-scale engagements could be obscured for long enough to complete the operation or seem to require so large an intervention that PRC leaders choose not to escalate.

Designing a counter-sensing and sensemaking campaign

During a peacetime competition, such as exists today between China and United States, the goal of a US-led counter-sensing and sense-making campaign would be to steer PRC leaders away from the most destructive paths to their objectives. As shown in Figure 7, the PRC has several different scenarios it could pursue to forcibly unify with Taiwan. The most undesirable path from the US and allied perspective is likely an invasion, followed by bombardment or a blockade.

By targeting the reconnaissance-intelligence system, a counter-sensing and sensemaking campaign would likely have the most impact on an invasion scenario. Aerial bombardment of Taiwan or its neighbors could rely on pre-determined aimpoints and implementing a blockade does not depend on timely, centrally-organized targeting information. An invasion, in contrast, will require PLA forces to quickly engage US and other allied ships, submarines, and aircraft that may seek to stop the invasion. These moving forces cannot be targeted in advance but the PLA would need to neutralize them

for an invasion to succeed.

A counter-sensing and sensemaking campaign would not render an invasion infeasible. The PLA has a sufficient capacity advantage to possibly succeed even with poor C3ISR performance. However, the higher dependence of an invasion on the reconnaissance-intelligence system suggests counter-sensing and sensemaking operations could drive down the preference of PRC leaders for that scenario and make other scenarios more attractive. These other scenarios may still be undesirable for US and allied leaders, but they may be less-destructive, slower-paced, and offer more off-ramps to de-escalation compared to an invasion.

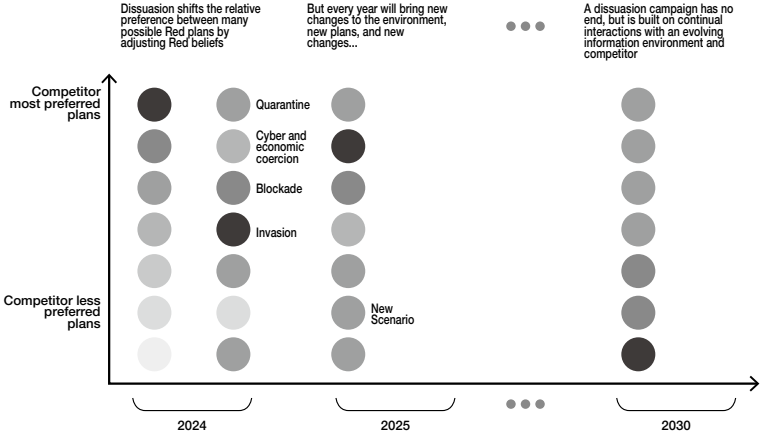


Figure 7: Implementation of a dissuasion strategy

Tell, don't show

US and allied forces have increased their use of lower rungs on the escalation ladders during the last several years. In response to rising PRC intrusions into its airspace and maritime zones, Japan's military stepped up interdictions and patrols. The US Navy is now routinely joined by Australian, Japanese, and European naval vessels in conducting freedom of navigation operations in waters illegally claimed by China.[27] And most prominently, Philippine ships regularly confront Chinese fishing and coast guard vessels attempting to block access to features in the Philippine's Exclusive Economic Zone, such

[27] Reuters, "Allies, Partners Conduct Joint Naval Exercises in South China Sea for Free and Open Indo-Pacific," Indo-Pacific Forum, October 4, 2024, https://ipdefenseforum.com/2024/10/allies-partners-conduct-joint-naval-exercises-in-south-china-sea-for-free-and-open-indo-pacific/.

as Second Thomas Shoal and Mischief Reef.[28]

These overt measures are effective at demonstrating allies' resistance to Chinese gray-zone operations for the international audience. However, they may be counter-productive in dissuading future Chinese gray-zone or more escalatory acts of aggression. By openly opposing Chinese intrusions, allied efforts create reputational risk for PRC leaders, who likely believe that gray-zone operations show their strength and resolve in establishing and enforcing regional hegemony. For example, the Philippines' open defiance of China's attempts to close the entrance of Second Thomas Shoal—where Philippine sailors operate a grounded tank landing ship—demands that Chinese leaders ramp up their efforts to hinder, harass, and contain Philippine efforts to resupply the ship. If China did not respond forcefully, Chinese leaders risk other countries in the region taking a similar stance regarding disputed territorial claims.[29]

Covert actions may offer more leverage in influencing Chinese leaders compared to overt actions. As shown in Figure 8, allied forces (in green) can send signals to PRC leaders (in red) through two main channels. One path, for overt actions, travels through the global information environment to be received by the opponent. The other, for covert actions, travels directly from one competitor to the other in what is essentially a closed feedback loop.

---

[28] John Pollock and Damien Symon, "China Blocks Philippines Access to South China Sea Reef," Chatham House, March 21, 2024, https://www.chathamhouse.org/publications/the-world-today/2024-02/china-blocks-philippines-access-south-china-sea-reef.

[29] Andrew Taffer, "The Puzzle of Chinese Escalation vs Restraint in the South China Sea," War on the Rocks, July 26, 2024, https://warontherocks.com/2024/07/the-puzzle-of-chinese-escalation-vs-restraint-in-the-south-china-sea/.

