MAY 2025

Conflict in Focus: Lessons from Russia-Ukraine

Episode Summaries

AUTHORS
Matthew Slusher
Krista Auchenbach
Scott Murphy
Quinton Packard
Scott Pence
Luke Slivinski

A Report of the CSIS Defense and Security Department

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

MAY 2025

Conflict in Focus: Lessons from Russia-Ukraine

Episode Summaries

AUTHORS
Matthew Slusher
Krista Auchenbach
Scott Murphy
Quinton Packard
Scott Pence
Luke Slivinski

A Report of the Defense and Security Department

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in 2015, succeeding former U.S. senator Sam Nunn (D-GA). Founded in 1962, CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

CSIS's purpose is to define the future of national security. We are guided by a distinct set of values—nonpartisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS's values work in concert toward the goal of making real-world impact.

CSIS scholars bring their policy expertise, judgment, and robust networks to their research, analysis, and recommendations. We organize conferences, publish, lecture, and make media appearances that aim to increase the knowledge, awareness, and salience of policy issues with relevant stakeholders and the interested public.

CSIS has impact when our research helps to inform the decisionmaking of key policymakers and the thinking of key influencers. We work toward a vision of a safer and more prosperous world.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

Acknowledgments

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

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

Contents

Introduction

By Matthew Slusher

Military Fellow, Defense and Security Department, Center for Strategic and International Studies

The Russia-Ukraine conflict has captivated global attention, revealing a new chapter in the evolution of warfare—one defined by resilience, innovation, and multidomain engagement. From ground offensives to cyberattacks and the contested use of space, this war has challenged traditional military assumptions and reshaped strategic thinking. ***Conflict in Focus***, a limited event series from CSIS running from February-March 2025, explored these developments through in-depth conversations with military fellows and expert guests. Each episode centered on a key domain—air, land, maritime, cyber, and space—drawing on firsthand experience to unpack the lessons of modern conflict and implications for future wars. This paper recaps these episodes and provides the main takeaways and conclusions from each.

While the conditions of the Russia-Ukraine War are unique, many of its features offer critical insights for anticipating future large-scale conflicts. The lack of clear air superiority, contested space access, and the widespread use of low-cost drones and defensive fortifications point to enduring trends in warfare. Yet, notable absences—such as U.S. stealth capabilities, nuclear deterrence, and expansive naval power—are a reminder that every conflict has its own character. For military professionals, policymakers, and strategists, understanding both the innovations and limitations of this war is essential. As future adversaries adapt and evolve, the enduring lesson is clear: Success will belong to those who can integrate all instruments of power to gain and maintain the advantage.

Land Domain Lessons from Russia-Ukraine

Overview

This panel featured **Colonel Roman Kostenko**, Ukrainian member of parliament; **Lieutenant General (Ret.) Ben Hodges**, former commander, U.S. Army Europe; and **Dr. Benjamin Jensen**, CSIS senior fellow; and was moderated by **Colonel Scott Pence**, CSIS military fellow.

Key Operational Context

The discussion began with an overview of how the Russia-Ukraine conflict evolved from February 2022 through the end of 2024:

- In February 2022, the Russian invasion was launched along multiple axes (north from Belarus toward Kyiv, east from Donbas toward Kharkiv, and south from Crimea toward Kherson).
- Initial Russian advances were repelled around Kyiv by April 2022.
- Ukraine recaptured territory in Kharkiv (September 2022) and Kherson (November 2022).
- The war then settled into attritional trench warfare with relatively static frontlines throughout 2023–24.
- Ukraine launched a surprise incursion into Russia's Kursk region in August 2024.

The current battlefield stretches approximately 1,000 miles, with 500 miles of active contact, where approximately 400,000 Russian troops face 250,000 Ukrainian soldiers.

Major Themes and Insights

UKRAINE'S STRATEGIC NEEDS

Kostenko emphasized that while Ukraine requires a consistent and uninterrupted weapons supply, true victory will depend on diplomatic efforts as well as military strength. He stressed that Western partners must distinguish between "stopping the war" and "defeating Russia," arguing that Ukraine needs strategic support to achieve victory, not merely to hold defensive positions. Hodges added that Ukraine's greatest challenge lies in maintaining confidence that the United States and Europe will continue supporting them, rather than pressuring Kyiv into a settlement that sacrifices Ukrainian territory.

THE KURSK INCURSION: A STRATEGIC MASTERSTROKE

The August 2024 Ukrainian incursion into Russia's Kursk region was highlighted as a significant strategic success. Jensen noted that Ukraine demonstrated the ability to restore mobility on a static front by attacking a "gap" in Russian defenses rather than a heavily fortified "surface." The operation showcased Ukrainian mastery of maneuver warfare principles, effectively combining drones, electronic warfare, and mobility corridors. Hodges emphasized that Ukraine achieved tactical surprise despite Russia's advanced drone and surveillance capabilities, exposed Russia's command and control weaknesses—particularly the friction between Federal Security Service (FSB) border forces and the General Staff—and created strategic dilemmas by forcing Russian resource reallocations. He argued that the operation not only provided Ukraine leverage for future negotiations but also challenged the narrative of Russian invincibility.

MODERN COMBINED ARMS AND TECHNOLOGY INTEGRATION

Panelists discussed how the character of warfare is evolving. Jensen emphasized the need for "super soldiers" capable of rapidly adapting to new technologies, pointing out how Ukrainian civilians quickly transformed into effective fighters. He stressed the importance of building systems designed to adapt as multiple technologies emerge and highlighted the challenge of turning tactical innovations into operational advantages. Regarding armored warfare, both Hodges and Jensen agreed that while tanks remain valuable, they must be used differently: Poorly trained and poorly employed tanks have proven easy prey for drones. Future tank designs, they suggested, might feature unmanned turrets, lighter armor, and integrated electronic warfare capabilities, with Jensen envisioning tanks as mobile power platforms supporting electronic warfare and drone operations.

THE TRANSPARENT BATTLEFIELD

Kostenko described how drones and satellites have rendered the battlefield almost fully transparent to both sides, making rapid, large-scale advances—like those seen during World War II—nearly impossible. Surprise attacks are now feasible only at the scale of a few brigades or smaller units. Jensen and Hodges emphasized the critical need for deception operations and signature management (visual, thermal, and electronic) to maintain operational surprise. They warned that U.S. forces are currently undertrained in the use of decoys and stressed that while new camouflage technologies can reduce detectability, disciplined execution is essential.

COMMAND AND CONTROL CHALLENGES

Jensen highlighted Ukraine's limitations in command and control. Ukraine currently lacks division- and corps-level structures, resulting in multiple brigades reporting directly to higher headquarters, which creates inefficiencies in resource use and coordination of combat power. In contrast, Russia maintains appropriate hierarchical command structures but struggles with leadership instability, corruption, and political interference, undermining its effectiveness.

THE NORTH KOREAN DIMENSION

The panel also addressed the role of North Korean troops fighting alongside Russian forces. Kostenko observed that while North Korean soldiers are well-trained, they rely on outdated tactics from the 1960s and 70s, advancing in large formations that make them vulnerable to modern drone warfare. Jensen noted that this development signals an early stage of broader international conflict, suggesting, "We're already in World War III." He pointed out the difficulty of coalition warfare without interoperability and reported that heavy casualties have forced North Korean units to be pulled from the front lines. This situation, he argued, challenges traditional notions of lethality, as physically fit soldiers are now being killed by drone operators operating at a distance.

INDIRECT FIRES AND MANEUVER

Jensen discussed how modern warfare demands the integration of electronic warfare with both direct and indirect fires. He explained how Russia successfully neutralized High Mobility Artillery Rockets System (HIMARS) effectiveness through GPS jamming but continues to struggle with synchronizing operational-level fires. He emphasized that achieving breakthroughs remains costly without well-executed deception or synchronized fires capable of overwhelming enemy defenses.

