The wreckage of a Russian SU-35 fighter shot down by the Ukrainian Air Force burns on the ground in the Kharkiv region circa 3 April 2022. Ukrainian forces captured the Russian pilot despite attempts by Russia to recover him by helicopter rescue. (Photo courtesy of the Ukrainian Ministry of Defence)

The Russia-Ukraine Conflict Laboratory

Observations Informing IAMD

Col. Todd A. Schmidt, PhD, U.S. Army

The Russia-Ukraine war is, in many ways, an open laboratory providing insights into what war and large-scale, multidomain combat operations may look like in the decades ahead. Allies and adversaries are studying the conflict closely, observing how new technologies are being militarized and used to gain advantage. Countless papers, studies, and articles will continue to be written as the Russia-Ukraine

conflict continues to rage. This article focuses broadly on six areas, warfighting functions, through the specific lens of integrated air and missile defense (IAMD) as well as through the wider lens of large-scale, multi-domain combat operations.[1]

I outline observations that will, hopefully, inform lessons that endure scrutiny in relationship to the current conflict as well as in relationship to the future operational environment. This operational environment is composed of multiple domains that include air, land, sea, space, and cyberspace. Each domain can be seen through multiple dimensions—physical, human, and information.[2] The overall intent of this article is to provide a catalyst for discussion and debate about our collective ability to enhance the defense of the United States and its allies and partners in the way ahead.

Scene Setter

Consider the following battlefield exchange in the Russia-Ukraine war that occurs over a twenty-four-hour period. It includes a wave of Shahed-136 attack unmanned aircraft, Killjoy nuclear-capable hypersonic missiles, Kh-101 air-launched cruise missiles, supersonic Kaliber cruise missiles, Iskander ballistic missiles, reconnaissance drones, Lancet loitering munitions, and barrages of conventional artillery and missiles. The attacks occur deep in friendly territory, targeting civilians, critical infrastructure, and urban government centers. In addition to these munitions, the adversary launches simultaneous cyberspace attacks and psychological operations that disrupt electrical grids, jam cellular networks, and replace internet and telecommunications capabilities with adversary-controlled services.

In response, friendly forces return limited counterfires, targeting enemy command-and-control (C2) nodes easily identifiable by their unique formations, equipment, and electronic signature. These C2 nodes remain static for long periods, unable to operate effectively on the move. They are unmasked and fully transparent to friendly intelligence, surveillance, and reconnaissance (ISR) capabilities. This makes the enemy's logistics exceptionally vulnerable to attack. Leadership is easily targeted and pays an existential price of attrition. The momentum of enemy attack forces is halted as dispersed, well-masked friendly forces rapidly return counterbattery fire and mimic enemy tactics.

This real-world vignette provides a relatively recent example of how aerial weapon systems converging with attack capabilities in multiple domains can overwhelm an opponent's defenses and ability to C2 forces in the field and on the front lines. It also demonstrates what U.S. Army authors have described as "The Graveyard of Command Posts."[3] Nearly 20 percent of Russian casualties are seasoned, experienced, highly trained officers.[4] This population of leaders is paying an incredible price. As of the drafting of this article, over 1,500 and counting have paid with their lives through the "relentless assault on command and control" posts through systematic attacks "at scale and across all tactical echelons."[5] Attacks on both sides have severely degraded the ability to mobilize, deploy, and conduct centralized planning and coordination, slowed momentum of operations, and prevented the ability to leverage any success or gains on the battlefield.

Command and Control

In a recent unclassified briefing, Lt. Gen. Chris Donahue, 18th Airborne Corps commanding general, shared lessons learned from his headquarters' recent deployment to Europe. Challenges Donahue outlined related to the speed and velocity of available data in relation to the speed and velocity of modern conflict—both are advancing very rapidly. Intuitively, the military that can leverage data the fastest, at speed and echelon, will have strategic, operational, and tactical advantages. Organizations that can quickly integrate data into planning, adapt operations on the ground, and persist through grueling conflict will win (much like the lessons learned by Joint Special Operations Command in Iraq and Afghanistan).