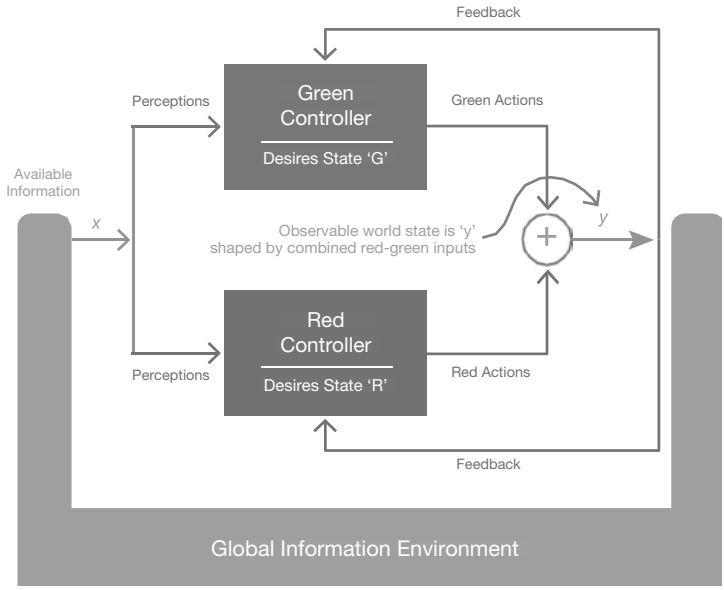


Figure 8: Information exchange between US and allies (Green) and PRC (Red)

Counter-sensing and sense-making operations exemplify operation of the feedback loop in Figure 8. Because they are designed to impact the adversary's sensors and associated C3 capabilities, actions like jamming, decoy deployment, or cyber attacks would normally only be perceived by the adversary. In some cases, counter-sensing and sensemaking actions could be observable to others, such as commercial satellite-sensing providers. However, these companies and the analysts who rely on them would not know whether the PLA was impacted by the operation. PRC officials may be reticent to complain about the counter-sensing and sensemaking operation to avoid revealing a potential vulnerability in the reconnaissance-intelligence system.[30]

Chinese leaders may not acknowledge an allied counter-sensing and sensemaking action, but effective jamming or deception should generate a reaction as PLA operators attempt to clarify their contact picture and remediate vulnerabilities in their sensors and C2 capabilities. US and allied observers could use the PRC response to assess

[30] Richard Manley, "Cyber in the Shadows: Why the Future of Cyber Operations Will Be Covert," (Washington, DC: US National Defense University, 2022), https://ndupress.ndu.edu/Media/News/News-Article-View/article/3105355/cyber-in-the-shadows-why-the-future-of-cyber-operations-will-be-covert/.

the relative importance of the affected system, process, or organization in the overall reconnaissance-intelligence system and whether the system's shortfalls were known to PLA and PRC leaders. For example, if after a decoy and jamming operation against Chinese ELINT satellites the PLA were to modify their orbits or begin flying more ISR aircraft in the area allied leaders could assess that either ELINT satellite performance was already suspect or that they form a critical node in the reconnaissance-intelligence system. Future counter-sensing and sensemaking operations could target the updated ELINT constellations or shift to other sensors or processes and evaluate their role in the reconnaissance-intelligence system.

A magazine of surprise

Counter-sensing and sensemaking actions can support US and allied combat operations by degrading adversary targeting and undermining its plans. But as the discussion above suggests, non-kinetic effects are also central to a peacetime dissuasion campaign. The two applications demand somewhat different types and orchestrations of cyber and EW effects. During combat operations, US and allied forces would likely rely on standardized and overt non-kinetic effects that are easy for operators to execute in battle and that can be observed by other friendly forces. However, a successful dissuasion campaign will require counter-sensing and sensemaking operations that produce unexpected effects. Predictable allied actions will generate proforma responses, such as China's now-standard demarches against US and allied freedom of navigation operations. Allied non-kinetic operations will need to be surprising if they are to undermine PLA plans and confidence and reveal insights regarding Chinese perceptions of its own systems, processes, and organizations.

The need for surprise in peacetime counter-sensing and sensemaking operations reinforces the importance these actions being covert. A surprising overt action in peacetime, like shutting down a Chinese state-owned commercial satellite surveillance constellation with a cyber attack, could be viewed by Chinese leaders as highly escalatory and necessitate a robust response that proves counter-productive to the goal of dissuading aggression. In contrast, Chinese leaders would be less likely to react substantially to a covert allied non-kinetic action because a strong response could confirm the existence of an underlying vulnerability to the attacker or wider public.

Non-kinetic effects could offer a new path to dissuading aggression, but allied forces will be challenged to generate covert and surprising non-kinetic effects at the scale needed to shape Chinese leaders' scenario preferences. Cyber and EW effects

are generally perishable because an adversary will likely quickly attempt to mitigate a C3ISR vulnerability once revealed. A sustained peacetime competition could require thousands of non-kinetic effects over time, but unlike conventional munitions, each non-kinetic effect will need to be different. This suggests the DoD will need to invest in the infrastructure to produce adaptable effects at scale.

As shown in Figure 9, allies will rapidly deplete their stockpile of non-kinetic effects as they take EW or cyber actions and the adversary fields countermeasures or the associated vulnerability is discovered and corrected by an opponent. At the same time, China will likely also take non-kinetic actions against allied interests to deter them from further cyber and EW operations. Allied forces will need a deeper magazine of non-kinetic effects compared to China for US and other leaders to be confident in carrying on the competition and to demonstrate to Chinese leaders that the PLA cannot sustain sensing and sensemaking superiority.

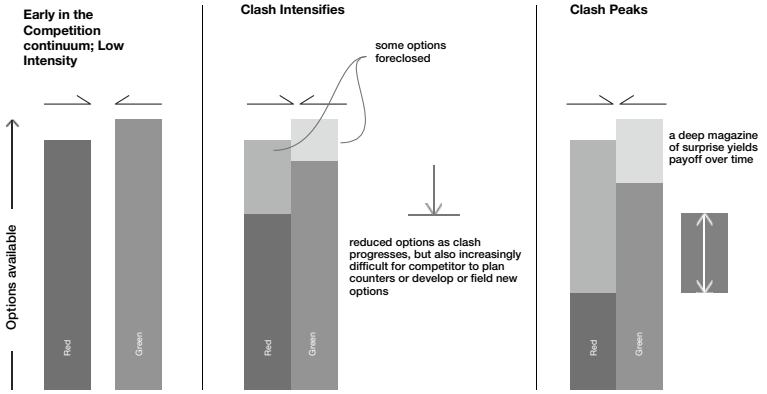


Figure 9: Representation of Allied (Green) and Chinese (Red) non-kinetic capability magazines