ENDURANCE: THE PATH TO VICTORY

Hodges stressed the importance of endurance for Ukraine's ultimate success. While Ukraine does not face a manpower shortage, he explained, it does suffer from a shortage of trained soldiers. He suggested greater integration of women into military roles and emphasized the importance of ensuring families that their loved ones will receive proper training. Despite the challenges, he suggested Ukraine will remain strong, with over 60 percent of the population opposing any territorial concessions. Jensen concluded that the war is likely to end through a combination of strategic defense and creative offensive actions. He argued that sustained economic pressure on Russia—through measures like oil price manipulation and sanctions—is critical. Ukraine's successful drone strikes against Russian refineries demonstrate the potential of such pressure. Ultimately, he said, the West must force Russia into a strategic dilemma: "Bleed in Ukraine or go broke in Moscow."

Key Takeaways

The panelists emphasized several crucial points for Western policymakers:

1. Supporting Ukraine is not charity; it serves U.S. strategic interests and deters China.
2. Greater economic pressure on Russia should complement military support.
3. Maintaining Western will to support Ukraine will be the decisive factor for a Ukrainian victory.
4. Future land warfare will require greater integration of traditional combined arms with electronic warfare, drones, and deception operations.

This conflict represents a watershed moment in the evolution of land warfare, with critical lessons about integration of technology, the importance of adaptability, and the enduring human role in modern combat.

Maritime Domain Lessons from Russia-Ukraine

Overview

This panel discussion featured **Rear Admiral Mike Mattis**, director of strategic effects, U.S. Naval Forces Europe/Africa; **Dr. Rebecca Grant**, vice president, Lexington Institute; and **Dr. Stacie Pettyjohn**, senior fellow and director, Defense Program, Center for New American Security; and was moderated by **Captain Quinton Packard**, CSIS military fellow. The panel examined how Ukraine, a nation with virtually no navy, successfully challenged Russia's formidable Black Sea Fleet through innovative asymmetric warfare. Despite Russia's overwhelming naval superiority at the start of the invasion, Ukraine has denied Russia sea control and inflicted heavy losses on the Black Sea Fleet using unmanned surface vehicles (USVs), cruise missiles, and other asymmetric approaches.

The Black Sea Maritime Conflict

Mattis detailed the conflict's maritime evolution: First, Ukraine used mines around Odesa to prevent an amphibious landing and deployed coastal defense cruise missiles (Harpoon and Neptune) to create an initial sea denial zone. After Russia terminated the Black Sea Grain Initiative in July 2023 and attempted to blockade Ukrainian ports, Ukraine responded with USV attacks against Russian warships, pushing the fleet further back. By January 2024, Ukraine had sunk multiple Russian vessels using USVs, including a Raptor-class patrol boat, a Ropucha-class landing ship, and a Bykov-class corvette. These losses prompted leadership changes in the Russian Navy and forced Russia's fleet to retreat to Novorossiysk and create a defensive bastion around the Kerch Strait.

Mattis outlined Ukraine's four maritime objectives and its success so far at achieving each:

1. **Prevent invasion from the sea.** Ukraine has successfully achieved this objective through mines and coastal defense cruise missiles.
2. **Prevent missile attacks from the sea.** Ukraine has partially achieved this objective; Russian vessels can still launch Kalibr cruise missiles but must quickly return to port rather than remaining deployed.
3. **Prevent a blockade.** Ukraine has successfully achieved this objective; it now exports more grain than before the war.
4. **Prevent resupply ashore.** Ukraine has been partially successful in achieving this objective; Russian naval logistics to Crimea and Syria have been severely disrupted.

Russia's primary objective to protect Crimea has been partly maintained, but Russia's armed forces have lost effective use of Sevastopol, their main naval base. Overall, Russia has failed to achieve most of its maritime objectives (amphibious invasion, effective missile attacks, and blockade), with its only success being the continued occupation of Crimea through land routes rather than maritime supply.

Key Technologies and Tactics

Panelists outlined how Ukraine's success has relied on several key capabilities:

1. **Unmanned surface vessels:** Maritime drones such as the "Sea Baby" have proven effective in constrained waters, conducting kamikaze attacks and serving as platforms for other weapons.
2. **Diversified drone capabilities:** Ukraine has developed modular USVs with various capabilities, including some equipped with air-to-air missiles (which have successfully taken down Russian helicopters), quadcopters for aerial reconnaissance, and cannons for surface threats.
3. **Coordinated multi-axis tactics:** Videos have shown USVs operating in coordinated packs, with some drones herding Russian ships into deeper waters where they could be engaged by other drone groups.
4. **Integration with deep strike capabilities:** When Russian ships retreated to ports, Ukraine shifted to attacking them with deep strike missiles.

Evolution of the Maritime Battle

The panelists emphasized that this is a dynamic contest of adaptation and counteradaptation. Early USV attacks exploited Russian unpreparedness and lack of effective countermeasures. In response, Russia increased air surveillance (helicopters and tactical aircraft) over the Black Sea, significantly reducing USV survivability. By mid-2024, Ukraine found it "10 times harder" to get USVs from Odesa to strike targets near Novorossiysk due to increased Russian air patrols.

Ukraine responded by developing USVs with air defense capabilities to target Russian helicopters, creating diversified drone groups, and exploring undersea drones for greater survivability.

The panel emphasized that this pattern of move and countermove will continue to evolve, with the advantage going to whichever side can innovate faster and stay ahead of its opponent's defensive measures.

Transferability to Other Theaters

The panel discussed whether Ukraine's maritime drone successes could transfer to other conflict zones. They pointed out that the Black Sea's unique characteristics (enclosed sea with limited access through the Bosphorus, which Turkey closed to additional Russian warships) created advantages for Ukraine that could be relevant in other constrained waters like the Baltic Sea, Taiwan Strait, and parts of the South China Sea, but would be less effective in open ocean environments like the Philippine Sea.

Overall, USVs offer a relatively low-cost method for smaller powers to deny sea control to larger naval forces in restricted waters near their shores. Pettyjohn noted this approach could significantly enhance Taiwan's "porcupine defense" strategy with layers of anti-ship cruise missiles supplemented by USVs and aerial drones.

Implications for Future Naval Operations

The discussion highlighted several implications for naval warfare:

1. **Need for counter capabilities:** Mattis called the Black Sea conflict a "warning shot to conventional navies," which must develop capabilities to counter threats from USVs and unmanned aerial systems (UASs).
2. **Cost-imposing strategies:** Pettyjohn compared USV swarms to the Houthi campaign against shipping in the Red Sea, where inexpensive drones have forced adversaries to expend costly missiles and resources, creating favorable cost-exchange ratios for the attacker.
3. **Integration with air power:** Grant emphasized the unique conditions of the Black Sea conflict, where Russia and Ukraine have an "air power stalemate." She questioned how USV tactics would work against a high-end air force able to establish air superiority.
4. **All-domain integration:** Mattis stressed that unmanned systems alone are insufficient—the most effective approaches integrate hybrid effects across multiple domains (sea, air, land, cyber, space) to overwhelm an adversary's defenses.
5. **Proliferation risk:** The panel agreed that these capabilities will likely proliferate to various actors, including nonstate groups like Hezbollah or the Houthis, posing challenges for maritime security globally.

Key Takeaways

The panelists concluded with their most important takeaways from the Black Sea conflict:

1. The maritime domain is more conducive to drone-enabled strategic effects than the land domain, where defensive measures create "a drone hellscape."
2. This is an action-reaction-counteraction fight requiring constant innovation and adaptation—there are no permanent solutions.
3. The United States needs to accelerate unmanned vessel tactics and operations but integrate them with existing naval capabilities.
4. Cost-effective counters to USVs are essential, as this technology will likely proliferate rapidly.

5. Unmanned systems are not a complete solution but one piece of a larger puzzle.
6. Drones are not direct substitutes for conventional platforms like aircraft carriers, submarines, or destroyers–they complement rather than replace these systems.
7. Traditional capabilities like air superiority should not be discounted.

The panelists agreed that the future of naval warfare will require effectively integrating unmanned systems within conventional force structures, developing both offensive capabilities and defensive countermeasures, and maintaining the ability to rapidly adapt as adversaries evolve their own approaches.