For allies and partners, this means that the passing and sharing of data is imperative. We know we can "pass data," but "sharing data" remains a hurdle. It is a strategic national policy puzzle that must be solved during

Col. Todd Schmidt, PhD, U.S. Army, is director of Army University Press at Fort Leavenworth, Kansas; a nonresident Fellow with the U.S. Military Academy's Simon Center for the Professional Military Ethic; and an AUSA Leadership Fellow. He is the author of the book *Silent Coup of the Guardians: The Influence of U.S. Military Elites on National Security*.

The Army Integrated Fires Mission Command and soldiers of the 3rd Battalion, 43rd Air Defense Artillery Regiment, conduct a missile flight test with the Integrated Air and Missile Defense Battle Command System at White Sands Missile Range, New Mexico, on 17 November 2022. The test was deemed a success. (Photo by Darrell Ames, Program Executive Office Missiles and Space)

relative peace, not in the midst of high-intensity conflict. These problems can be investigated for potential policy solutions in events like those hosted by Nimble Titan.[6] With an alignment of national policies between allies and partners, the hurdles to information sharing and integration of platforms can be overcome. As of today, however, the United States and its allies and partners are significantly challenged to provide C2 in a combined-joint fight, and the first solutions must be solved by common national policies that address this challenge in a multilateral context.

Secondly, a 2022 report from the Royal United Services Institute for Defense and Security Studies in the United Kingdom describes observations from British and NATO militaries related to events in Ukraine. One of the many takeaways is that the modern battlefield is increasingly transparent: "There is no sanctuary in modern warfare."[7] Static systems will be relentlessly attacked. This raises the question, How expeditionary and mobile are some strategic and operational IAMD systems and C2 nodes in our current inventory? Our most capable defeat mechanisms are also our least mobile. Dispersion of highly mobile capabilities is imperative to survivability. The ability to maneuver under surveillance and fire is critical. Redundant, agile, rapidly deployable capabilities are essential to minimizing vulnerability to enemy detection and targeting.

Indeed, persistent identification, surveillance, and targeting of systems is a fundamental component of "systems warfare," a key adversarial strategy.[8] Systems warfare is identifying and isolating or destroying critical subsystems and components to degrade or destroy an opponent's overall system and capability.[9] This dynamic concept requires offensive measures to attack an opponent's system and defensive or countermeasures to protect against attack. To minimize risks, ensuring seamless connectivity across threat detection platforms (terrestrial and space), C2, and IAMD systems is crucial. This raises an additional question: What are our current capabilities to swarm satellites in the space domain and defeat adversarial swarming capabilities? These capabilities and integration must be real-time and effective because the timeline between the launch of a threat and impact is extremely short.

An example of system warfare is the defense of command posts and IAMD C2 at each echelon. For the United States and its allies, command posts, particularly in the IAMD fight, are exceptionally vulnerable to attack—an easy target for our adversaries because of the magnitude of multispectrum electromagnetic transmissions, generators, vehicles, personnel, and other logistical support requirements. Western command posts are no longer a sanctuary, having become less mobile and less survivable in the context of modern large-scale, multidomain combat operations.[10]

Likewise, tactical and operational units must decentralize operations and C2, empowering leaders at every level to exercise disciplined initiative as C2 nodes are heavily targeted to destroy, disintegrate, isolate, dislocate, and disrupt operations.

Future command posts must have a smaller, less detectable signature. C2 nodes must be more resilient, mobile, and agile. These C2 nodes and electromagnetic signatures must also be easily masked. Deception capabilities should allow for blending allied military signatures into the "white noise" of populated urban centers. However, this capability must be developed in accordance with the rules of land warfare.

Finally, future combined-joint doctrine needs to direct C2 nodes and leaders to be less reliant on the physical dimension and far more capable of leveraging the human and information dimensions through artificial intelligence (AI), augmented and virtual reality, and analysis of large amounts of data. This translates into C2 nodes that may partially exist in a virtual construct, aggregating and integrating functions, processes, and capabilities without depending on the physical (and targetable) construct of people, equipment, and the support capabilities required to sustain them.[11]

Fires and Maneuver

To support fires and maneuver, from an IAMD perspective, offensive and defensive unmanned aircraft systems (UAS) and counter-UAS capabilities must be fielded at echelon. While UASs will have an exceptionally critical role in future conflicts, they will also be subject to exceptionally low survivability rates. Multinational, jointly developed IAMD systems using interoperable, off-the-shelf solutions offer flexible and scalable ways for nations to strengthen IAMD in an efficient and cost-effective way.