US forces arguably field the world's most capable portfolio of non-kinetic effects. And the US military is deploying new families of EW systems in each service that are beginning to move beyond self-protection to execute offensive effects such as decoying, deception, and stand-in jamming. For example, the Army is fielding its Terrestrial Layer

System at the soldier, brigade, and division level.[31] The Navy is installing upgraded versions of its SLQ-32 Surface EW Improvement Program system on DDGs.[32] And the Air Force is expanding its spectrum warfare wing with new squadrons and missions.[33]

The US government may have the world's most capable cyber and EW systems and operators, but it is generally focused on protecting troops, ships, and aircraft in wartime and specific, highly specialized offensive actions in peacetime. The DoD's supply chain for cyber tools and EW techniques and systems lacks the diversity and capacity needed to engage in a protracted sensing and sensemaking competition. US forces will need a wide variety of effects for a peacetime dissuasion campaign ranging from the most-capable "silver bullets" needed to gain the upper hand in a war to the "lead" or "brass" bullets needed to undermine adversary sensing and sensemaking over a sustained, multi-year competition.

3. Mounting a counter-sensing and sensemaking campaign

US and allied forces can most effectively employ EW and cyber effects as part of a campaign. As described in the DoD's cyber strategy, readying a few highly-classified non-kinetic "silver bullets" does not contribute to deterrence or dissuasion.[34] And from the perspective of sensing and sensemaking, DoD leaders who plan to use only a small set of highly-sophisticated non-kinetic tools in wartime accept the risk that an aggressor could overcome targeting shortfalls with greater mass. US and allied forces are likely to confront the PLA in China's near-abroad where the PRC will have an advantage in munitions capacity and resupply, making this "silver bullet" approach unlikely to succeed.

The DoD cyber strategy emphasizes use of non-kinetic capabilities as part of campaigns, but concerns itself primarily with thwarting and deterring espionage and non-kinetic attacks on US military forces and civil infrastructure. US and allied forces attempting to deter or dissuade multi-domain aggression will need to degrade an

---

[31] Mark Pomerleau, "Army Pursuing New Electronic Warfare Architecture," DefenseScoop, August 21, 2024, https://defensescoop.com/2024/08/21/army-pursuing-new-electronic-warfare-architecture/.

[32] Sam LaGrone, "Navy Refining Plan for its $17B Destroyer Electronic Warfare Backfit with 4 Test Ships," USNI News, January 19, 2024, https://news.usni.org/2024/01/19/navy-refining-plan-for-its-17b-destroyer-electronic-warfare-backfit-with-4-test-ships.

[33] Greg Hadley, "Spectrum Warfare Wing Adds Two New Squadrons to Handle Growing Mission," *Air and Space Forces Magazine*, May 1, 2024, https://www.airandspaceforces.com/spectrum-warfare-wing-two-new-squadrons/.

[34] US DoD, *Summary of the 2023 Cyber Strategy of the U.S. Department of Defense* (Washington, DC: US DoD, 2023), https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF.

adversary's operational capabilities overall —not just those in cyberspace or the EMS. As described previously, PLA strategy and concepts hinge on the reconnaissance-intelligence system's ability to understand opposing forces' positions and actions and target long-range fires. Therefore, US non-kinetic campaigns should focus on winning the sensing and sensemaking competition.

Allied forces can take multiple paths to degrading PLA sensing and sensemaking, but one approach is described below. This example is intended to illustrate at an unclassified level the kinds of capabilities and operations that could be used as part of a campaign. An actual campaign would be more complex and incorporate a range of classified and specialized EW and cyber effects.

Avoid an "own goal" in sensing and sensemaking

The first principle of counter-sensing and sensemaking is to "do no harm." US and allied forces will need to avoid providing enemy reconnaissance systems easily-detected and classified signals that could obviate allied deception operations. For example, the monostatic radars and datalinks that became essential to air surveillance, early warning, and missile defense during the last half-century can also reveal a platform's location as well as its type and classification.

Due in large part to the vulnerability of monostatic radars and datalinks, the US military prioritized emission control (EMCON) operations during the Cold War. Understandably, EMCON became a lower priority in the decades since the Soviet Union fell.[35] However, in recent years US forces reestablished these practices as part of their operational routines.[36] EMCON primarily involves minimizing the use of radios and radars when enemy forces could detect them. However, given the ubiquity of passive RF and signals intelligence (SIGINT) sensors, allied forces will need to increasingly turn to passive and multistatic sensing combined with low-probability of intercept/low-probability of detection (LPI/LPD) communications.

As shown in Figure 10, allied forces could pursue several types of new sensing modalities that move away from monostatic radar. Using multiple RF receivers on nearby uncrewed vehicles, allied forces could geolocate enemy forces by detecting their radio

---

[35] Robert G. Angevine, "Hiding in Plain Sight—The U.S. Navy and Dispersed Operations under EMCON, 1956–1972," Naval War College Review, Volume 64, Issue 2, 2011, https://digital-commons.usnwc.edu/nwc-review/vol64/iss2/6.

