MAY 2025

Lessons from the Ukraine Conflict

Modern Warfare in the Age of Autonomy, Information, and Resilience

By Matthew N. Slusher

Executive Summary

The Russia-Ukraine war has emerged as a watershed moment in modern military history, fundamentally reshaping our understanding of contemporary warfare. This white paper analyzes five transformative domains that have defined this conflict: autonomous systems, information operations, electronic warfare, contested logistics, and evolving air defense strategies. By examining the practical applications and lessons learned from this ongoing conflict, this paper provides military planners, defense policymakers, and security professionals with actionable insights for adapting force structures, doctrines, and capabilities to meet the challenges of future warfare. The conflict serves as both warning and blueprint—demonstrating how technological innovation, organizational adaptability, and strategic resilience have become the defining characteristics of military effectiveness in the twenty-first century.

Introduction

Russia's invasion of Ukraine in 2022 marked a pivotal moment in modern military history, opening new avenues for studying the evolving nature of warfare. What Russian leadership initially anticipated would be a swift campaign has instead developed into a protracted conflict, transforming the battlefield into a real-world laboratory for testing new military technologies, doctrines, and operational adaptations.

Among the most significant developments observed in Ukraine has been the transformative role of autonomous systems, particularly unmanned aerial vehicles (UAVs). These emerging technologies are revolutionizing battlefield dynamics, extending operational reach while minimizing risks to human forces and challenging traditional force structures. Simultaneously, the conflict has elevated

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

the importance of information operations, electronic warfare, contested logistics, and innovative air defense strategies in shaping the military landscape of future conflicts.

This white paper provides a comprehensive analysis of modern warfare through five interconnected characteristics that have been prominently displayed throughout the Ukraine conflict:

1. The rise of autonomous systems and their impact on force architecture
2. The information domain as a critical battleground
3. Electronic warfare and spectrum superiority
4. The challenges of sustaining logistics in contested environments
5. The evolution of air defense strategy

By examining these dimensions, this paper aims to provide deeper insights into how military operations are adapting to contemporary challenges and what these adaptations portend for the future of armed conflict. The lessons derived from the Ukraine conflict serve as critical waypoints for military organizations seeking to navigate the rapidly changing character of modern warfare.

The analysis presented in this paper draws on firsthand insights from four senior defense experts **interviewed by the author** in March 2025: Austin Gray, former U.S. Navy intelligence officer and co-founder of Blue Water Autonomy; Major General Gregory Gagnon, deputy chief of space operations for intelligence of the U.S. Space Force; Lieutenant General (Ret.) Lance Landrum, former deputy chair of the NATO Military Committee; and Air Marshal Johnny Stringer, deputy commander of NATO's Allied Air Command.

The Rise of Autonomous Systems and Their Impact on Force Architecture

RANGE EXTENSION AND RISK REDUCTION

Unmanned systems are dramatically transforming the battlefield by extending operational reach while reducing risks to personnel. They enable longer-range engagement with adversaries while minimizing soldiers' exposure to danger. It is generally recognized by military leaders that drones offer a significant advantage in modern conflicts due to their ability to strike at longer ranges with reduced risk.

In the Ukraine conflict, both sides have leveraged drones extensively for reconnaissance, target acquisition, and precision strikes—often beyond the effective range of conventional direct-fire weapons. This capability to project force across dimensional and operational planes while removing personnel from immediate danger has fundamentally altered tactical and operational planning considerations.

DEMOCRATIZATION OF AIR POWER

Perhaps the most significant strategic impact of autonomous systems has been the democratization of air power. Historically, air superiority was the exclusive domain of wealthy nations that could afford expensive aircraft and specialized pilot training. The proliferation of small, affordable drones has dramatically lowered these barriers. As Air Marshal Stringer observed in the **CSIS interview series** mentioned above, "you could conduct most if not all of the airpower roles for the price of a drone, a laptop, and some imagination."

This democratization raises profound questions for military strategy and force planning. Nations and non-state actors now possess means to contest airspace and project power previously considered beyond their reach. In Ukraine, this reality has manifested in a complex and contested aerial environment, despite Russia's nominal advantages in conventional air assets. The dual-use nature of military and adapted civilian drones has further complicated the operational picture, blurring traditional distinctions between military and commercial technologies.

SUPPLY CHAIN AND TECHNOLOGY ACCESSIBILITY

The accessibility of drone technology has significantly influenced drones' battlefield proliferation. The hardware components essential for drone development—batteries, lightweight computing systems, and airframe materials—are readily available through commercial supply chains, with many components sourced from standard e-commerce platforms. Similarly, 3D printing capabilities have facilitated rapid prototyping and scaling of drone production.