It is imperative that the United States and allies possess fires capabilities and technologies that provide both precision and volume. Epic "artillery duels" and requisite air and missile defense "umbrellas" across an expansive and deep battlespace will be a requirement and attribute of future war. This requires inexpensive, high-capacity multinational industrial manufacturing capabilities that allow for stockpiling of these critical, revolutionary systems that provide for ISR, target acquisition, and fire control; can be designed as a munition; and support nearly all warfighting functions with developing capabilities in logistics and resupply.

Second, we must continue to develop and train to utilize systems and subsystems that ensure an "any sensor, best shooter" capability, particularly for IAMD. Combined-joint training events, at the Army Corps level, must be expanded to rehearse and exercise targeting and airspace management procedures in an exceptionally fluid and contested environment. Various weapon platforms such as UASs, fighter jets, ground-based systems, maritime air defense assets, information technology systems, and satellites will be utilized to establish defense synergies and layer interconnected and overlapped spheres. The aim of alliance IAMD policy and strategy must be to challenge and complicate adversary efforts to overcome these friendly defenses.

IAMD must be able to respond promptly to an array of threats at multiple ranges and altitudes. These capabilities must be designed to prevent successful adversary attacks and to prevent friendly IAMD systems from being overwhelmed, whether through technical or quantitative superiority.[12] More importantly, but not fully addressed in the scope of this article, will be the component of leadership.

Third, as we have observed, Russia has dedicated immense resources to targeting and destroying Ukrainian IAMD systems because of their exceptional success in shooting down Russian aircraft and munitions. The success of Ukrainian air defenses has been a strategically and internationally embarrassing and politically damaging coup. The lesson for the United States and allies is that dispersion and protection of IAMD assets, without losing C2 capability, is imperative.

To improve the survivability of friendly forces, allied IAMD concepts and capabilities must be hardened and operationalize basic principles such as speed, mobility, protection, defense-in-depth, and overlapping fires. Because adversaries will engage in the full spectrum of conflict across all dimensions and domains, allied capabilities may be disrupted and degraded before the outbreak of kinetic conflict. National will and resilience will be challenged before the first military units or service members deploy from their home stations; before any first shots may be fired.

NATO's IAMD mission, as outlined in the 2021 Brussels Summit communiqué, describes an all-encompassing strategy that aims to counter IAMD

threats from all strategic directions through a 360-degree approach.[13] However, only a limited number of capabilities have been allocated to this mission thus far. Introducing a long-range system like THAAD (Terminal High Altitude Area Defense) or Arrow 3 would not only expand alliance capacity but also broaden the range of capabilities, conveying a strong deterrent message. This, of course, necessitates a delicate balance among political, strategic, military, industrial, and economic considerations.[14] Similar policies must be implemented in the Pacific theater.

Intelligence

Clear from observations of the Russia-Ukraine war, IAMD operations occur in all domains. Likewise, IAMD systems will be contested by peer competitors, kinetically targeted and attacked from the ground, air, sea, space, and cyberspace. Increasingly, IAMD systems and personnel will also be targeted through the electromagnetic spectrum and the information and human (or cognitive) dimensions as conflict and capabilities evolve and improve.

Intelligence related to and informing IAMD operations must help leaders understand the operational environment at echelon. As previously noted, we must assume we are under constant, persistent observation and targeting. We must have the capability to operate at the smallest element possible, enabled by resilient C2 systems and networks, including information and data sharing.

Information and data sharing is a key strategic, operational, and tactical enabler and asset. It is not a "zero-sum" asset that is lost when given to an ally. Therefore, the willingness to exchange information and data is a prerequisite for effective IAMD. Moreover, in contrast to sharing and common procurement of weapon systems to partners, IAMD information and data sharing does not impede the capacity of assets but, by contrast, enables partners. There is no loss of information and data but, rather, increased leverage of this critical component across an IAMD system. These imperatives can force multiple dilemmas on our adversaries while providing allies with decision dominance.