[36] Bryan Leese, "Living in TACSIT 1," *USNI Proceedings*, February, 2017, https://www.usni.org/magazines/proceedings/2017/february/living-tacsit-1.

or radar emissions. Uncrewed aircraft or missiles could illuminate with RF energy an enemy ship or aircraft to allow bistatic targeting by an allied platform that can remain in EMCON. Allied forces could use the background emissions from local television or mobile communication towers to illuminate enemy targets using passive radar. And allied forces could use IR sensors such as IR search and track (IRST) to find and classify enemy forces using their heat signatures.[37]

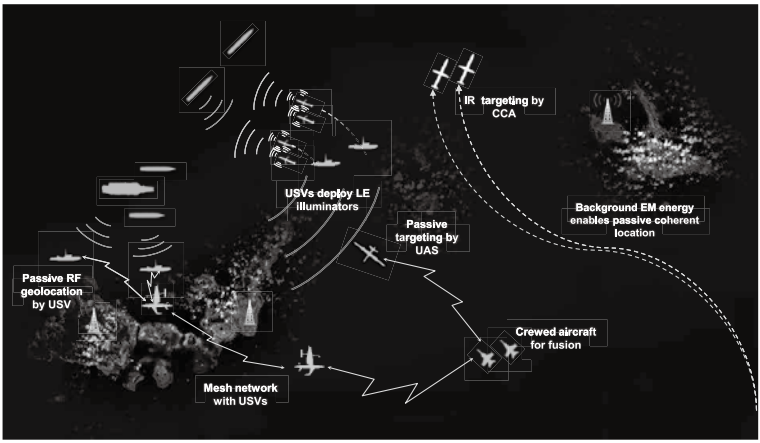


Figure 10: Concepts for passive and multistatic sensing

Passive and multistatic sensing is generally shorter-range and less precise than active monostatic radar. However, emerging technologies and techniques can help allied forces mitigate these shortfalls.[38] For example, expendable uncrewed systems could be used to closely approach enemy forces or illuminate a target to enable detection with lower consequences compared to a crewed ship or aircraft. Higher-density RF or electro-optical sensors can obtain more precise bearings to a radar, radio, or infrared emission. And artificial intelligence (AI) can be applied to improve predictions of adversary target

---

37 US DoD, "Selected Acquisition Report (SAR): F/A-18 E/F IRST," (Washington, DC: US DoD, 2023), https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Selected_Acquisition_Reports/FY_2022_SARS/IRST_SAR_DEC_2022_final.pdf.

38 Jheng-Sian Li, Yung-Cheng Yao, Chun-Hung Chen, and Jyh-Horng Wen, "A Method to Improve the Accuracy of the TOA Position Location Solution in Multistatic Radar Systems," Proceedings - 6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS 2012, Pages 500-505, 10.1109/IMIS.2012.36.

locations and classifications through training on actual targets with human supervision.[39]

US and allied forces will also need to reduce their IR signatures. This largely is done through platform design, but could be augmented by camouflage or additional heat sources that could obscure the ship, aircraft, or vehicle signature and reduce the opponent's ability to discern the target's classification or identification.[40] These approaches are being employed by Russian and Ukrainian troops to counter opponents' sensing and sensemaking during their ongoing conflict.[41]

Deceiving SIGINT sensors

A counter-sensing and sensemaking campaign would start with decoy operations. By creating numerous false targets for enemy sensors and obscuring returns from real targets, US and allied forces can degrade the reliability of PLA sensors and, by extension, the confidence of PLA leaders in plans that depend on this targeting and assessment information. Decoys would predominantly be uncrewed vehicles, which could allow them to perform double-duty as elements of a passive or multistatic sensing network as described above.

The campaign prioritizes operations against SIGINT satellites, as shown in Figure 12, because they are likely the primary sensors in the PLA reconnaissance-intelligence system. Able to stare across wide areas, commercial and military SIGINT satellites can identify the rough location of hundreds of emitters at a time and determine their classification using characteristics such as frequency, pulse width (PW), pulse repetition frequency (PRF), or scan pattern. SIGINT satellites in a geostationary orbit (GEO), like those in Figure 11, can view almost an entire hemisphere at once. However, GEO satellites cannot locate emitters precisely because they only receive one line of bearing and the beamwidth of the emitter is widened due to the satellite being at a high altitude. Low earth orbit SIGINT satellites can receive multiple lines of bearing because they are

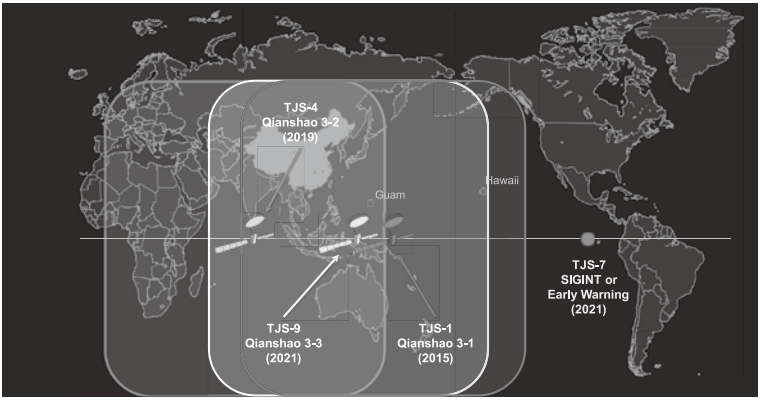
---

[39] Denghui He, Yuanhui Cui, Fangchao Ming, and Weiping Wu, "Advancements in Passive Wireless Sensors, Materials, Devices, and Applications," *Sensors*, Volume 23, Issue 19, 2023, Page 8200, https://doi.org/10.3390/s23198200.

[40] "Better camouflage is needed to hide from new electronic sensors," *The Economist*, March 29, 2023, https://www.economist.com/science-and-technology/2023/03/29/better-camouflage-is-needed-to-hide-from-new-electronic-sensors.

[41] Dylan Malyasov, "Russia Uses Advanced Camouflage to Hide Their Iskanders from Ukrainian Drones," Defense-Blog, April 19, 2022, https://defence-blog.com/russia-uses-advanced-camouflage-to-hide-their-iskanders-from-ukrainian-drones/; Sam Cranny-Evans, "The Role of Artillery in a War Between Russia and Ukraine," *RUSI Commentary*, February 14, 2022, https://rusi.org/explore-our-research/publications/commentary/role-artillery-war-between-russia-and-ukraine.

in motion relative to the emitter and are more numerous than GEO satellites, which affords them more precise location information.



Notes: All shown constellations are in geosynchronous (GEO) orbit.