Software development for drone operations has likewise accelerated, with advances in firmware, operating systems, and semi-autonomous functionalities. While full autonomy remains a developing capability, even basic remote control systems with limited autonomous functions have proved highly effective in combat conditions. This accessibility has enabled Ukraine to rapidly field large numbers of autonomous systems despite limited indigenous defense industrial capacity.

EVOLUTION OF ASSET CATEGORIES

The Ukraine conflict has revealed an evolution in military force architecture. Traditional military planning distinguished between two primary categories of assets: expendable (ammunition) and survivable (high-value platforms). The drone revolution has expanded this taxonomy to include four categories:

- **Expendable assets:** Single-use, deployable systems like conventional ammunition
- **Attritable assets:** Low-cost systems whose loss poses no strategic consequences
- **Risk-tolerant assets:** Medium-tier unmanned systems that commanders prefer to preserve but can afford to lose if militarily necessary
- **Survivable assets:** High-value platforms and personnel that require protection

This revised architecture creates operational flexibility that previously did not exist. Where commanders once faced a binary choice between risking high-value assets or foregoing operations entirely, they now have degrees of risk appropriate to different threat environments. This framework is particularly valuable for conventional forces structured around high-value platforms.

THE ECONOMICS OF MODERN WARFARE

The Ukraine conflict has upended traditional cost-benefit calculations in military operations. The conventional emphasis on firepower-heavy forces built around expensive platforms—tanks, warships, and advanced aircraft—is being challenged by the effectiveness of low-cost attritable assets, particularly drones. **According to NATO**, Ukrainian drones have been responsible for more than 65 percent of destroyed Russian tanks, representing what many analysts see as a fundamental disruption in the economics of warfare. This dynamic extends beyond Ukraine, with similar cost asymmetries observed in other theaters where non-state actors have employed inexpensive drones against high-value naval

assets. These developments validate a new perspective on the "cheap-expensive" and "targetability" matrix, wherein low-cost but precision-targetable systems produce outsized operational effects when deployed at scale.

TACTICAL VERSATILITY OF AUTONOMOUS SYSTEMS

The conflict has demonstrated the remarkable tactical versatility of unmanned systems across multiple mission profiles. Some of these varied functions are listed below:

- **All-seeing eyes:** Small, difficult-to-detect drones provide unprecedented situational awareness, enabling forces to identify enemy positions, activities, and vulnerabilities without risking human observers.
- **Targeting and battle damage assessment:** Drones play a crucial role in designating targets for indirect fire systems and assessing strike effectiveness.
- **Strike operations:** Armed drones ranging from weaponized commercial models to purpose-built military platforms have been employed against personnel, vehicles, and infrastructure with high precision.
- **Electronic warfare and communications:** UAVs serve as platforms for electronic warfare, communications relays, and signals intelligence collection.
- **Logistics support:** Unmanned ground vehicles enable resupply to isolated units or positions under direct fire, reducing risk to logistics personnel.

These applications demonstrate the flexibility of autonomous systems in maintaining and enhancing traditional military capabilities across numerous operational domains.

VULNERABILITIES AND MITIGATIONS

Despite their strengths, autonomous systems exhibit significant vulnerabilities. Drone operators have become high-value targets, as they are often easier to locate and neutralize than the platforms they control. This has accelerated the development of increased autonomy to reduce operator vulnerability.

Both Ukraine and Russia have developed techniques to trace drone control signals to their source, enabling counter-battery fire or direct strikes against operators. This has necessitated frequent relocation of control stations and the development of more resilient command and control architectures, including relay systems and distributed control networks.

Electronic warfare and cyberattacks reveal additional vulnerabilities. The Ukraine conflict has demonstrated that these threats can be mitigated through technological and operational approaches, such as

- mesh networks that maintain functionality even when individual nodes are compromised;
- multiple communications pathways, including satellite communications, airborne relays, and ground-based systems; and
- local autonomy capabilities that enable operation when communications are degraded.

Surprisingly, these approaches have enabled autonomous systems to function effectively even in sophisticated electronic warfare environments, suggesting that while electronic warfare remains important, it may not be as decisive as some analysts had predicted.