To achieve superiority, as previously mentioned, training events and exercises must combined-joint in nature and increasingly incorporate AI to aid in rapid decision-making, target acquisition, and engagement processes. Current and future alliance considerations will also need to address the development and incorporation of virtual reality or augmented reality capabilities into multidomain operations and IAMD.

Intelligence will be further enabled through the convergence of multiple technologies and capabilities. This convergence is intended to create revolutionary, multidomain, interoperable, and seamlessly integrated effects within allied air and missile defense against a peer or near-peer adversary. The U.S. military defines convergence in its new military operations doctrine (Field Manual 3-0, *Operations*) as a spectrum of outcomes that can be created by an orchestrated, simultaneous employment of capabilities across multiple domains against a combination of key targets.[15] Convergence creates effects against an adversary's formations, systems, processes, and key individuals and publics across time, space, and geography.[16]

For allies, multinational convergence of technologies and weapon systems and multifaceted approaches can offer flexible and scalable options that create unforeseen outcomes wherein the sum of the advantages and effects is far greater than any individual technology, capability, or system. The intent is to disrupt an adversary and create multiple, simultaneous dilemmas for an enemy combatant while creating exploitable opportunities for friendly forces. This increases freedom of action, allows for consolidation and expansion of gains, and results in favorable outcomes for friendly forces.

To manifest the principles and reality of convergence, particularly in intelligence and IAMD, Pacific allies should expand observation and participation in Project Convergence and the upcoming 2024 Capstone Event 4 in the United States. While previous capstone events have incorporated cruise missile threats, the 2024 Capstone 4 event will, for the first time, incorporate ballistic missile threats. The intent will be to use combined-joint exercises such as Pacific Pathways to test new capabilities and attempt to understand and solve persistent information sharing, data transfer, and platform integration challenges that have plagued previous events.[17]

As previously noted, allies must enact common policies that promote integration and interoperability as a critical component of modernization. Too often, national caveats and policies prevent combined-joint interoperability. In the future, combined-joint operations

U.S. Army Futures Command's Artificial Intelligence Integration Center tests an Inspired Flight 3 artificial intelligence drone 27 October 2022 during Project Convergence 2022 at Fort Irwin, California. Project Convergence 22 experimentation incorporated technologies and concepts from all services and from multinational partners, including in the areas of autonomy, augmented reality, tactical communications, advanced manufacturing, unmanned aircraft, and long-range fires. (Photo by Spc. Lessitte Canales, U.S. Army)

must be well-rehearsed, if not routine. To achieve the potential revolutionary capabilities enabled by the convergence of technologies, multinational acquisition, integration, and interoperability with allies cannot be an afterthought. Peer competitors and adversaries will persistently challenge the alliance across all domains, searching for and exploiting identifiable gaps, seams, and weaknesses to fracture and disintegrate friendly coalitions. The alliance should aspire to compel the enemy to fight the alliance's preferred fight. Likewise, it must avoid being dragged into fighting the preferred fight of the enemy.

Protection and Sustainment

Another observation of the Russia-Ukraine conflict is the unrelenting contest between adversaries in multi-domain operations. This contest will challenge historical norms and past theories of war and victory. It will target civilian populations in the information and cognitive domains in ways that the current Russia-Ukraine war hints but, in total, remains unforeseen. Future contests will require opponents to fight their way to the fight, meaning military targets will be engaged before deployment. This will challenge national will, damage national infrastructure, and stress national mobilization.

Allied countries must accept that they are under constant and persistent surveillance. There will be nowhere to hide from enemy targeting. Militaries will be targeted across every domain, at home or abroad, as will their families and friends, through capabilities that include developing capabilities in AI, cyber, drones, robotics, augmented reality, hypersonic vehicles, and space-borne systems. The law of land warfare, as we may know it, must remain relevant to these changes.