Figure 11: PLA SIGINT satellite coverage[42]

Although US and allied forces can greatly reduce their detectability to SIGINT sensors using EMCON practices, sometimes radio communications and radar operations will be necessary. Ships, aircraft, and troop formations can use decoys operating away from actual forces to prevent these limited, but necessary, emissions from providing enemy forces actionable targeting information. Decoys can create confusion for enemy sensing and sensemaking by providing more numerous targets for assessment and tracking in lieu of, or in addition to, the real targets provided by necessary allied emissions. Knowing that false targets are present in the SIGINT constellation's view will lead operators to investigate each detection, slowing the sensemaking process and perhaps ceding the initiative to allied forces.

Realistic decoys will need to incorporate RF transmitters that can emulate at least some signals the actual platform is likely emit. A low-cost decoy is unlikely to have sufficient power to fully represent a large radar like the Navy SPY-1 or Army Patriot, but RF decoys can exploit creative tactics and new technologies to provide a realistic simulation. For example, radar operators seeking to avoid detection may operate their

---

[42] J. Michael Dahm, "Testimony before the U.S.-China Economic and Security Review Commission," March 21, 2024, https://www.uscc.gov/sites/default/files/2024-03/J.Michael_Dahm_Testimony.pdf.

systems at low power or use spot beams to avoid detection. A decoy operating in a contested environment could simulate a SPY-1 or Patriot operating in one of these less-demanding modes.

Waveform generation is the other significant challenge with RF decoys. To be versatile, a decoy may need to use a software-defined radio (SDR) to generate its signal. SDRs can be programmed to produce a wide variety of signal characteristics such as pulse repetition rate, pulse width, or frequency within the limitations of the antenna hardware. But SDRs also demand substantial power for processing, which increases depending on how versatile the SDR is intended to be.[43] US and allied forces should develop modular low-cost, low-power decoy transmitters that each specialize in a small range of signals that can be incorporated onto a variety of uncrewed systems.

While the power and waveforms of radars can be challenging to emulate, decoys can more easily create realistic radio communication signals. Radios—especially those carried by ground troops and vehicles—are small, low-power, and relatively inexpensive. Rather than building decoy emulators, US and allied forces should simply incorporate real radios into decoys to provide a high-fidelity deception for enemy SIGINT sensors.[44] Several companies are pursuing this approach in uncrewed vehicles that simulate armored vehicles or missile launchers.[45]

Navies are also experimenting with active RF decoys and defense companies are beginning to develop and field RF decoy systems designed for deception, rather than simply self-protection.[46] For example, Thales demonstrated a surface decoy that combined the company's Halcyon unmanned surface vehicle (USV) with the EW payload of the French Accolade airborne self-protection decoy, shown in Figure 12.[47]

---

43 Tore Ulversoy, "Software Defined Radio: Challenges and Opportunities," *IEEE Communications Surveys and Tutorials*, Volume 12, Issue 4, 2010, Pages 531-550. 10.1109/SURV.2010.032910.00019.

44 Walker Mills, "A Tool for Deception: The Urgent Need for EM Decoys," US Military Academy, February 27, 2020, https://warroom.armywarcollege.edu/articles/tactical-decoys/.

45 Remy Hermez, "To Survive, Deceive: Decoys in Land Warfare," War on the Rocks, April 22, 2021, https://warontherocks.com/2021/04/to-survive-deceive-decoys-in-land-warfare/.

46 David Tremper, "Unmanned Sea Surface Vehicle Electronic Warfare," *Naval Research Laboratory*, 2007, https://apps.dtic.mil/sti/tr/pdf/ADA518455.pdf.

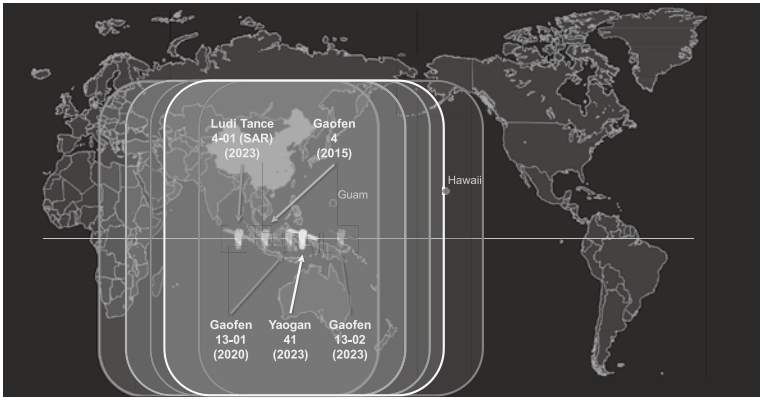
47 Thomas Withington, "Winning Accolades," Armada International, February 5, 2020, https://www.armadainternational.com/2020/02/winning-accolades/.

Figure 12: Thales Halcyon USV used in decoy experiments

While the majority of counter-SIGINT operations would rely on decoys, cyber operations could also be used to create false targets in the processing systems of the SIGINT constellation. For commercial SIGINT providers, these cyber effects could be introduced via a wired network, but military SIGINT constellations are likely firewalled from global communications networks like the Internet. As a result, allied forces may need to inject these cyber tools via an RF aperture, such as the SIGINT satellite's own antenna.

Countering imaging sensors

Faced with potentially large numbers of RF decoys, PLA operators would turn to imagery satellites, which provide the ability to scan large areas and obtain high-fidelity synthetic aperture radar (SAR) returns or visual and IR signatures. The PLA reconnaissance-intelligence system uses both electro-optical/infrared (EO/IR) and SAR imaging satellite constellations, as shown in Figure 13.



Notes: Gaofen and Yaogan satellites constellations use EO/IR sensors and Ludi Tance uses a SAR sensor. All shown constellations are in GEO orbit.