Human Domain Lessons from Russia-Ukraine

Overview

This panel discussion included insights from **Lieutenant Colonel Volodymyr Dutko** of the Ukrainian Army; **Colonel (Ret.) Mark Cancian**, CSIS senior adviser; **Lieutenant General (Ret.) David Barno**, professor at Johns Hopkins University; and **Dr. Ben Connable**, adjunct professor of security studies at Georgetown University. The discussion was moderated by **Colonel Scott Pence**, CSIS military fellow. The panel examined how this war—described as "the first epic land conflict of the twenty-first century"—offers crucial lessons about warfare's human elements that remain constant despite technological advances.

The Human Toll and Psychological Impact

The immense psychological burden commanders and soldiers face in modern warfare was a central theme of the panel. Dutko described the emotional strain of leadership: "You are responsible for human life, and you need to execute the different types of mission[s] . . . to protect native land, homes, relatives, or people, and to minimize casualty." He noted the emotional preparation required before missions, knowing people might not return.

The experts highlighted the war's devastating casualty rates, with reports of approximately 430,000 Russian and 60,000 Ukrainian casualties—figures that dwarf recent U.S. military operations. This scale of loss creates tremendous psychological pressure that most Western militaries have not experienced in generations.

The constant exposure to danger presents a challenge unlike anything in recent U.S. military experience. Barno emphasized that unlike the episodic combat experiences in Iraq and Afghanistan, where troops could return to secure bases with amenities, the Ukraine war features "perpetual, continual, unending exposure to danger." This sustained combat stress tests resilience in ways that U.S. forces, for comparison, have not faced since Korea.

Drawing on lessons from Ukraine and wargaming a potential conflict, Cancian offers a sobering prediction of what U.S. forces might face in a future conflict with China: troops arriving at bases surrounded by wreckage, with hundreds of destroyed aircraft, improvised cemeteries, and hospitals filled with wounded. "This is an experience that we have not had, really, for 70 years," he noted.

Will to Fight and Adaptation

Connable emphasized that despite technological changes, warfare fundamentally remains "a contest of two opposing, hostile, and irreconcilable wills." He criticized how military planners often acknowledge this principle theoretically but fail to properly assess and understand it practically. This failure led to misjudgments about both Russian and Ukrainian will to fight at the war's outset, continuing a pattern seen in U.S. conflicts in Afghanistan, Vietnam, and Iraq.

The experts identified the importance of adaptation as perhaps the most critical lesson from the conflict. Ukrainian and Russian forces have demonstrated remarkable speed in adapting tactics, techniques, and technologies. Barno observed that both sides are "moving at a pace that I think any other military in the world would have great difficulty replicating, to include the U.S. military."

This adaptability extends to drone warfare, where both sides are continually developing countermeasures against electronic warfare tactics. Dutko described this ongoing evolution as "development and blocking since development," referring to how quickly jammers adapt to new drone communication frequencies.

Drones and the Changing Battlefield

The panel identified drone proliferation as a transformative element, though they differed on whether to call it a "gamechanger." The experts noted that while drones will likely be important in future conflicts, larger systems like Predator and Reaper are expected to be more prominent than small, expendable drones.

Barno warned that the United States is "behind in drone warfare," failing to learn from the realities that Ukrainians and Russians face daily. Beyond the technical challenges drones present, he also highlighted the psychological impact of "having a machine looking at you all the time that is devoted to killing you."

The panel discussed recent innovations like fiber-optic-controlled drones that cannot be jammed by electronic warfare systems. While not invincible, these drones represent the rapid technological evolution occurring on the battlefield. Connable provided important context, noting that drones have been part of warfare since World War II, with significant deployment since the 1980s. He cautioned against overgeneralizations, pointing out the unique conditions in Ukraine—a static 1,200-kilometer front line and industrial bases feeding endless drones—that may not exist in other conflicts.

Tanks and Combined Arms

The experts explored whether tanks still have relevance on modern battlefields. While Russian forces have suffered thousands of tank losses, Cancian noted that similar losses occurred in the Battle of Kursk during World War II without rendering tanks obsolete. Connable, citing his study of 423 modern battles, including 61 in Ukraine, asserts that tanks remain critical by providing "shock, speed, [and] mobile protected firepower up to the line of contact."

The panel agreed that tanks are now "vulnerable but useful," with their future effectiveness hinging on cost dynamics: How many multimillion-dollar tanks can militaries afford if they can be destroyed by swarms of thousand-dollar drones? Dutko emphasized that the psychological impact of tanks remains powerful, especially when used in coordinated assaults with infantry.

Surprise in Modern Warfare

Despite claims about "transparent battlefields," the panel affirmed that surprise remains possible at tactical and strategic levels. Cancian identified four types of surprise evident in this conflict: strategic (the war's occurrence), technical (drone developments), political/diplomatic (NATO expansion), and battlefield (ongoing trench warfare resembling World War I).

The experts agreed that while more sensors make hiding harder, deception and concealment remain important. As Dutko explained, forces now "try to conceal in different forests, buildings," to hide as much as possible. Connable rejected the notion that technological advances will eliminate surprise, saying that "if it were [completely transparent] then nobody would be fighting anymore."

North Korean Involvement

The panel discussed the 2024 addition of North Korean troops, whose human wave tactics have reportedly led to thousands of casualties, creating psychological challenges for defenders forced to kill large numbers of attackers.

Connable cited reports of Ukrainian machine gunners needing to be pulled off the line because they were killing so many North Koreans, echoing similar psychological trauma from the Iran-Iraq War. Barno identified this as an overlooked aspect of combat: "The psychological impact of killing is probably underestimated, especially killing masses of your adversary." He questioned how militaries can prepare soldiers for this reality.

The panel also noted that North Korea's participation in this conflict marks its first battlefield experience since 1953, potentially making its military more capable for future conflicts.

Key Takeaways

The experts emphasized several key takeaways:

1. Surprise is inevitable in warfare—the focus should be on coping with it rather than avoiding it.
2. Precision weapons face new challenges due to widespread jamming and countermeasures.
3. Cyber warfare proved less decisive than many predicted.
4. War remains fundamentally about people and physical control of territory, as summarized by Cancian: "If you really want to control it, occupy it, then you have to do it the same way the Roman legions did."

Barno concluded by questioning whether the U.S. military is adequately preparing for adaptation: "How much time and energy and effort gets put into instilling a culture of rapid adaptation once you get in a battle where things don't look like what you expected?"

The discussion emphasized that despite technological evolution, warfare's human dimension remains paramount. The psychological burden of combat, the will to fight, and the capacity to adapt remain decisive factors that can determine victory or defeat.

Defense Industrial Base Lessons from Russia-Ukraine

Overview

The panel covered lessons for the defense industrial base and featured experts with firsthand experience in Ukraine's defense innovation ecosystem: **Dr. Phillip Karber**, professor of military strategy and warfighting at the Eisenhower School; **Mark Valentine**, president and general manager of global government at Skydio; and **Kateryna Bondar**, CSIS fellow. The discussion was moderated by **Captain Luke Slivinski**, CSIS military fellow.

Historical Context and Industrial Base Transformation

PREWAR DEFENSE INDUSTRY CHALLENGES

Prior to the 2014 conflict, Ukraine's defense industry faced systematic challenges. As Karber noted, approximately 43 percent of Russian weapon components came from Ukraine. The state conglomerate Ukroboronprom prioritized foreign military sales and employment over Ukraine's own defense needs. Bondar highlighted that there appeared to be a targeted effort to weaken Ukraine's defense industrial independence during President Yanukovych's pro-Russia administration.

Major prewar defense industry issues included underfunding of new developments, massive outflow of engineering talent due to lack of investment, and difficulties integrating Western technologies with Soviet legacy systems.

EVOLUTION AFTER THE 2014 CONFLICT

The initial 2014 conflict sparked the beginnings of transformation. Both volunteer groups and established defense entities began developing solutions to battlefield challenges. Software engineers created situational

awareness and fire control systems when they recognized frontline troops lacked such capabilities. This organic response created the foundation for systems like Delta and Kropyva that were later formally adopted by Ukraine's Ministry of Defense.