The Information Domain as a Critical Battleground

THE STRATEGIC IMPORTANCE OF INFORMATION

A fundamental lesson from the Ukraine conflict highlights the paramount importance of the information domain. As Major General Gregory Gagnon, Deputy Chief of Space Operations for Intelligence of the U.S. Space Force, observed in the **CSIS interview series**, "the information space became incredibly important in that conflict"—not only for military command and control but also for shaping strategic narratives that influence international support and domestic perceptions.

Russia's approach reflects its established doctrine of "informational confrontation," which comprises two elements: the "information technical" (controlling the means of information) and the "information political" (shaping the message itself). This represents a continuation of Soviet-era tactics, adapted for the modern digital battlefield.

CYBERATTACKS AND SPACE ASSETS

The **Viasat cyberattack** executed immediately before Russia's invasion exemplifies the "information technical" component of this doctrine. Though aimed at Ukrainian military command-and-control infrastructure, this operation had cascading effects that disrupted approximately 5,800 German wind turbines and internet services for thousands of European users. This incident demonstrates how cyberattacks targeting space capabilities can produce widespread, often unintended consequences.

This episode underscores the importance of gaining cyber and space superiority over one's adversaries as an early objective in ground campaigns—a principle likely to become foundational in twenty-first-century conflicts. Successful military operations increasingly depend on establishing control in these domains from the outset.

SPACE SUPERIORITY AND MODERN WARFARE

The Ukraine conflict has highlighted the critical role of space assets in modern warfare, particularly for intelligence, surveillance, and reconnaissance (ISR). Commercial satellite operators have effectively negated Russia's potential space advantage over Ukraine, with the constellation of space assets contributing to Ukraine's capabilities increasing from approximately **200 to 300 satellites** during the conflict.

This democratization of space capabilities has profound implications for conventional forces, as "large mass conventional forces will have a hard time executing surprise in the future" due to the proliferation of commercial remote sensing capabilities, **according to Major General Gagnon**. During Russia's pre-invasion buildup along Ukraine's borders, commercial imaging companies published satellite imagery that enabled think tanks and analysts to accurately assess Russian force dispositions. As Gagnon **noted**, "the commercial remote sensing market in outer space is becoming rapidly an unblinking eye," making it increasingly difficult to conceal conventional force movements.

Commercial satellite systems have also played a crucial role in providing communication links for autonomous vehicles when terrestrial networks are disrupted or jammed. Starlink's services, for

instance, have enabled Ukrainian forces to maintain control of drone operations despite Russian efforts to degrade communication infrastructure.

ORGANIZATIONAL STRUCTURES AND INFORMATION INTEGRATION

The effective integration of information and space assets into operations depends less on technological capabilities than on organizational structures that can incorporate these capabilities into overall military operations. Russia's compartmentalized military organization and lack of trust between units have contributed to its inability to fully leverage its information warfare potential.

Organizational structure similarly affects professional military education and the role of non-commissioned officers (NCOs). Major General Gagnon highlights how Russia's military is disadvantaged by its conscription model (11 percent of personnel are conscripted for one-year terms) and the absence of a professional NCO corps. Effective coordination among space, air, ground, and maritime forces in combined arms operations requires communication and empowerment at lower organizational levels—a capability that depends heavily on experienced NCOs. As Major General Gagnon **notes**, "The reason the American yardstick is the largest yardstick in the world is because of our NCO Corps."

Electronic Warfare and Electromagnetic Spectrum Superiority

RETURN TO CONTESTED ELECTROMAGNETIC ENVIRONMENTS

The Ukraine conflict has revealed a return to contested electromagnetic environments after decades of Western dominance in this domain. Lieutenant General Landrum observes in the **CSIS interview series** that "the biggest stark difference is, as we fought in coalition warfare in Iraq and Afghanistan . . . we were really uncontested in the electromagnetic spectrum." For three decades following the Cold War, Western forces allowed their electromagnetic operations capabilities to atrophy, creating a significant capability gap.

Meanwhile, Russia, China, and other potential adversaries **continued developing** their electronic warfare capabilities and units. This development has created an electromagnetic environment in Ukraine where neither side has been able to establish clear advantage—a stark contrast to Western experiences in recent conflicts.

IMPACT ON AIR SUPERIORITY AND GROUND OPERATIONS

The most direct consequence of this electromagnetic contest has been the inability of either Russia or Ukraine to achieve air superiority—a factor that has contributed to the conflict's positional and attritional warfare characteristics. The contested electromagnetic environment has severely restricted both sides' ability to conduct rapid maneuvers, protect ground forces, and shield maneuvering elements from enemy fire.

