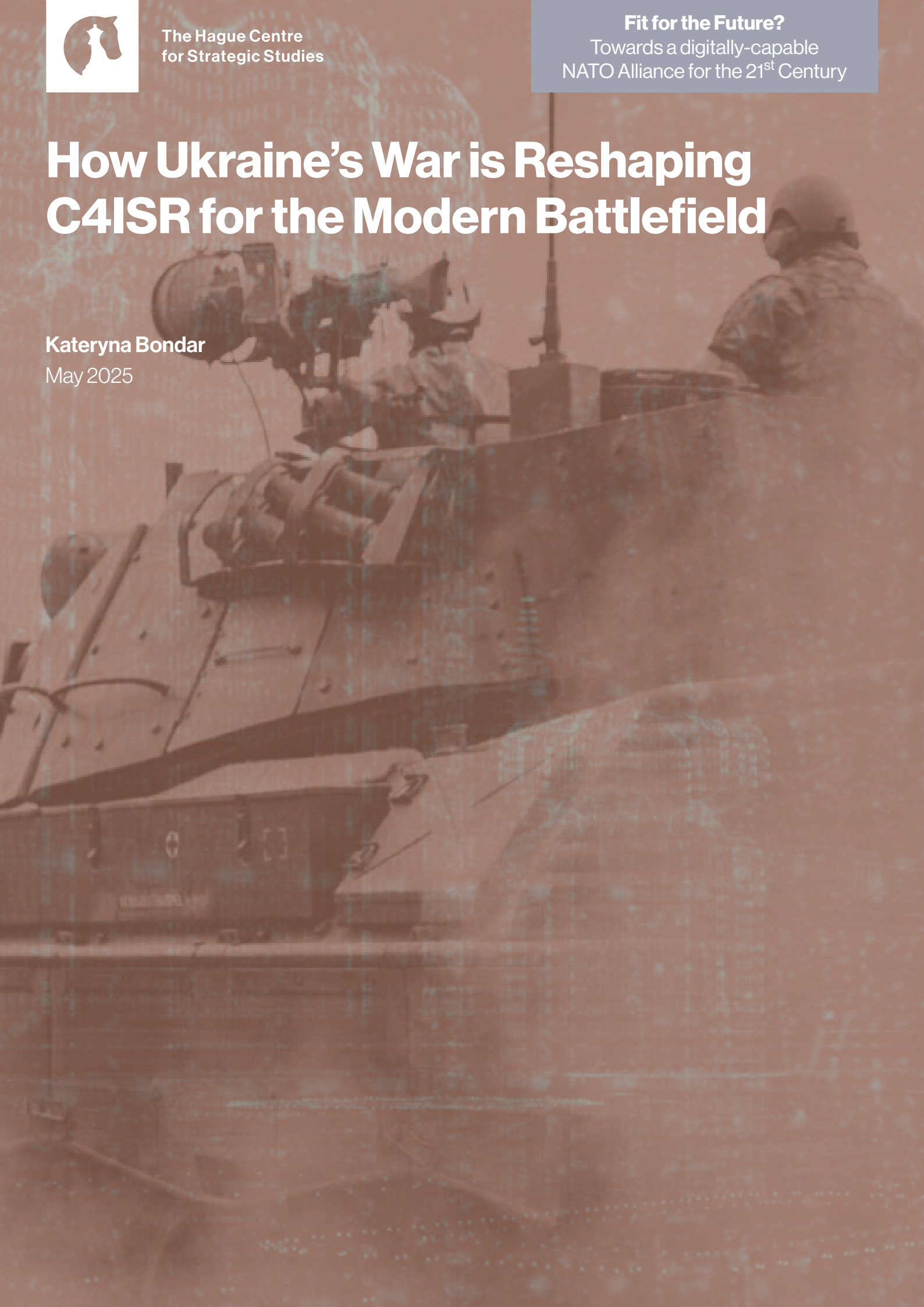
The Hague Centre
for Strategic Studies

Fit for the Future?
Towards a digitally-capable
NATO Alliance for the 21st Century

How Ukraine's War is Reshaping C4ISR for the Modern Battlefield



Kateryna Bondar

May 2025

The Hague Centre
for Strategic Studies

How Ukraine's War is Reshaping C4ISR for the Modern Battlefield

Author:
Kateryna Bondar, Fellow, Wadhwani AI Center at the Center for Strategic & International Studies

Editor:
Tim Sweijs

May 2025

This HCSS paper is part of a series of guest contributions related to the "NATO's digital capabilities" project, established in the run up to the 2025 NATO summit in The Hague. The research was made possible through a financial contribution from Microsoft to the Hague Centre for Strategic Studies (HCSS).