FULL-SCALE INVASION IMPACT AND RESPONSE

The 2022 full-scale Russian invasion dramatically accelerated transformation of Ukraine's defense industrial base. Key developments included the following:

1. **Civilian-military fusion:** Bondar described the development of "civil-military fusion in the Ukrainian way," with IT professionals and engineers either joining the armed forces directly or providing technical support.
2. **Decentralized innovation:** Beyond formal defense industries, entrepreneurs and small groups emerged as significant innovation sources.
3. **Infrastructure damage:** Approximately 43 percent of Ukraine's defense industrial facilities have been struck by Russian missiles. Karber highlighted one particularly devastating strike on a design bureau, in which 40 staff members who chose to continue working through air raid alarms were killed.
4. **Western equipment maintenance:** The Ukrainian defense industry pivoted to maintaining and modifying Western equipment, which often arrived with issues (dead batteries, missing reactive armor, etc.).

Rapid Innovation Cycles and Field Testing

Perhaps the most emphasized insight from all the panelists was the unprecedented speed of innovation cycles in Ukraine. Karber observed that major changes in drone technology occur approximately every six months—dramatically faster than typical Western defense acquisition timelines. "We in the West, including the United States, are just not keeping up. It takes us six years to get it designed," he noted. For software-based weapons systems, Bondar indicated the innovation cycle could be as short as one to two weeks, with immediate battlefield testing and feedback loops. Valentine highlighted how traditional U.S. acquisition processes rely on requirements developed years before contracts are awarded, often based on lessons from previous conflicts rather than emerging threats. He explained how Skydio's drones, designed for U.S. military needs from the Iraq and Afghanistan era—where the United States controlled the airspace and spectrum—initially failed in Ukraine's contested electronic environment.

Forward-Deployed Engineers

A critical factor identified as enabling rapid innovation was the direct connection between developers and frontline users:

1. **Embedded development:** Valentine described deploying 20–30 multidisciplinary teams to Ukraine monthly, eventually establishing a permanent presence including Ukrainian engineers.
2. **Organic process:** Bondar explained the process was not formally designed, but rather emerged naturally due to widespread mobilization—many engineers had friends or family at the front, creating direct feedback channels.
3. **Combat experience:** Karber described seeing drones constructed in brigade workshops by scientists who were integrated into military units and taking direct feedback from combat operators.

Drone Warfare Evolution and Challenges

PROLIFERATION AND TACTICAL IMPACT

Karber detailed the progression from limited drone availability in 2014–15 to nearly company-level drone operations today. This proliferation has fundamentally changed battlefield dynamics, rendering previously survivable platforms like tanks highly vulnerable.

ELECTRONIC WARFARE CHALLENGES

Both Russia and Ukraine rapidly developed electronic warfare capabilities. Early Ukrainian drones (like U.S.-provided Ravens) were vulnerable to Russian electronic warfare, sometimes being captured and turned against Ukrainian forces. Skydio had to transition from single-band radios to multi-band frequency-hopping capabilities to counter jamming. Visual inertial odometry technology also helped counter GPS jamming and spoofing.

FUTURE DIRECTIONS

The panel discussed several emerging trends:

1. **Human-to-machine ratio evolution:** Valentine traced the evolution from MQ-1 drones, which require 60–70 personnel per drone, to one-to-one operator/drone relationships, to future concepts of one operator controlling multiple autonomous systems.
2. **Swarm development:** While true autonomous swarm capabilities remain experimental, multiple panelists identified this as a likely future direction. Bondar emphasized that effective swarms require sophisticated artificial intelligence (AI) for autonomous decisionmaking and navigation.
3. **Remote operations centers:** Valentine described an interim step between current operations and full swarm autonomy—operations centers where small teams could control hundreds or thousands of semiautonomous drones.

Supply Chain and Production Scale Challenges

SCALE REQUIREMENTS FOR PEER CONFLICT

Valentine highlighted the unprecedented scale of drone usage: "In certain phases of the war, the Ukrainians were going through 10,000 small drones a month." He noted that existing U.S. stockpiles would only last about a month and a half at such consumption rates.

STRATEGIC SUPPLY VULNERABILITIES

Critical components like sensors, batteries, and chips often have international supply chains vulnerable to disruption. Valentine recounted how Skydio was sanctioned by China, cutting off access to battery components and forcing urgent development of Western alternatives.

REGULATORY BARRIERS

Several regulatory barriers were identified as hampering U.S.-Ukrainian cooperation:

1. **ITAR restrictions:** The International Traffic in Arms Regulations (ITAR) create significant challenges for technology transfer and collaboration.
2. **Export control classifications:** Valentine noted that commercially available components (like thermal sensors available on Amazon) become highly restricted when incorporated into drone systems.

3. **Security classifications:** Karber mentioned difficulties providing Ukrainians with secure help due to classification restrictions.

Post-Conflict Considerations and Deterrence

CEASEFIRE CHALLENGES

Karber emphasized that any potential ceasefire would face significant challenges. For one, Ukraine would need to maintain forces along a 2,000-kilometer potential front. Beyond that, Russia has historically violated previous agreements (Minsk I, Minsk II, Budapest, Intermediate Nuclear Forces Treaty). Without external enforcement, a ceasefire would be "inherently unstable."

REQUIREMENTS FOR LONG-TERM DETERRENCE

The panel identified several requirements for sustainable Ukrainian security:

1. **Self-sufficient defense industry:** Bondar emphasized the need for talent, funding, investment, and technology transfer to rebuild Ukrainian defense capabilities.
2. **Allied support:** Given the long-term nature of building defense industrial capacity, continued Western support is essential to "fill the gap."
3. **Credible deterrence:** Valentine stressed that deterrence depends on demonstrating the capability to impose unacceptable costs on an adversary.

Policy Recommendations

The panel offered several recommendations for U.S. policymakers:

1. **Streamline collaboration.** Reform ITAR and export control processes to facilitate faster U.S.-Ukrainian cooperation.
2. **Create strategic partnerships.** Establish formal partnerships to expedite technology transfers with key allies.
3. **Secure supply chains.** Consider Defense Production Act authorities to establish domestic production of critical components and stockpile materials.
4. **Support knowledge transfer.** Establish deeper information sharing about Ukrainian battlefield innovations and tactical applications.
5. **Consider production scale.** Reassess U.S. production capacity to meet the consumption rates demonstrated in Ukraine.
6. **Plan for the long term.** Support rebuilding Ukraine's indigenous defense industrial capacity through investment and technical assistance.

Conclusion

The Russia-Ukraine conflict has demonstrated dramatic changes in modern warfare, particularly regarding the speed of innovation cycles, drone proliferation, and electronic warfare evolution. The traditional Western

defense acquisition model struggles to match the pace of battlefield-driven innovation seen in Ukraine. For the United States to maintain technological superiority and support allies, significant adaptations in regulatory frameworks, supply chain security, and innovation methodologies will be necessary. As Valentine succinctly stated, “It’s about deterrence. And if we can’t demonstrate that we have the capability to do something, that’s how deterrence fails and wars start.”

Air and Space Domain Lessons from Russia-Ukraine

Part One

This panel, part one of two sessions, featured **Austin Gray**, cofounder of Blue Water Autonomy, and **Major General Gregory Gagnon**, deputy chief of space operations for intelligence at the U.S. Space Force. The event was moderated by **Colonel Matthew Slusher**, CSIS military fellow. Panelists discussed the impact of autonomous vehicles in warfare and the evolving role of space in modern conflict.

Drone Warfare Evolution

Gray, a former U.S. Navy intelligence officer with hands-on drone production experience inside of Ukraine, highlighted how autonomous vehicles have fundamentally transformed modern warfare thanks to several key characteristics:

1. **Extended range and reduced risk:** Drones allow forces to strike targets from greater distances while minimizing personnel exposure.
2. **Accessible technology:** The hardware components for military drones are increasingly available through commercial channels, with many parts ordered from Amazon and Alibaba for Ukrainian production.
3. **Rapid development cycles:** Ukrainian forces update drone software nightly and hardware every few weeks, demonstrating agility that is impossible in traditional procurement.