This reality contrasts sharply with Western doctrines of air power that evolved from the Gulf War, where air superiority was achieved and maintained throughout operations. The Ukraine conflict suggests that in contested electromagnetic environments, conventional applications of air power may face significant limitations.

SPECIFIC ELECTRONIC WARFARE APPLICATIONS

Several electronic warfare applications have proved particularly significant in the Ukraine conflict:

- **GPS jamming:** Disruption of GPS signals has impeded navigation capabilities for autonomous systems and precision-guided munitions, forcing reliance on alternative guidance methods.
- **Communications disruption:** Both sides have systematically jammed communications networks, degrading command and control capabilities.
- **Signals intelligence:** Electronic warfare operations have included signals intelligence collection critical for battlefield decisionmaking.
- **Tactical jamming of autonomous systems:** Localized jamming operations have targeted UAVs to degrade both reconnaissance and attack capabilities.
- **Frequency agility:** When facing successful Ukrainian jamming of small UAV operations, Russian forces have demonstrated frequency-hopping agility, creating brief windows of operational opportunity.

THE DYNAMIC INTERACTION OF DRONE OPERATIONS AND ELECTRONIC WARFARE

The vulnerability of autonomous systems to electronic warfare represents a defining characteristic of the Ukraine conflict. GPS jamming has proved particularly effective, as many autonomous systems rely on GPS for navigation. Large-scale jamming by Russian forces has forced Ukrainian operators to develop alternative navigation methods including inertial navigation and line-of-sight communications. However, these alternatives present their own vulnerabilities, as line-of-sight communications remain susceptible to electronic interception and further jamming.

Ukrainian forces have rapidly developed defenses and countermeasures to preserve operational effectiveness, including satellite communications, relay stations, and mesh networks that address vulnerabilities while maintaining reliable command and control capabilities.

FUTURE IMPLICATIONS FOR ELECTRONIC WARFARE

The Ukraine conflict points toward a new set of characteristics for electromagnetic warfare strategies:

- **Modern, agile systems:** Future electronic warfare systems will be increasingly adaptable, software-defined, and capable of responding rapidly to changing electromagnetic conditions.
- **Integrated architecture:** Effective electronic warfare architectures will integrate military, government, and commercial domains.
- **Public-private partnerships:** Managing shared spectrum requirements will require collaboration among industry, government, and military stakeholders.
- **Artificial intelligence integration:** Artificial intelligence and machine learning will be central to future electronic warfare, enabling cognitive electronic warfare platforms capable of sensing, analyzing, and responding autonomously at speeds beyond human capabilities.

These technologies will be essential as warfare accelerates, requiring decisionmaking at machine speed while preserving human judgment in critical areas.

The Challenges of Sustaining Logistics in Contested Environments

VULNERABILITY OF TRADITIONAL LOGISTICS MODELS

The Ukraine conflict has exposed fundamental vulnerabilities in traditional logistics approaches. Lieutenant General Landrum **emphasizes** how the conflict has "brought reality to the vulnerability of supply chains, the vulnerability of logistics centers, and how we move and project force."

The war has demonstrated the extreme vulnerability of large infrastructure nodes, supply centers, distribution facilities, and transportation networks including rail, roads, bridges, and ports. These vulnerabilities are magnified by adversaries' long-range precision strike capabilities, non-kinetic attacks, and electromagnetic interference.

THE POST-COLD WAR EFFICIENCY TRAP

A critical insight from analysis of the conflict is how Western militaries have systematically reduced their organic logistics capabilities over the past 30–40 years in favor of commercial outsourcing. While this approach delivered efficiencies through "just-in-time" delivery systems and elimination of redundancies, it also created strategic vulnerabilities. As Lieutenant General Landrum **stated**, "over the decades . . . [the U.S. military] became incredibly efficient. We outsourced and divested of military logistics capability, using commercial capability to get this service that we needed, because we had the luxury of planning well in advance for our operations."

This model functioned effectively when operations were planned months or years in advance in uncontested environments like Iraq and Afghanistan. However, it is dangerously inadequate for rapid response in contested environments where commercial providers may be unwilling to operate in high-threat areas.

HYBRID THREATS TO LOGISTICS INFRASTRUCTURE

The Ukraine conflict has highlighted emerging hybrid threats to logistics infrastructure, including **targeted attacks** against supply nodes, cyber operations, underwater infrastructure sabotage, and difficult-to-attribute asymmetric operations. These new threats compound traditional challenges such as infrastructure limitations (e.g., road weight restrictions, bridge capacities), rail gauge differences, port throughput constraints, and customs and border regulations.