From a more specific IAMD perspective, using a UAS enabled by AI is revolutionizing warfare. UASs are a game changer. Small, inexpensive, and increasingly lethal, this AI-enabled capability will only become more challenging. Allied IAMD efforts must focus on and expand detection capabilities and countermeasures

to defend against UASs, particularly in the electromagnetic spectrum. Critical to this effort will be terrestrial, sensors-based platforms, space-based satellite imagery, and human-enabled crowdsourced intelligence. Additionally, allies must ensure that they maintain capability and advantage in other low-cost measures such as tactical air defense, deception capabilities, and shroud technology.

responsive doctrine enabled by common national policies. Finally, allies must have the right capability and capacity to confront and defeat potential competitors and opponents.

Policy. When crisis or conflict develop, barriers to allied integration are often quickly overcome. However, in the future combined-joint operational environment, where the velocity of war is exponentially increased,

> Archaic, costly, and overly political, protective, and bureaucratic processes and decision-making frameworks are self-defeating encumbrances.

Sustainment of IAMD platforms in large-scale, multidomain combat operations will be critical, particularly in the Pacific region. Logistical planning assumptions need to be frequently assessed. Stockpiling munitions with long lead times for production is a key consideration. Ammunition and equipment need to be reevaluated based on the requirements of the future operational environment, taking into consideration cost, size, mobility, lethality, survivability, and sustainability. Finally, allies will not have the convenience of choosing when and where it will fight. It must be prepared to engage in exceptionally contested, expeditionary environments with no interior lines and exacerbated long, vulnerable exterior lines.

A Way Ahead

As stated in the introduction, there are countless observations being gathered from the Russia-Ukraine war. Potential future adversaries are observing and noting these same lessons, particularly in the Pacific theater. At the most basic level, allies must preserve the capability and freedom to maneuver at scale and echelon, and be prepared to overcome massing or swarming efforts, particularly in the IAMD fight. Opponents should be assumed to have massive inventories of threat capabilities that will be choreographed and deployed across every domain and dimension of war. With this premise, it is imperative that allies have the right policies in place. Allies must develop and train on common,

waiting for conflict to occur and delaying the removal of barriers and hurdles to allied integration and interoperability will have catastrophic consequences. National information and data-sharing disclosure policies must reflect current and future realities.

Archaic, costly, and overly political, protective, and bureaucratic processes and decision-making frameworks are self-defeating encumbrances. Allies can no longer afford disjointedness that can feed irrelevance and, at worst, massive destruction and tragic casualties. Information and data sharing, and interoperability in periods of crisis and high-intensity conflict require highly responsive policy and decision-making processes backed by common, shared procurement vision; shared resource commitment; and operationalization by military power and forces that are indoctrinated, trained, and conditioned for combined-joint coalition action.

Specifically, national policies among allies must incentivize collaborative efforts and align to ensure and enable real convergence potential at scale and echelon. Investment consortiums in research, development, and testing of the defense applications of AI, "big data," cyber capabilities, augmented reality, drones, robots, hypersonic vehicles, and space capabilities must take on a "whole of alliance" priority and approach. Likewise, national and allied investments in human capital and force structure must reflect and be commensurate with capability development. Events like Nimble Titan are a great catalyst to achieving these aspirations.[18]

Doctrine and training. A key observation of the current Russia-Ukraine conflict is that professional Western-style militaries that are highly trained, educated, experienced, proficient, competent, and well-equipped can defeat opposing, less professional military forces, even if vastly outnumbered. In contrast, when U.S.-NATO forces are advising and assisting foreign militaries, it is imperative to consider that Western-style doctrine and training may not be optimal with partners that do share similar military institutional culture and learning style. This was a key finding in a recent public briefing by the U.S. Army Air Defense Artillery School at the 2023 Association of the United States Army (AUSA) Annual Conference in Washington, D.C. In other words, as U.S. alliances and partnerships expand, how we train and fight must be adaptable and considerate of foreign military culture, knowledge, learning, and professional development, particularly as the United States seeks to expand its network of allies and partners in the Pacific.

For historic U.S. allies and partners in the Pacific, however, there should be a clear intention to create fully interoperable, theater-wide air and missile defense systems through common acquisition programs. To achieve this objective, more than common policy and proportional investment are required. Policy and investment must be reflected in common doctrine and training. Pacific allied forces, whether forward stationed or regionally aligned, must be well-versed and practiced in common doctrine and training, especially if there are doctrinal differences at the national or military service levels.