Gray emphasized the importance of understanding cost and targeting dynamics through a framework where military assets are categorized along two axes: (1) cheap to expensive, and (2) easy to target versus difficult to target.

This framework reveals the emergence of a critical middle category between expendable/attritable assets (like ammunition or infantry) and expensive survivable assets (like carrier groups). Autonomous systems like collaborative combat aircraft (CCA) occupy this middle space, where they are valuable enough to not be expendable but can take on dangerous missions without risking human lives.

Gray argued that the U.S. defense procurement culture needs to shift toward a portfolio approach that embraces more risk-taking and competition between providers. He anticipates the main technological advancements will come not from breakthrough capabilities but from better integration of existing hardware and software, creating more resilient mesh networks and improved command and control systems.

Space Domain Insights

Gagnon offered critical observations about space operations in the Russia-Ukraine conflict, which are summarized below.

INFORMATION CONFRONTATION

Russia's Viasat cyberattack leading up to the invasion exemplified its "information confrontation" doctrine, which employs two types of control: (1) technical information, using cyber and electronic warfare to control communications; and (2) political information, controlling messaging and narratives.

Though intended to disrupt Ukrainian command and control, the attack had unintended consequences, affecting wind turbines in Germany and internet services across Europe. This demonstrated how gaining cyber and space superiority is an early objective in modern campaigns.

RUSSIAN MILITARY FAILURES

Despite being the world's third most powerful conventional army prior to the invasion, Russia has failed to achieve space superiority in the conflict. There are a number of key factors for this failure:

- There is no professional non-commissioned officer corps capable of executing combined arms operations.
- There has been an inability to integrate space assets into the "reconnaissance strike complex" due to organizational silos.
- Russia has been unable to counter commercial satellite intelligence provided to Ukraine by Western partners.

CHINA-RUSSIA SPACE COOPERATION

The conflict has accelerated concerning trends in Russia-China cooperation:

- Chinese companies are providing commercial satellite imagery to Russia.
- There is growing economic integration between the two countries, including a 43 percent increase in bilateral trade in 2023.
- China is supplying 90 percent of Russia's microelectronics.
- There has been increased joint military exercises including ground, maritime, and bomber operations.

LOSS OF CONVENTIONAL SURPRISE

Large conventional force buildups can no longer achieve strategic surprise thanks to the availability of commercial satellite imagery. Think tanks and news organizations could use satellite imagery to track and

count Russian forces on Ukraine's border before the invasion; Gagnon referred to this as the "commercial unblinking eye" that has the potential to benefit global security.

U.S. SPACE FORCE STRATEGY

U.S. adversaries have increasingly weaponized space in recent years, and China is rapidly expanding its presence in space, adding 200 satellites per year in 2022 and 2023. In response to adversaries weaponizing space, the U.S. Space Force is taking steps to protect U.S. interests, including

- moving from single, large satellites to proliferated architectures with increased resilience;
- increasing the number of U.S. satellites in space, with over 100 new satellites planned to be launched in 2025 alone;
- developing capabilities to protect U.S. assets and hold adversary assets at risk; and
- countering China's rapid space expansion.

Gagnon emphasized that the U.S. military's reduced size—the Army is down from 732,000 personnel in 1990 to 445,000 personnel today, the Navy from 600 to 300 ships, and the Air Force from around 10,000 to around 5,000 aircraft—is only sustainable with space superiority. Without control of this high ground, a conflict with a peer competitor could resemble the stalemate in Ukraine.

Key Electromagnetic Spectrum Insights

Both experts highlighted the critical importance of the electromagnetic spectrum in modern warfare. The electromagnetic spectrum is essential for targeting mobile assets from a distance and crucial for networking sensors, decisionmakers, and shooters. However, it is a domain in which the United States may have lost its edge after 20 years of fighting adversaries who didn't challenge spectrum use.

Gray noted that despite electronic warfare and jamming attempts, drones continue to operate effectively through spectrum maneuver, resilient communications networks, and mesh networking principles.

Key Takeaways

The event highlighted several transformative lessons from the Russia-Ukraine conflict:

1. Drone proliferation is creating asymmetric opportunities for smaller forces and nonstate actors to challenge conventionally superior forces.
2. Space domain awareness has permanently altered the strategic calculus by eliminating the element of surprise for large conventional operations.
3. Force architecture evolution requires a spectrum of capabilities from expendable to survivable, with a critical middle zone of autonomous systems.
4. Human factors remain decisive; Russia's failures have stemmed largely from organizational issues rather than technology gaps.
5. Space superiority is no longer optional but foundational to modern warfare, enabling smaller but more lethal conventional forces.

The discussions underscored the critical importance of investing in space capabilities, embracing autonomous systems, and developing professional military personnel who can execute combined arms operations in contested electromagnetic environments.

Air and Space Domain Lessons from Russia-Ukraine

Part Two

Overview

This panel was the second part of a CSIS event focused on air and space domain lessons from the Russia-Ukraine conflict. The discussion featured **Lieutenant General Lance Landrum**, former deputy chair of the NATO Military Committee, and **Air Marshal Johnny Stringer**, deputy commander of NATO Allied Air Command. The conversation, moderated by **Colonel Matthew Slusher**, explored critical insights about electronic warfare, contested logistics, air defense systems, drone warfare, and the future of NATO air doctrine in light of evolving modern warfare.

Electronic Warfare

THE NEW CONTESTED ELECTROMAGNETIC ENVIRONMENT

Landrum emphasized that neither Russia nor Ukraine has achieved air superiority in this conflict, which has resulted in positional warfare and attrition. The contest for superiority in the electromagnetic spectrum is ongoing; unlike in Iraq and Afghanistan, where Western coalition forces operated uncontested in the electromagnetic environment, Ukraine represents a fully contested space.

TECHNOLOGICAL REGRESSION AND ADAPTATION

After the Cold War, Western forces shed three decades of electromagnetic expertise, in both human capital and equipment modernization. Meanwhile, Russia formed specialized electromagnetic warfare units and developed capabilities that gave it superiority in certain areas. The conflict has demonstrated the vulnerability of GPS-dependent systems to jamming, forcing adaptation through alternative navigation methods.

IMPACT ON MODERN SYSTEMS

Nearly all modern systems rely on connectivity through the electromagnetic spectrum, making them vulnerable to interference. Specific examples include

- jamming of GPS signals affecting autonomous systems' navigation;
- disruption of communications networks;
- electronic eavesdropping and signals intelligence; and
- tactical jamming of drone operations.

Landrum described how Russia initially operated small UASs in a specific frequency band. When Ukraine began jamming those frequencies effectively, Russia adapted by moving to different frequency bands, creating a temporary vulnerability window for Ukrainian forces.

FUTURE DIRECTIONS

Future systems will need to be "modern, agile, nimble, software-defined, and able to react and maneuver" within the electromagnetic space, as Landrum highlighted. Cognitive electronic warfare using machine learning and AI will be crucial for

- rapidly sensing and analyzing the electromagnetic environment;
- automated decisionmaking at machine speed;
- deconflicting friendly systems from adversary jamming; and
- managing the increasingly complex shared electromagnetic space.

Contested Logistics

SUPPLY CHAIN VULNERABILITIES

The Ukraine conflict has demonstrated the vulnerability of logistics centers, infrastructure, and transportation networks. Landrum noted that Western militaries have divested significant military logistics capabilities over decades, outsourcing to commercial industry for efficiency. This approach worked when operations had months of planning time in uncontested environments but is problematic when forces are facing contested spaces from the beginning.

DISAGGREGATION FOR SURVIVAL

A key lesson is the need to disaggregate logistics and sustainment capabilities for survival while maintaining the ability to reaggregate them when needed. This presents significant command and control challenges.

INFRASTRUCTURE AND POLICY CHALLENGES

Moving forces across Europe faces numerous obstacles, such as road infrastructure and weight-bearing limitations, rail infrastructure and gauge changes in eastern Europe, inadequate port structures, customs regulations and border-crossing complexities, and the challenges associated with transporting hazardous materials across borders. Landrum emphasized that these procedures must be practiced and streamlined during peacetime operations to ensure smooth transitions during crises.