Introduction

As the war in Ukraine entered its fourth year, it has fundamentally reshaped modern warfare, compelling both Ukraine and Russia to adapt their strategies, tactics, and technology at a relentless pace. This war has not only accelerated innovations on the battlefield but also exposed the critical importance of robust and agile C4ISR—Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance. In many respects, Ukraine found itself racing to keep pace with a much better-resourced adversary. Despite facing existential threats, the Ukrainian Armed Forces had to adapt rapidly, creatively leveraging limited resources to strengthen their C4ISR capabilities.

One of the most pressing challenges Ukraine encountered was its constrained capacity—financially, technologically, and in terms of human capital.

One of the most pressing challenges Ukraine encountered was its constrained capacity—financially, technologically, and in terms of human capital. At the outset, there was no overarching C4ISR strategy in place; the country was forced to respond to threats in real time. Equipment shortfalls, lack of formal doctrine, and the urgent need for reliable surveillance and communication systems posed serious hurdles. Yet, it was precisely under these daunting circumstances that Ukrainian forces discovered new ways to operationalise commercial technologies, implement AI-driven ISR solutions, and integrate digital battlefield management systems—at times outpacing their more traditional allies.

Alongside these resource-driven challenges, the Ukrainian experience demonstrates that warfare success is often predicated on a continuous learning process, particularly in the high-stakes realm of C4ISR. Every frontline encounter, every intelligence report, and every technology test feeds into a feedback loop of rapid adaptation. Ukrainian forces have become adept at iterating new procedures quickly, integrating field data back into command structures, and refining tactics in near real time. This cyclical "learn-and-adapt" mindset ensures that even under pressing conditions, lessons gleaned from one engagement shape the planning and execution of the next. Consequently, Ukrainian forces have improved an operational culture that prizes flexibility and creative problem-solving—an ethos that has proven at least as valuable as hardware or official protocols.

In discussing C4ISR, it is tempting to focus solely on advanced equipment or cutting-edge AI. However, Ukraine's case shows the delicate balance between technology, human expertise, and procedural rigor. Simply acquiring sophisticated assets without the right people and organisational frameworks often falls short. Conversely, highly skilled personnel can only do so much if they lack the right tools or are shackled by rigid bureaucracy. By comparing C4ISR to the human body's central nervous system[1]—where the "brain" (command centers) processes information from "senses" (ISR systems) and dispatches directives via a "nervous system" (communications)—it is becoming obvious how effective orchestration of technology, people, and procedures enables agility and synchronised action across domains.

This paper examines the key lessons that emerge from Ukraine's ongoing struggle through the lens of C4ISR. Each subsequent section explores one component of this "nervous system," outlining the challenges the Ukrainian Armed Forces faced, the ways in which they learned and adapted, and how they balanced technology, human expertise, and procedural rigor. Different lessons will demonstrate different aspects of these three considerations.

[1] Defense One, "C4ISR: The Military's Nervous System," n.d., https://www.defenseone.com/insights/cards/c4isr-military-nervous-system/.

Command and Control (C2)

Ukraine inherited a rigid, Soviet-era C2 structure,[2] closely resembling the system used by Russia. This familiarity initially gave Russia an advantage in the 2014 war, as it could anticipate Ukrainian military responses based on shared doctrinal foundations. However, as the conflict in Donbas unfolded, Ukraine began adopting NATO standards[3] in C4ISR while simultaneously gaining invaluable battlefield experience. These developments created both the necessity and the opportunity for Ukraine to make its C2 more adaptable—incorporating lessons from allies, refining tactics, and responding to emerging threats in the East of the country. By the time of the 2022 full-scale invasion, Ukraine's C2 had evolved significantly, better equipping it to handle new challenges, integrate intelligence from Western partners, and coordinate effectively with allied advisors. After 2022, Ukraine also began contributing to developing new NATO standards based on the lessons it learned during the war.[4]

The war created a dynamic environment in which Ukrainian forces had to continuously learn, adjust procedures, and integrate new technologies on the fly.

This transformation did not happen overnight—it was the result of an ongoing process of adaptation under fire. The war created a dynamic environment in which Ukrainian forces had to continuously learn, adjust procedures, and integrate new technologies on the fly. The following examples illustrate how Ukraine's Armed Forces responded to key C2 challenges in practice, what adaptations were made over time, and how success depended not only on technological assets but also on the ability of people and institutions to absorb lessons and evolve.

1. Decentralisation of command is essential for operational agility across a wide and dynamic frontline.

The war in Ukraine has demonstrated the effectiveness of decentralised command and control,[5] especially when forces must manage a sprawling frontline and rapidly changing nature of threats. Early in the conflict, the Ukrainian Armed Forces had to conduct hundreds of mission along a front line of more than a 1,000 km. Therefore, rapid Russian advances could not be contained through purely centralised directives. In response, Ukrainian military leadership granted small units and junior officers extensive autonomy and decision-making authority, which allowed swift tactical responses with on-the-ground intelligence.[6] This flexible approach grew stronger when Ukraine rapidly integrated local militias into the Territorial Defense Forces, enabling newly formed units to operate independently while maintaining overarching coordination within the Armed Forces.[7]

2 Yurii Poita and Center for Army, Conversion and Disarmament Studies, "Some Lessons From Command and Control (C2) in the Russian-Ukrainian War," *Some Lessons From Command and Control (C2) in the Russian-Ukrainian War*, n.d., https://indsr.org.tw/uploads/indsr/files/202311/7eba0534-512b-4275-a2f5-9d7b3ef20e1d.pdf.