Observations from the Russia-Ukraine war demonstrate the profound importance of combined-joint operations, mobility and logistics, dispersion of forces, and redundant C2 capabilities at scale and echelon—all under protection of a well-integrated, interoperable, allied-empowered IAMD umbrella. Likewise, doctrine and training must be responsive to these fast-changing dynamics of current and future

The Northrup Grumman and Shield AI V-BAT is one of five project agreement holders for the Future Tactical Unmanned Aircraft System (FTUAS) Increment 2 rapid prototyping effort. The FTUAS is the Army's premier vertical take off and landing unmanned aircraft modernization effort. Shield AI and Sentient modified the V-BAT with AI imagery to detect and classify machine-invisible targets on the move. (Photo courtesy of Shield AI)

operations. If a target can be found, it can be degraded or killed.

Lastly, urban centers, rear areas of operation, and C2 nodes will be under persistent targeting and attack in an effort to disrupt operations, undermine civilian spirit and will, and destroy the ability to conduct integrated, combined-arms warfare. Opponents will be in persistent information warfare. Cyber and telecommunications capabilities will be targeted, taken hostage, or mimicked and ghosted to disrupt communications. Cyber and information will also be used to contest the cognitive domain, creating and achieving psychological effects and advantages, and deceiving adversary leaders, formations, and publics. Doctrine, training, and capability development in IAMD operations must take these asymmetric threats into account.

Capability and capacity. From an IAMD perspective, achieving air supremacy or superiority will not be fully achievable. At best, friendly forces must field a combination of capabilities that ensure enemy forces and capabilities are insufficient to prejudice friendly operations.[19] Active air and missile defense capabilities must be able to defend against and withstand pulse attacks, hypersonics, and swarms (from both UASs and satellites), and effectively engage in counter-UAS fights. Friendly forces must reinforce passive measures that reduce heat, electromagnetic, and optical signatures by emphasizing concealment, camouflage, obscuration, and deception, whether through conventional tactics and techniques or future "hider" capabilities such as shroud technology.

Many, if not most, IAMD capabilities come with high price tags due to the cost of research, development, and testing. However, the military-industrial complex should adopt a novel approach to capability development that necessarily emphasizes affordability. This will be incredibly challenging in a free market, capitalist system, but it is achievable with the appropriate incentives and capability development strategies. However, if allied forces and formation are to be prepared to face the massive inventories of low-cost capabilities being developed by our adversaries, we should not depend on defeating $100 drones with $1 million munitions.

Conclusion

Imagine the dynamic principle of convergence applied to IAMD in the context of the Pacific theater. The challenges can seem to be insurmountable. With the rapid evolution of adversary capabilities competing with allied aspirations of decision dominance, maintaining relevant policy has fallen behind, leaving easily exploitable gaps and seams in national policies and across multidomain environments. This requires a top-down, alliance-wide directed effort that aligns information and data-sharing policies with allied integration priorities. Allies must ensure that formal agreements, interactions, shared systems, and capabilities are not overly encumbered or unnecessarily stymied by archaic policies and processes from a bygone era.

To succeed, allies must be more persistent and serious about improving information and data sharing, common weapons system acquisition policy, integration of national systems, and interoperability in training and operations, whether in peacetime, crisis, or conflict. Information and data-sharing barriers that prevent or overly constrain allied integration come in all shapes and sizes. Granted, there are legitimate concerns related to the classification and protection of sensitive information and data. It is imperative, however, that the puzzle of policies that prevent information and data sharing be navigable if not fully solved.

Allied efforts must facilitate integrating a broad range of air and missile defense systems. Furthermore, policy must address and ensure alignment of allied military doctrine, operations, training, logistics, and more. Failure to remove barriers now to allied integration in the current and future operational environment will prove to be disastrous and expensive and cannot wait until new conflict erupts to be addressed. The United States must be a central leader and partner in this effort.