STOCKPILING AND SUPPLY CHAIN INNOVATION

The Russia-Ukraine conflict revealed inadequate stockpiling of critical munitions like artillery shells. With this in mind, future procurement strategies should

- accept the cost of maintaining larger stockpiles;
- utilize additive manufacturing (e.g., 3D printing) for certain components;
- move away from proprietary systems toward interoperable solutions; and
- improve command and control of disaggregated logistics.

Air Defense and NATO's Adaptation

EVOLVING THREAT LANDSCAPE

The evolving threat landscape has forced NATO to fundamentally rethink its approach to integrated air and missile defense. Stringer described how the modern battlefield now presents a dramatically expanded range of aerial threats, divided broadly into two categories. On the low end, inexpensive one-way attack drones and first-person view drones can be produced in the thousands, overwhelming traditional defenses through sheer volume. On the high end, advanced weapons like hypersonic missiles, including systems such as the AS-24 air-launched ballistic missile, pose existential challenges to existing detection and interception frameworks. This dual-threat environment demands a new level of speed, agility, and adaptability from NATO forces.

MULTILAYERED RESPONSE

In response, NATO is developing a multilayered air and missile defense strategy built around several critical components. First, sensing capabilities must move beyond traditional radar systems, taking cues from Ukraine's use of thousands of inexpensive acoustic sensors to detect incoming threats. Second, command and control structures must be modernized to facilitate faster, more flexible decisionmaking. Third, strategic force posturing and alert states must be recalibrated to reflect the dynamic threat environment, ensuring forces are ready to respond at varying levels of intensity. Finally, NATO must recognize that true defense requires a blend of both defensive and offensive actions—striking enemy launch sites and systems preemptively when necessary to blunt potential attacks.

AIR COMMAND AND CONTROL SYSTEMS

To support this evolving approach, NATO is making significant investments to enhance interoperability across its air command and control networks. This includes a renewed emphasis on standardization agreements to ensure common protocols and procedures across member states. Interoperability efforts also focus on bridging national air command and control systems, enabling seamless cooperation during joint operations. A modular approach to software development is replacing traditional monolithic systems, allowing NATO forces to rapidly integrate new technologies and tools. Additionally, intuitive user interfaces are being prioritized to reduce training burdens and increase system accessibility for operators. Supporting all of these initiatives is the cultivation of an agile development ecosystem that draws on multiple suppliers, fostering innovation and resilience across the alliance.

Drone Warfare

DEMOCRATIZATION OF AIRPOWER

Stringer noted that drone technology has democratized airpower, allowing actors with limited resources to perform traditional airpower roles (air superiority, strike, intelligence, surveillance, and reconnaissance (ISR), and lift) at a fraction of the cost. This presents both challenges and opportunities for NATO.

HIGH-LOW MIX APPROACH

While high-end military systems continue to grow more expensive, drones and related technologies provide opportunities for a "high-low mix" that can multiply effectiveness: Packaging cheaper drone systems with high-end weapons can reduce the number of expensive munitions needed, creating an effective increase in mass and weapons effectiveness

BEYOND PLATFORM GENERATIONS

Stringer argued that NATO should shift away from discussing generations of platforms (e.g., fifth-generation F-35) and instead focus on what sixth-generation warfare looks like—emphasizing integrated systems and combined capabilities rather than individual platforms.

Future of NATO Air Doctrine

INTEGRATION AND UTILITY OF LEGACY SYSTEMS

Both speakers emphasized that while new technologies are important, existing platforms can maintain utility through continuous upgrades of systems, imaginative employment strategies, and incorporation into broader, integrated force packages.

CAPABILITY DEVELOPMENT THROUGH EXPERIMENTATION

NATO's Allied Air Command is placing greater emphasis on capability development with new methods including weapons and tactics conferences (the first was held in 2023), high-end air exercises like Ramstein Flag, and synthetic training environments.

DETERRENCE THROUGH CREDIBILITY

Effective deterrence requires forces with technical capability, sufficient capacity and numbers, and the credibility to win in a fight.

Stringer emphasized integration across domains (multidomain operations) and providing a range of deterrent options that avoid a "cliff edge" between conventional and nuclear responses.

Key Takeaways

1. Air superiority remains essential to prevent conflicts from devolving into costly attritional warfare.
2. Integration of kinetic and non-kinetic effects is becoming increasingly critical on the modern battlefield.
3. Greater use of autonomy and human-machine teaming is reshaping air operations.
4. Operating at machine speed through AI and advanced systems is now a necessity for maintaining an edge.

5. Continuous experimentation and validation are vital.

As Stringer emphasized, NATO must relentlessly iterate and adapt to stay ahead of adversaries: "You're never going to get to the place of perfection here. You have to be continually iterating what you're doing so your opponents know that you are serious."

Space and Data Domain Lessons from Russia-Ukraine

Overview

This panel discussion explored how space capabilities, data technologies, and commercial services have transformed warfare during the Russia-Ukraine conflict. Speakers were **Giorgi Tskhakaia**, adviser to Ukraine's deputy prime minister and minister of digital transformation and innovations; **Dr. David Gauthier**, chief strategy officer of GXO Inc. and senior associate with the CSIS Aerospace Security Project; and **Aaron Jaffe**, senior vice president at Palantir. The discussion was moderated by **Krista Auchenbach**, CSIS visiting fellow.

Digital Transformation and Technological Adaptation

Ukraine's Ministry of Digital Transformation has played a crucial role in the country's resilience against Russia's invasion. Established in 2019 to create a "government on a smartphone," the ministry quickly adapted to wartime needs. The Diia app became essential for Ukrainians, providing digital passports that were recognized at international borders. The e-Enemy app allowed citizens to send valuable intelligence directly to the military, creating a crowdsourced intelligence network in the early days of the conflict.

When the war began, Russia held superiority in conventional warfare aspects, including electronic warfare capabilities, ISR, artillery, and drone technologies. Ukraine compensated through technological innovation, moral superiority, and international support. Ukraine formed a cyber army of both professional and volunteer "ethical hackers" to defend critical infrastructure against Russian cyberattacks. Tskhakaia emphasized that "this is the war of technologies, of the minds," noting that the character of the war continues to change dramatically every six months as new technologies emerge and countermeasures develop.

Commercial Space and Data Capabilities

The war demonstrated how commercial satellite imagery could be effectively used for tactical battlefield operations rather than just strategic intelligence. Gauthier described how the U.S. National Geospatial-Intelligence Agency initially faced "bureaucratic challenges" and "cultural challenges" in providing direct, real-time satellite imagery to Ukrainian forces. The agency eventually established alternative dissemination paths through private industry companies, allowing raw imagery to flow directly to Ukrainian forces.

Radar imagery proves particularly valuable, enabling detection of Russian convoys through clouds and at night. Companies like Ursa Space use radar imagery to continuously monitor evacuation routes, check road clearance, and map damage to Ukraine's electric grid infrastructure, supporting both military and civilian needs.

Radio frequency collection capabilities from firms like HawkEye 360 allow near-real-time mapping of GPS interference, helping Ukrainian forces identify and counter Russian electronic warfare activities. When Russia attempts to deny or attack remote sensing systems, private industry demonstrates remarkable resilience, finding ways to persist and adapt.

Private Sector Partnerships and Innovation

The panelists emphasized the critical importance of private sector partnerships in supporting Ukraine.

Jaffe highlighted how Palantir's technologies, particularly AI features and computing power, significantly enhanced Ukraine's capabilities. Palantir had to "evolve incredibly, incredibly quickly" to support changing on-the-ground conditions, he said, focusing on building meaningful common operating pictures by fusing disparate information, moving at the speed required by the dynamic intelligence and operational environment, and rapidly incorporating AI for imagery analysis and logistics automation.

Starlink's deployment in Ukraine represented a "gamechanger" in the conflict, according to Tskhakaia. After Vice Prime Minister Mykhailo Fedorov directly requested assistance from Elon Musk, the rapid response and deployment of Starlink terminals provided Ukraine with superior communication capabilities. This is one of the few areas where Ukraine has maintained a technological advantage over Russia, enabling reliable battlefield communications, coordination, and data flow throughout the country.