REIMAGINING LOGISTICS FOR CONTESTED ENVIRONMENTS

The conflict has catalyzed a new paradigm for logistics in contested environments based on the principle that Lieutenant General Landrum **describes** as "disaggregate to survive, reaggregate when necessary." This approach relies on several key characteristics:

- **Disaggregated logistics networks:** The distribution of supply nodes and capabilities enhances survivability against precision strikes.
- **Command and control of dispersed assets:** The development of command and control systems capable of managing widely distributed logistics elements is essential for enhancing operational efficiency and coordination across complex supply chains.
- **Rapid reaggregation capability:** The ability to concentrate logistics resources quickly based on operational requirements is crucial for ensuring timely support and mission success in dynamic environments.

- **Renewed focus on stockpiling:** Accepting increased costs associated with maintaining larger reserves of critical munitions and supplies reflects a strategic shift, reversing the "just-in-time" paradigm in favor of enhanced readiness and resilience.

This transformation represents a fundamental shift from efficiency-driven logistics toward approaches prioritizing resilience and survivability in contested environments.

LOGISTICS INNOVATION THROUGH TECHNOLOGY

The Ukraine conflict has revealed several opportunities for technological innovation in logistics:

- **Additive manufacturing:** 3D printing capabilities reduce dependence on vulnerable supply chains for certain components.
- **Interoperable systems:** Movement away from proprietary systems toward open architectures enables integration across platforms and nations.
- **Distributed command and control:** Development of robust communications networks allows for managing disaggregated logistics assets effectively.

These innovations will be essential for creating logistics systems capable of operating in contested environments while maintaining the flexibility required for modern military operations.

The Evolution of Air Defense and Strategy

HISTORICAL CONTEXT AND STRATEGIC RESET

Two significant historical factors have shaped NATO's current air defense posture, according to Air Marshal Stringer:

- **Post–Cold War disinvestment:** The three decades following the Cold War saw significant reductions in NATO air defense capabilities, creating vulnerabilities exposed by Russia's 2022 invasion of Ukraine.
- **Counterinsurgency operations:** Counterterrorism and counterinsurgency campaigns in Iraq and Afghanistan and against the Islamic State diverted resources and attention from developing capabilities against conventional or near-peer threats.

These factors created military structures optimized for specific types of operations while leaving NATO inadequately prepared for the hybrid warfare techniques deployed in Ukraine.

EXPANDED THREAT SPECTRUM

- The Ukraine conflict has highlighted a dramatic expansion in the range of threats confronting modern air defense systems:
- **Low-cost threats:** One-way attack drones and first-person view (FPV) drones equipped with simple warheads that can be mass-produced at minimal cost
- **High-end threats:** Advanced systems such as hypersonic air-launched ballistic missiles capable of extreme speeds and ranges
- **Asymmetric approaches:** Exploitation of social media, legal mechanisms, and disinformation to create favorable conditions for military operations

This evolving threat landscape necessitates a fundamental reconsideration of integrated air and missile defense (IAMD) approaches, focusing on what Air Marshal Stringer **describes** as going "back to first principles."

ENHANCED SENSING CAPABILITIES

Ukraine has demonstrated innovative approaches to air defense detection, including implementation of extensive networks of inexpensive acoustic sensors linked to create comprehensive recognized air pictures; diversification beyond traditional radar systems to improve situational awareness; and integration of multiple sensing modalities to establish resilient detection networks.

COMMAND AND CONTROL TRANSFORMATION

In the face of evolving threats, modernizing command and control systems is critical. According to Air Marshal Stringer, this should be done through a renewed commitment to standardization agreements (STANAGs) that were neglected during the post-Cold War period; ensuring interoperability across national air command and control systems within NATO's architecture; and shifting from monolithic software development toward modular, agile approaches.

This transformation **would not require** "one big program to try and do everything," but rather adopting smartphone-like models with intuitive interfaces and specialized applications, while embracing development, security, and operations (DevSecOps) principles to create an "intelligent, imaginative ecosystem" of suppliers. DevSecOps integrates security throughout the software development cycle, fostering collaboration while providing mechanisms for rapidly developing secure software.

FORCE POSTURE INNOVATIONS

The Ukraine conflict has prompted military strategists to reconsider force positioning and employment, including by reimagining defense postures and alert states for enhanced responsiveness; drawing inspiration from Cold War integration models while adapting them to contemporary threats; and balancing offensive and defensive operations, recognizing that being "necessarily offensive to be defensive" as Marshal Stringer **puts it**, may be required against mass drone threats.