In conclusion, the observations and recommendations presented in this article can revolutionize how Pacific allied militaries operate and wage war, particularly in the IAMD domain. To succeed, however, requires a common vision of procurement, integration, and interoperability of joint services and capabilities, as well as combined, allied services and capabilities. There is still a long way to go in achieving these goals and objectives. The Russia-Ukraine war signals that large-scale, multidomain combat operations remain a distinct and ever-present threat from a disruptive adversary. This should be a reminder, catalyst, and accelerant for action. ■

DISCLAIMER: *The information and opinions expressed in this article are unclassified, found in open-source media, and do not reflect the policies or opinions of the government or military institutions of the author's parent nation and organizations.*

Notes

1. Field Manual (FM) 3-0, *Operations* (Washington, DC: U.S. Government Publishing Office, 2022), 2-1. Warfighting functions are composed of command and control, movement and maneuver, fires, intelligence, protection, and sustainment. "Multidomain operations are the combined arms employment of [combined and joint capabilities] to create and exploit advantages that achieve objectives, defeat enemy forces, and consolidate gains [within each domain]" (ibid., 3-1).

2. Ibid., 1-18, 1-21–1-23. A domain is "a physically defined portion of an operational environment requiring a unique set of warfighting capabilities and skills." Dimensions span across or through these domains. Other domains may include the cognitive domain and the electromagnetic domain.

3. Milford Beagle, Jason C. Slider, and Matthew R. Arrol, "The Graveyard of Command Posts: What Chornobaivka Should Teach Us about Command and Control in Large-Scale Combat Operations," *Military Review* Online Exclusive, 28 March 2023, https://www.armyupress.army.mil/journals/military-review/online-exclusive/2023-ole/the-graveyard-of-command-posts/.

4. Ibid.

5. Ibid.

6. Joint Functional Component Command for Integrated Missile Defense, "Nimble Titan Event to Explore IAMD Issues, Potential Solutions," Defense Visual Information Distribution Service, 23 October 2023, https://www.dvidshub.net/news/456319/nimble-titan-event-explore-iamd-issues-potential-solutions.

7. Mykhaylo Zabrodskyi et al., *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022* (London: Royal United Services Institute, 30 November 2022), 2, https://rusi.org/explore-our-research/publications/special-resources/preliminary-lessons-conventional-warfighting-russias-invasion-ukraine-february-july-2022.

8. Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare* (Santa Monica, CA: RAND Corporation, 2018), https://www.rand.org/pubs/research_reports/RR1708.html.

9. Ibid., 28.

10. Samuel Northrup, "New Army Vehicles Being Developed to Counter Modern Threats," Army.mil, 3 April 2019, https://www.army.mil/article/219567/new_army_vehicles_being_developed_to_counter_modern_threats; see also Zabrodskyi et al., *Preliminary Lessons in Conventional Warfighting*.

11. Beagle, Slider, and Arrol, "Graveyard of Command Posts."

12. Sven Arnold and Torben Arnold, "Germany's Fragile Leadership Role in European Air Defence: The Need for Adjustments at All Levels of the European Sky Shield Initiative," SWP Comment No. 6 (Berlin: German Institute for International and Security Affairs [SWP], February 2023), https://www.swp-berlin.org/publikation/germanys-fragile-leadership-role-in-european-air-defence.

13. "Brussels Summit Communiqué: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 14 June 2021," NATO press release no. 086, last updated 1 July 2022, https://www.nato.int/cps/en/natohq/news_185000.htm.

14. Arnold and Arnold, "Germany's Fragile Leadership Role."

15. FM 3-0, *Operations*, 3-3.

16. Ibid.

17. Ashley Roque, "Project Convergence Events Set for Spring 2024, with Ballistic Missile Defense Addition," Breaking Defense, 29 March 2023, https://breakingdefense.com/2023/03/project-convergence-capstone-event-set-for-spring-2024-with-ballistic-missile-defense-addition/.

18. James Dickinson, "Protect, Defense, Exploit: Air and Missile Defense Evolves for Multidomain Operations," Army.mil, 21 June 2019, https://www.ausa.org/articles/protect-defend-exploit-air-and-missile-defense-evolves-multidomain-operations.

19. Joint Doctrine Publication 0-30, *UK Air and Space Power*, 2nd ed. (Swindon, UK: Development, Concepts and Doctrine Centre, UK Ministry of Defence 2017), https://assets.publishing.service.gov.uk/media/5a8238bd40f0b62305b9320c/doctrine_uk_air_space_power_jdp_0_30.pdf.