Figure 13: PLA SAR and EO/IR satellite coverage[48]

EO/IR and SAR sensors each have advantages and disadvantages. Because they are active sensors, SAR sensors can penetrate clouds and do not require sunlight or heat sources on the target to generate detections. SAR sensors also can provide greater precision for weapons targeting compared to EO/IR satellites that is require large and expensive sensors to achieve high resolution.[49] However, EO/IR satellites may enable classification and identification against a wider variety of targets because SAR sensors view the earth's surface from an angle, which can distort the radar image.[50]

Deceiving SAR

The most important difference between EO/IR and SAR imaging satellites for a counter-sensing and sensemaking campaign is their susceptibility to decoys and jamming. Lasers can disrupt visual and IR sensors. However, because these sensors are passive, the laser

---

[48] J. Michael Dahm, "Testimony before the U.S.-China Economic and Security Review Commission," March 21, 2024, https://www.uscc.gov/sites/default/files/2024-03/J.Michael_Dahm_Testimony.pdf.

[49] G. M. Koretsky, J. F. Nicoll, and M. S. Taylor, *A Tutorial on Electro-Optical/Infrared (EO/IR) Theory and Systems* (Alexandria, VA: Institute for Defense Analysis, 2013), https://www.ida.org/-/media/feature/publications/a/at/a-tutorial-on-e-lectro--opticalinfrared-eoir-theory-and-systems/ida-document-d-4642.ashx.

[50] Mark Ashby and Edmund Zelnio, "Multi-platform EO and SAR Fusion for Target ID," *Proceedings of SPIE 12095: Algorithms for Synthetic Aperture Radar Imagery XXIX*, paper 1209505, May 31, 2022, https://doi.org/10.1117/12.2624109.

operator would need to know from other sources the sensor's presence and exact location. SAR satellites can be detected and located by their emissions. And like other radars, SAR satellites could be disrupted by noise jamming or deceived by decoys that provide a false return emulating a different platform at a different location.[51]

Because it can use digital signal processing to manipulate the radar return, a SAR jammer could be smaller than the system or vehicle being emulated.[52] The Leonardo AN/ALQ-260(V1) BriteCloud countermeasure, shown in Figure 14, is an expendable decoy incorporating that provides a return to radar-guided missiles that looks like the defended aircraft.[53] Sweden's Saab recently began testing a similar decoy for its Gripen fighter aircraft that incorporates a propulsion system so it can draw a threat away from the defended aircraft.[54] And the Thales decoy USV shown in Figure 12 carries a jammer that could provide a radar return like that of the simulated ship.

Source: Leonardo

Figure 14: BriteCloud decoy simulating a defended aircraft

---

51 Hua Li, Zhenning Li, Kaiyu Liu, Kaijiang Xu, Chao Luo, You Lv, and Yunkai Deng, "A Broadband Information Metasurface-Assisted Target Jamming System for Synthetic Aperture Radar" *Remote Sensing, Volume 16,* Issue 9, 2024, Page 1499, https://doi.org/10.3390/rs16091499.

52 Dahai Dai, X. F. Wu, X. Wang, and Shunping Xiao, "SAR Active-Decoys Jamming Based on DRFM," in *Proceedings of the IET International Conference on Radar Systems* (Edinburgh: IET, 2007), pp. 1-4.

53 Steven D'Urso, "A Deep Dive Into BriteCloud Advanced Expendable Active Decoy," The Aviationist, July 6, 2021, https://theaviationist.com/2021/07/06/a-deep-dive-into-britecloud/.

54 Thomas Withington, "Decoy and Destroy," Armada International, October 7, 2020, https://www.armadainternational.com/2020/10/decoy-and-destroy/.

Although most of the radar decoys described above are intended to draw incoming weapons away from the defended platform, they could be repurposed to be decoys against satellite or airborne radars. In these counter-sensing and sensemaking use cases, the decoys would need to operate far enough from the defended platform for it to not attract attention toward actual US and allied forces.

Deceiving EO/IR

EO/IR satellites are more difficult to deceive compared to SAR sensors. As noted above, the defending force would need to know EO/IR sensors are in the area and their approximate location to either disrupt or decoy them. If available, lasers could disrupt EO/IR sensors regardless of the size of the system being protected. To deceive an EO/IR sensor, the decoy would need to have a similar size and shape as the system being emulated and have a comparable heat signature. Although the US and its Asian allies largely stopped widespread fielding of decoys after the Cold War, Eastern European US allies worried about potential Russian aggression continued R&D on decoys and fielding demonstration systems. Most of these decoys are inflatable, which makes them light and easy to deploy. Many incorporate radar-reflecting material to make them show up in radar searches as well.

Inflatable decoys like that shown in Figure 15 are built by the Czech company Inflatech and are likely being supplied to the Ukrainian military. In addition to providing a visual and radar signature to overhead sensors, newer inflatable systems like that in Figure 15 incorporate heaters to simulate the heat from engines or generators to deceive IR sensors. These signatures can appear realistic at ranges of more than several hundred yards away, making the decoys effective against overhead sensors on ISR aircraft or satellites.

Source: Inflatech

Figure 15: Inflatable decoy High-Mobility Artillery Rocket System (HiMARS)[55]

However, enemy UAVs may be able to approach inflatable decoys closely enough to distinguish them from real systems. For example, even if they incorporate radar-reflecting material, inflatable decoys lack the hard edges radars use to identify and classify a contact and the internal structure to allow accurately positioning heaters for realistic IR signatures.

Decoy developers are improving the fidelity of decoys while keeping their cost and complexity low enough that they can be deployed at scale and potentially lost without regret. Constructed, rather than inflated, decoys can provide the structure and power generation for more realistic decoys, like the wooden radar being built in Figure 16.[56] The US Army recently teamed with students from Georgia Institute of Technology to build working deception systems during a three-day "hack-a-thon."[57]

---

55 Associated Press, "Inflatable Tanks, Missiles: Czech Firm Makes Decoy Armaments," March 6, 2023, https://apnews.com/article/czech-decoys-war-ukraine-russia-inflatable-a9c478adb9d7ecaa615cb19b25f4833f.