DRONE WARFARE IMPLICATIONS

The widespread deployment of drones in Ukraine presents both challenges and opportunities, as outlined below:

- **Democratization effect:** Even resource-constrained adversaries can now execute traditional air power functions including air superiority, strike, ISR, and transport.
- **Mass vs. quality trade-offs:** Drones enable "high-low mix" strategies that increase effective force mass while maintaining capability.
- **Rethinking generations:** Military leaders can evolve beyond platform-centric definitions, such as fifth-generation aircraft, and embrace **warfare-centric concepts** that define the emerging paradigm of sixth-generation warfare, emphasizing integrated capabilities, information dominance, and multi-domain operations.

AIR SUPERIORITY IN MODERN CONFLICT

Both Russia and Ukraine have experienced the consequences of failing to secure air superiority, resulting in a protracted, attrition-based conflict. This underscores that while warfare's character evolves rapidly, certain principles–including air superiority–remain essential.

However, the concept of air superiority itself is evolving to encompass control of the electromagnetic spectrum, integration of kinetic and non-kinetic effects, and employment of autonomous systems. Future air operations will require this expanded understanding of air superiority to address increasingly complex and interconnected operational variables.

DETERRENCE RECALIBRATION

The Ukraine crisis has reinforced the fundamental elements of effective deterrence:

- **Technical capability:** Ensuring forces possess necessary equipment and technology
- **Capacity:** Maintaining sufficient quantities of platforms and weapons
- **Credibility:** Combining capability, capacity, and readiness to establish a believable deterrent posture

Experts emphasize the need to **avoid** a "cliff edge" between conventional and nuclear options, instead providing graduated deterrent options that offer political leaders flexibility in responding to escalation. An optimally balanced force structure should include capabilities across the entire conflict spectrum, from low-intensity operations to high-end warfighting.

Conclusion: Continuous Adaptation as the New Military Imperative

BEYOND STATIC SOLUTIONS

A central theme emerging from the Ukraine conflict is the need for continuous evolution in military capabilities, doctrines, and organizations. As Air Marshal Stringer **observes**, "better never stops"–leaders should reject the notion of achieving perfect end states for military capabilities. Instead, military effectiveness increasingly depends on continuous testing, experimentation, and validation of approaches.

This mindset represents a significant departure from traditional military procurement and doctrine development, which seeks definitive solutions to military problems. In the rapidly evolving environment revealed in Ukraine, such static approaches quickly become obsolete against technological and tactical innovations.

REALISTIC TRAINING FOR COMPLEX ENVIRONMENTS

The lessons from Ukraine underscore the importance of incorporating realistic conditions into military training and exercises, including electromagnetically contested environments, logistics challenges and disruptions, hybrid threats across multiple domains, and operations with degraded communications and command and control systems.

As Lieutenant General Landrum **emphasizes**, "we have to practice, train, and exercise" these capabilities during peacetime to ensure their effectiveness in crisis or conflict. This approach requires directly confronting difficult operational problems rather than "wishing . . . [them] away" in training environments.

ALLIANCE COORDINATION AND PUBLIC-PRIVATE INTEGRATION

The Ukraine conflict demonstrates the critical importance of collaboration between military, government, and commercial entities across multiple domains, including managing shared electromagnetic spectrum use, integrating commercial space capabilities into military operations, developing new models for public-private logistics partnerships, and leveraging commercial technology development for military applications.

These partnerships require innovative approaches that balance commercial efficiency with military resilience requirements, creating effective systems for both peacetime and conflict.

The five dimensions examined in this paper—autonomous systems, information operations, electronic warfare, resilient logistics, and adaptive air defense—represent interconnected and mutually reinforcing aspects of modern warfare. Future success will depend on mastering these domains while developing organizational structures and doctrines that facilitate continuous adaptation to emerging challenges. The Ukraine conflict suggests that military forces must embrace perpetual evolution rather than seeking static solutions to dynamic problems.

As armed forces worldwide adapt their planning, acquisition, and strategic processes, the military organizations that internalize these lessons—embracing technological innovation, organizational adaptability, and operational resilience—will be best positioned to succeed in the complex security environment of the twenty-first century. ■

Colonel Matthew N. Slusher *is a military fellow with the Defense and Security Department at the Center for Strategic and International Studies in Washington, D.C.*

This report is made possible by general support to CSIS. No direct sponsorship contributed to this report.

The views expressed in this paper are those of the author and do not reflect the official policy or position of the U.S. government or the Department of Defense.