Other companies like Amazon, Google, and Oracle have also provided valuable support. The panelists noted that private companies demonstrate greater flexibility and agility than government sectors in responding to Ukraine's needs.

Technological Evolution and Innovation Cycles

One striking observation concerned the accelerated pace of technological innovation in Ukraine: From the onset of the war, Ukraine's defense industrial base ballooned to over 500 companies producing various kinds of military equipment, including drones, unmanned ground vehicles, ammunition, and rockets. The Ukrainian government facilitated this growth by reducing regulatory requirements, creating tax incentives for military equipment producers, and enabling increased profit margins from 1 percent to 25 percent (above the 17 percent NATO average) to encourage risk-taking.

Tskhakaia noted that technological innovations in this conflict are typically replicated or countered within 6 to 12 months. This rapid cycle requires continuous innovation to maintain a battlefield advantage.

Decisionmaking and the OODA Loop

The conflict has highlighted the critical importance of accelerating the "OODA" loop—observe, orient, decide, act. As Gauthier explained, commercial imagery and algorithmic warfare have significantly accelerated this cycle, allowing an "underdog" military to effectively counter a superior force relying on traditional doctrine and mass.

Jaffe emphasized that the primacy of decisions has shifted from incremental improvements to "one, two, three orders of magnitude faster" decisionmaking. Two key themes have emerged in this evolution:

- **Integration:** Networks, warfighting functions, and supply chains are increasingly combined to bring stakeholders, information, and components together.
- **AI incorporation:** AI is now used to improve detections, evaluate data, and make decisions at "the speed of relevance."

Shifting the Power Dynamic in Modern Warfare

The Russia-Ukraine conflict has demonstrated that traditional military advantages like superior numbers of tanks or infantry are becoming less decisive. As Tskhakaia stated, "If you are not innovating constantly, you are going to be losing anyway." The conflict has shown that technology and innovation are key factors in modern warfare, with data superiority providing significant advantages in decision quality and speed.

The Ukrainian experience of having a "transparent battlefield" has shifted the advantage from "hiders to finders," creating a new dynamic in warfare. Drones, commercial satellite imagery, and advanced data analytics have fundamentally altered how military operations are conducted.

Logistics and Sustainment Are Warfighting Systems

The Ukraine conflict has underscored that logistics and sustainment systems are not merely administrative functions but critical warfighting systems. Jaffe noted that these systems directly constrain operational capabilities, making them "exceptionally integral" to operations.

Logistical networks challenges include

- network interoperability issues across partner nations;
- disparities between advanced intelligence capabilities and basic sustainment systems;
- need for automation in logistics to enable "push" rather than "pull" models; and
- importance of integrating the entire supply chain from frontline expenditure back to industrial base production.

Key Takeaways

The panelists concluded by sharing their main takeaways from the Russia-Ukraine conflict, and implications for future wars:

1. Information advantage and decision speed: Commercial imagery and algorithmic warfare have enabled Ukraine to achieve tight decision cycles (OODA loops) against a superior military force. In

future conflicts, systems designed to improve the quality and speed of decisions rather than simply processing information will gain an edge amid faster decision cycles.

2. Direct delivery vs. curated intelligence: Providing raw intelligence capabilities directly to frontline forces rather than curating solutions has allowed for innovative tactical use and adaptation.
3. Innovation cycles: Technological advantages typically last at most a year before countermeasures are developed, requiring constant innovation.
4. Comprehensive integration: Integration across networks, warfighting functions, and supply chains is essential and requires treating everything from the front line to the industrial base as one integrated system.
5. AI as a force multiplier: AI is transforming all domains from intelligence to logistics. Tskhakaia predicted that within a year, we'll see "drones flying purely on AI" and AI-driven decisionmaking.
6. Transparency and narrative control: Commercial imagery helped Ukraine document Russian actions, bringing the reality of the conflict into living rooms worldwide and garnering international support. Despite technological shifts, the moral high ground remains a critical factor in sustained resistance.
7. Bottom-up innovation and user-centric design: Providing tools directly to frontline forces enables innovative tactical solutions that would not emerge from top-down approaches, particularly when they can be easily adopted on smartphones with minimal training.

The Ukraine conflict has become a testing ground for military technologies and operational concepts, accelerating innovation cycles and demonstrating how smaller nations can effectively counter larger adversaries through technology, adaptability, and international partnerships.

Whole of Society Resilience Lessons from Russia-Ukraine

Overview

This panel, which examined whole-of-society resilience lessons from the Russia-Ukraine War, featured **Iryna Nykorak**, Ukrainian member of parliament and founder of Arm Women Now; **Kathleen McInnis**, director of the CSIS Smart Women, Smart Power Initiative; and was moderated by **Lieutenant Colonel Scott Murphy**, CSIS military fellow.

Bottom-Up Resilience: The Foundation of Ukraine's Defense

One of the most significant insights highlighted throughout the discussion was that Ukraine's successful resistance stemmed from a bottom-up approach rather than top-down government directives. Nykorak emphasized that Ukraine's resilience came from its people, not its institutions: "This war has taught us many lessons, but perhaps the most important is this: Resilience is not built in institutions alone; it is built in people."

When Russia launched its full-scale invasion in February 2022, thousands of Ukrainian civilians immediately volunteered for military service, while others supported the war effort as volunteers. Businesses donated supplies, and ordinary citizens found ways to contribute. This organic mobilization demonstrated a powerful will to fight that surprised many international observers who had predicted Ukraine would quickly fall due to Russia's overwhelming military superiority.

The panelists noted that this grassroots, population-centric approach to national resilience represents a crucial lesson for other nations. Traditional security frameworks often focus on top-down, authority-directed preparations, but Ukraine's experience suggests the importance of cultivating resilience at the population level.

Women's Role in Defense and the Evolution of Military Equipment

A substantial portion of the discussion centered on women's contributions to Ukraine's defense capabilities. Nykorak shared some remarkable statistics:

- Ukraine has the largest number of women in combat positions globally.
- Over 70,000 women serve in the Ukrainian Armed Forces.
- Approximately 50,000 women hold full combat positions.
- As of early 2025, about 25,000 women were actively serving at the front line (up from 5,000 in early 2024).

Nykorak emphasized that "women are as capable as men of taking up arms and fighting" and have demonstrated high levels of efficiency across various combat roles, from combat medics to drone pilots to intelligence operatives.

The discussion highlighted how women's involvement is driving innovation in military equipment design. Nykorak demonstrated a specially designed female body armor that addresses anatomical differences and provides better protection while being lighter (weighing just 5 kilograms, compared to the standard 12-kilogram armor). This equipment is not just beneficial for women—it represents an advancement in human factors engineering for all soldiers, as male soldiers have also requested the lighter, more ergonomic equipment.

This innovation also points to broader lessons about adapting military equipment to the evolving nature of warfare. As Nykorak explained, the war has transformed from traditional combat to a "war of drones," where 96 percent of injuries come from shrapnel rather than bullets, necessitating different protective approaches for all soldiers.

Indigenous Production and Economic Resilience

Another remarkable achievement highlighted in the discussion was Ukraine's ability to maintain and even grow its industrial base during wartime. In the face of the full-scale invasion, Ukrainian manufacturers have developed high-quality military equipment domestically, including uniforms, boots, and body armor, creating what Nykorak called a "win-win story": These manufacturers employ internally displaced people, particularly women who have lost their homes and livelihoods due to the war. This approach simultaneously strengthens Ukraine's military capabilities while providing economic opportunities for displaced citizens, demonstrating how whole-of-society resilience extends beyond military defense to include economic sustainability.

The Arm Women Now Initiative

Nykorak described her organization, Arm Women Now, which advocates for equal opportunities and proper equipment for women serving in Ukraine's defense and security sectors. The initiative has provided free equipment to more than 12,000 women defenders at the front line and works to amplify Ukrainian women defenders' voices internationally.