56 Isabel Coles, "How Ukraine Tricks Russia Into Wasting Ammunition," The Wall Street Journal, October 2, 2023, https://www.wsj.com/world/how-ukraine-tricks-russia-into-wasting-ammunition-799ed95f.

57 "GTRI, Army Team Up for Decoy Hackathon," Georgia Tech Research Institute (GTRI), January 18, 2023, https://www.gtri.gatech.edu/newsroom/gtri-army-team-decoy-hackathon.

Figure 16: Decoy radar under construction at Metinvest in Ukraine

To effectively emulate an actual platform, a decoy will need to also behave and be protected like a real system. Therefore, mobility and camouflage—techniques used to protect real vehicles, ships, and aircraft from detection—would also need to be employed with decoy systems. Many of the ground decoys being deployed by Ukrainian or Russian forces can be moved to simulate a real mobile system, but this creates risk for troops conducting the movement. To achieve greater realism and reduce risk to forces, several companies are fielding uncrewed vehicles that can either tow or carry visual and IR decoys or are themselves able to emulate a real system to enemy EO/IR sensors, as shown in Figure 17.[58]

[58] Raider Targetry, "ATTLAS," https://raidertargetry.com/attlas-3/; Nick Reynolds, 'Heavy Armoured Forces in Future Combined Arms Warfare', *RUSI Occasional Papers*, 12 December 2023, https://www.rusi.org/explore-our-research/publications/occasional-papers/heavy-armoured-forces-future-combined-arms-warfare.

Source: Raider Targetry

Figure 17: The Raider Targetry Mobile Moving Target System, which combines an uncrewed ground vehicle with a rigid target

Camouflage provides additional benefits beyond simply improving the quality of a decoy's simulation. If used on both real and decoy systems, camouflage can make differentiating between them more difficult and allow lower-fidelity decoys to be effective. Many companies are fielding camouflage that works across multiple regions of the electromagnetic spectrum, such as the Saab Barracuda family of camouflage systems.[59]

Denying sensor fusion

US and allied decoy and deception operations will not be perfect. Decoys will not perfectly represent the emissions or behavior of real platforms and militaries will have difficulty fielding and operating visual or IR decoys for larger platforms like ships and aircraft. As a result, US and allied forces will face the risk of PLA operators, aided by AI algorithms, using inputs from multiple sensor types to determine real from false targets. This process is called sensor correlation when multiple detections are associated with the same target. With the advent of modern data processing, operators often now pursue sensor fusion, which combines data from multiple sensors to create a single target. Sensor correlation can help reveal which sensor contacts could be real or fake. Sensor fusion could allow attackers to create high-quality tracks that can be used for engagement

[59] Saab, Barracuda MCS, Saab, https://www.saab.com/products/mcs-mobile-camouflage-system.

despite the defender's attempts at jamming and obscuring.[60]

The PLA reconnaissance-intelligence system would likely attempt to correlate or fuse target tracks from space-based sensors with those from ground-based radars and passive RF receivers on the PRC mainland, complemented by airborne and shipboard sensors deployed in China's near abroad. The decoys, jammers, and camouflage US and allied forces use against SIGINT, SAR, and EO/IR satellites would be effective against similar sensors deployed ashore or on aircraft. However, ground, ship, and aircraft sensors would likely have different characteristics and view US and allied forces from different and more unpredictable angles compared to space-based sensors. This would make effective decoy and jamming operations more challenging.

While seemingly simply in theory, sensor fusion is difficult in practice. Data formats, refresh rates, and the characteristics associated with detections differ widely between sensor types. Differing levels of latency can make reports of the same contact from multiple sensors appear to be of different targets. And data from deployed sensors depend on RF communications that are subject to environmental conditions and jamming or electronic deception.[61]

Allied forces can exploit the difficulty of sensor fusion by hindering the PLA reconnaissance-intelligence system's ability to fuse data from multiple sensors in real time. As shown in Figure 18, decoys would create false SIGINT, SAR, and EO/IR targets. When airborne early warning (AEW) aircraft are sent to investigate, their sensors are obscured by jammers and their communications blocked by small UAVs with EW systems. SAR jammers would hide the real ships behind a wall of noise in the SAR satellite's frequency range.

The decoy and jamming operations shown in Figure 18 could predominantly be done using uncrewed systems. When emulating a ship applying EMCON practices, a USV would only need emit low radio or radar power levels to fool a SIGINT satellite or shore-based listening station. SAR satellites operate at long range and the power reaching the earth's surface is within the level possible from an USV. And USV-borne radio or

---

[60] Joseph Peri, "Approaches to Multisensor Data Fusion," Johns Hopkins University Technical Digest, 2001, https://secwww.jhuapl.edu/techdigest/Content/techdigest/pdf/V22-N04/22-04-Peri.pdf/; Ashraf M. Aziz, "Fuzzy Track-to-track Association and Track Fusion Approach in Distributed Multisensor–multitarget Multiple-attribute Environment," *Signal Processing*, Volume 87, Issue 6, 2007, Pages 1474-1492, ISSN 0165-1684, https://doi.org/10.1016/j.sigpro.2007.01.001.

[61] S. Hamed Javadi and Alfonso Farina, "Radar Networks: A Review of Features and Challenges," *Information Fusion*, Volume 61, 2020, Pages 48-55, ISSN 1566-2535, https://doi.org/10.1016/j.inffus.2020.03.005.

radar jammers working against a terrestrial system like an AEW aircraft or ground-based HF radar can compensate for their lower power levels by more closely approaching the targeted system.