This work demonstrates how civil society organizations can complement government efforts, especially in areas where bureaucratic systems may be slow to adapt. As Nykorak noted, as representatives of civil society, organizations like hers can move quickly to address immediate needs while advocating for systemic changes.

Implications for Future Security and Deterrence

The discussion concluded with reflections on the broader implications of Ukraine's experience for global security. McInnis emphasized that whole-of-society resilience should be considered a critical component of deterrence strategies: "When we've talked about deterring Russia, we talk about porcupine strategies, we talk about mutually assured destruction . . . whole-of-society resilience really does need to be a component of this broader suite of strategies necessary to convince Russia to not cross the line."

She noted that deterrence is fundamentally a psychological calculation, requiring a convincing demonstration of will and capability to resist. Ukraine's experience shows that this will to fight—bolstered by whole-of-society resilience—can be decisive even when facing a numerically superior adversary.

Nykorak added that "Putin understands only a language of power" and emphasized the need for both strong will and adequate military capabilities to deter future aggression. She characterized Ukraine as "a wall of security to all European countries," suggesting that Ukraine's resistance has broader implications for European security.

Key Takeaways

1. Bottom-up versus top-down resilience: Ukraine's experience demonstrates that national resilience emerges from a population's will to fight rather than solely from government or military directives.
2. Inclusive defense forces: Integrating women into combat roles has significantly expanded Ukraine's military capabilities, with tens of thousands of women serving effectively in frontline positions.
3. Human-centered equipment design: The war has driven innovations in military equipment that account for human factors and anatomical differences, improving effectiveness for all soldiers.
4. Domestic production capabilities: Even during wartime, Ukraine has maintained and developed its industrial base, producing high-quality military equipment domestically while creating employment opportunities.
5. Civil society complementing government: Organizations like Arm Women Now demonstrate how civil society can address needs quickly while advocating for systemic changes.
6. Whole-of-society deterrence: Ukraine's experience suggests that whole-of-society resilience should be considered an essential component of deterrence strategies, complementing traditional military capabilities.
7. Evolving nature of warfare: The transition to a "war of drones" requires adaptations in equipment and tactics, highlighting the importance of flexibility and innovation.

This discussion offers valuable insights for other nations considering how to build societal resilience in the face of potential threats, emphasizing that military hardware alone is insufficient without the corresponding will to fight and whole-of-society mobilization capabilities.

About the Authors

COLONEL MATTHEW SLUSHER, U.S. AIR FORCE

Matthew Slusher is a military fellow with the Defense and Security Department at the Center for Strategic and International Studies (CSIS). Currently a colonel in the U.S. Air Force, Matthew provides significant strategic and real-world expertise to the program. Most recently he was the NATO Director for Ballistic Missile Defense, where he directed command and control over the BMD mission, management of resources, conduct of operations, and joint planning efforts. Prior to that, Matthew was a dual-hatted Commander of 22 Wing (Royal Canadian Air Force) Operations Support Squadron, and Commander of all U.S. forces assigned to the Canadian Air Defense Sector, North Bay, Ontario, Canada. He has deployed and flown combat missions in support of Operation AFGHAN ASSIST and deployed and directed combat missions supporting Operation UNIFIED PROTECTOR. Colonel Slusher is a Master Air Battle Manager with over 100 combat hours and more than 2,000 total hours flown in E-3A/B/C/G aircraft. He received graduate and undergraduate degrees from Embry-Riddle Aeronautical University, and completed the Joint and Combined Warfighting School in Norfolk, Virginia.

KRISTA AUCHENBACH, OFFICE OF THE SECRETARY OF DEFENSE

Krista Auchenbach is a visiting fellow from the Office of the Secretary of Defense (OSD) in the Defense and Security Department at the Center for Strategic and International Studies (CSIS). Previously, she was the deputy director of the Campaign Decision Support Team in OSD and the division chief for strategic assessments at Headquarters Air Force A5/7, where she provided strategic analysis to senior leaders. Prior to these roles, she served as a senior adviser, strategist, and country director for various portfolios within the Office of the Under Secretary of Defense for Policy from 2008 until 2020. She is a term member with the Council on Foreign Relations and was a 2020 Next Generation Fellow with the Center for a New American Security. Auchenbach has a BA in international affairs and an MA in security policy studies from George Washington University's Elliott School of International Affairs, where she also serves as part-time faculty.

Lieutenant Colonel Scott Murphy, U.S. Marine Corps Lieutenant Colonel Scott Murphy is the 2024–2025 Commandant of the Marine Corps fellow in the Defense and Security Department at the Center for Strategic and International Studies (CSIS). Scott commissioned into the Marine Corps in May 2005. After entry-level and MOS training as an Armor officer, he reported to his first duty station in Twentynine Palms, California. Following his time in Twentynine Palms, Scott served in a variety of operational and staff roles in Quantico, Virginia; Camp Lejeune, North Carolina; and Washington, DC. Most recently, Scott was a training adviser at Training and Education Command in Quantico, helping Marine Corps units incorporate new concepts and equipment. Throughout his career, Scott has had the privilege of serving alongside the most talented servicemembers in the Marine Corps and Joint Force. Scott has a BS in political science and an MA in security studies.

CAPTAIN QUINTON PACKARD, U.S. NAVY

Quinton Packard is a military fellow representing the United States Navy in the Defense and Security Department at the Center for Strategic and International Studies (CSIS). He joined CSIS after serving as the executive assistant to the chief of the Navy Reserve in the Pentagon. He is a naval aviator with over 3,000 flight hours in the CH-46E, HH-60H, and MH-60F airframes. He spent the first 11 years of his total 27 years of military service as a United States Marine before transferring to the Navy Reserve in 2008. His aviation tours included deployments to Kosovo, Djibouti, the United Arab Emirates, and Jordan, as well as multiple tours in Iraq. His command tours include serving as Commanding Officer of Helicopter Sea Combat Squadron-84 and the Commodore of the Maritime Support Wing. Quinton holds a BA in international relations from the University of Delaware and an MS in national resource strategy from the Eisenhower School for National Security and Resource Strategy, with a concentration in weapons of mass destruction. He is a Harvard Kennedy School senior executive fellow, an MIT Seminar XXI fellow, and earned his executive certification in public policy from the Harvard Kennedy School.

COLONEL SCOTT PENCE, U.S. ARMY

Scott Pence is a military fellow representing the U.S. Army in the Defense and Security Department at the Center for Strategic and International Studies (CSIS). Scott served on the Joint Staff as the book briefer to the secretary of defense, responsible for conveying global force management decisions. Before that, he was the garrison commander of Fort Liberty in North Carolina, where he reached consensus on renaming Fort Bragg to Fort Liberty. Scott has deployed three times to Afghanistan and once to Iraq, and he has lived in South Korea, Italy, Germany, Kansas, and Georgia. As the first Armor officer to serve with the 75th Ranger Regiment, Scott served as a company commander and the liaison officer to Kabul Station, Afghanistan. Scott earned an MBA from Webster University, an MA in military operational art and science from the School for Advanced Military Sciences, an MA in strategic studies from the Marshall Program at Fort Leavenworth in Kansas, and a BA in organizational psychology from the University of Michigan.

CAPTAIN LUKE SLIVINSKI, U.S. COAST GUARD

Luke Slivinski is a military fellow with the Defense and Security Department at the Center for Strategic and International Studies (CSIS). He is a captain in the U.S. Coast Guard specializing in afloat operations. He came to CSIS from the Coast Guard Headquarters Office of Cutter Forces, where he served as deputy office chief, overseeing policy, capabilities, and readiness of 240 cutters, and developed requirements for cutter acquisition programs totaling $25 billion. He has been assigned aboard five cutters, including command of CGC Diligence and CGC Blue Shark. His staff tours included joint liaison with the Department of State Office of Marine Conservation and the National Oceanic and Atmospheric Administration Office of Law

Enforcement as well as the Coast Guard Fifth District patrol boat manager. Luke holds a BS in marine and environmental sciences from the U.S. Coast Guard Academy and a Master of Environmental Management degree from Duke University.

COVER PHOTO ADOBE STOCK

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | **www.csis.org**