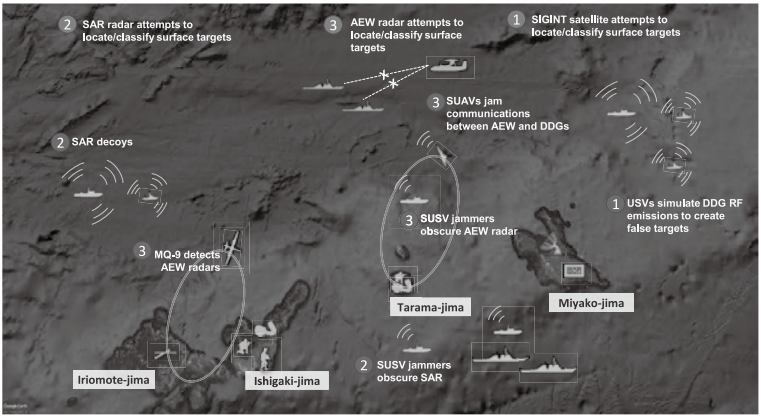


Figure 18: Lines of effort in notional counter-sensing and sensemaking campaign

Jammers like those shown in Figure 18 would also be useful for injecting cyber tools into enemy networks and systems. Deployed aircraft and ships may not be connected to the wide internet and the PLA has likely hard-wired its ground-based radars and SIGINT sensors to reduce their susceptibility to jamming and interdiction. However, this still leaves them vulnerable to a "front-door" attack that injects a cyber tool into the system's antenna.

Against a major power like the PRC, US and allied forces are unlikely to prevail in a salvo competition. These militaries and their leaders will need to focus on deterring conflict, not just hoping to win the war when it comes. The DoD will need a robust non-kinetic capability development process and industrial base to sustain a peacetime counter-sensing and sensemaking campaign that could dissuade PRC aggression.

4. Conclusion

The US military is no longer broadly dominant against all adversaries across all scenarios. To regain an edge against peer competitors like China, US forces will increasingly need

to rely on counter-sensing and sensemaking operations. In addition to reducing the effectiveness of enemy fires in wartime, these operations can undermine the confidence of adversary commanders and leaders in their ability to accurately target allied forces and predict future allied operations.

To stay ahead in the sensing and sensemaking competition, US and allied militaries will need to improve their own C3ISR capabilities through improved interoperability, new proliferated LEO satellite constellations, and continued advancements in uncrewed systems on, under, and over the water. More important, allied forces will also need to field a large and diverse array of non-kinetic cyber and EW effects that can degrade adversary efforts to see and understand their operational picture.

The DoD's non-kinetic capabilities are arguably second to none. However, the relatively small number of exquisite "silver bullet" effects US forces develop to meet ambitious requirements may only be useful in wartime, when their expenditure can have maximum impact. To deter conflict, US and allied forces will need non-kinetic effects they can employ during peacetime competition to show opponents that their C3ISR capabilities may be unreliable in combat.

A sustained peacetime effort to dissuade aggression through non-kinetic means will depend on a deep magazine of cyber and EW effects that are unlikely to cause widespread or permanent damage. These "brass" or "bronze" bullets would incur a lower risk of escalation compared to their more damaging counterparts and likely could be fielded in greater numbers because they may need less-challenging access to adversary systems or networks and could employ common attack methodologies.

Competition-phase non-kinetic effects will also need to be unexpected, even if they are usually less dramatic than attacks like the Stuxnet virus or the supply chain attack on Solar Winds software.[62] Predicable non-kinetic effects are desirable in uses like self-protection jammers, but in counter-sensing and sensemaking could ironically act to encourage an opponent by implying its C3ISR systems can address allied cyber and EW attacks. US and allied forces could achieve surprise in their non-kinetic capabilities through novel coding or waveforms in the effect itself as well as through the entire effects chain's delivery mechanism, target, or tactics.

Achieving a deep magazine of surprising non-kinetic effects will require different

---

[62] National Public Radio, "A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack," NPR.org, April 16, 2021, https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack; David Kushner, "The Real Story of Stuxnet," *IEEE Spectrum*, February 26, 2013, https://spectrum.ieee.org/the-real-story-of-stuxnet.

approaches to the EW and cyber supply chains and a defense industrial base that is incentivized to build capabilities at scale and pursue independent innovation. Using existing acquisition and contracting authorities, the proposed consortium and process of this report would provide a "sandbox" for industry to develop and assess new approaches and effects using government-approved intel and models. By buying the most promising non-kinetic capabilities at competitive prices, the government would produce a "pull" for new effects that would incentive further industry-led innovation. An example of such a process is shown in Figure 19.

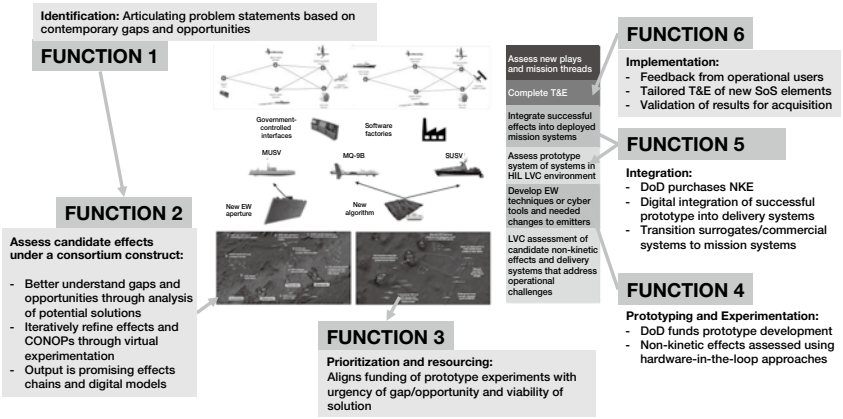


Figure 19: Potential future non-kinetic capability development process

US and allied militaries can no longer depend on their general superiority to deter and defeat aggression. Recent events in multiple theaters highlight how regional powers, transnational organizations, and peer competitors all are gaining the ability to stress or overmatch US and allied forces in their regions. Non-kinetic effects offer a way for the DoD to take advantage of an area of US and allied strength and regain the ability to dissuade opponents through sustained efforts to undermine their sensing and sensemaking. Exploiting these strengths, however, will require buying and delivering non-kinetic capabilities in ways more akin to their kinetic counterparts.