3 "NATO's Support of Ukraine's C4 Capabilities," AFCEA International, December 7, 2023, https://www.afcea.org/signal-media/defense-operations/natos-support-ukraines-c4-capabilities.

4 "Now Ukraine Not Only Implements NATO Standards, but Also Can Participate in the Development of New Standards - Address by President Volodymyr Zelenskyy — Official Website of the President of Ukraine," Official Website of the President of Ukraine, July 12, 2022, https://www.president.gov.ua/en/news/ukrayina-teper-ne-lishe-vprovadzhuye-standarti-nato-j-mozhe-76449.

5 "Institute for Future Conflict (IFC)," September 11, 2024, https://www.ifc.usafa.edu/articles/pivotal-lessons-from-the-war-in-ukraine#:~:text=Ukraine%20has%20employed%20decentralized%20command,but%20tentative%20advantage%20for%20Ukraine.

6 Victoriano Vicente and Dimitra Pateraki, "The Role of Command and Control Dynamics in the Ukraine Conflict and Implications for European Land Forces," journal-article, ed. Belén Padrón Salinas, 2024, https://finabel.org/wp-content/uploads/2024/10/IF-PDFs.pdfxx_.pdf.

7 Martpork, "Ukraine's Territorial Defence on a War Footing - ICDS," ICDS, April 13, 2022, https://icds.ee/en/ukraines-territorial-defence-on-a-war-footing/.

2. Survivability of command infrastructure requires mobility, dispersion, and disciplined communication.

High-tech weapon systems and precise targeting capabilities have made command centers highly vulnerable in modern warfare, as numerous successful strikes on both Ukrainian and Russian headquarters illustrate. To counter this threat, Ukrainian commanders frequently relocated or dispersed their command posts, used mobile command solutions, and enforced strict communication discipline to avoid detection.[8] Despite these efforts, Ukrainian units lost personnel when Russian forces intercepted signals or pinpointed headquarters locations.[9] Russian command posts experienced similar vulnerabilities, and Ukraine relied on Western intelligence to locate and strike them. Militaries now recognise that they must protect command infrastructure by enhancing mobility, practicing stealth, and deploying defensive measures against precision-guided munitions to ensure operational continuity and survival.

Militaries now recognise that they must protect command infrastructure by enhancing mobility, practicing stealth, and deploying defensive measures against precision-guided munitions to ensure operational continuity and survival.

3. Rapid integration of commercial technologies enhances situational awareness and tactical effectiveness.

The conflict has demonstrated the Ukrainian military's willingness to embrace and adapt emerging technologies rapidly, particularly at lower command levels. Frontline units adopted unmanned systems and software tools,[10] collaborating directly with tech manufacturers to offer feedback, refine systems, and maintain a competitive edge.[11] At higher command levels, leaders expanded their focus beyond unmanned systems by boosting overall situational awareness through platforms such as the Delta system,[12] which fuses real-time intelligence for a near-real-time common operating picture. Meanwhile, volunteer-built applications like GIS Arta and Kropyva have improved fire control by linking forward observers, drones, and artillery units, greatly reducing the time from target detection to strike. These innovations thrive under a leadership culture that welcomes new software, promotes direct cooperation with civilian developers, and quickly fields commercial technologies to strengthen communication and operational awareness.

4. Standardised, secure data-sharing protocols enable real-time coordination with partners and allies.

Ukraine's ability to exchange intelligence with NATO partners and integrate Western weaponry into its command infrastructure highlights the importance of interoperable data-sharing protocols.[13] By tapping into secure, cloud-based systems and encrypted channels, Ukrainian

8 "Lessons Learned From the Ukrainian Territorial Defense Forces: Command Post Survivability," www.army.mil, February 6, 2024, https://www.army.mil/article/273510/lessons_learned_from_the_ukrainian_territorial_defense_forces_command_post_survivability.

9 "Smart Phones Playing Prominent Role in Russia-Ukraine War | TRADOC G2 Operational Environment Enterprise," TRADOC G2 Operational Environment Enterprise, August 10, 2023, https://oe.tradoc.army.mil/2023/08/10/smart-phones-playing-prominent-role-in-russia-ukraine-war/.

10 Kateryna Bondar, "Why Ukraine is Establishing Unmanned Forces Across Its Defense Sector and What the United States Can Learn from It," January 21, 2025, https://www.csis.org/analysis/why-ukraine-establishing-unmanned-forces.

11 Kateryna Bondar, "Closing the Loop: Enhancing U.S. Drone Capabilities Through Real-World Testing," January 21, 2025, https://www.csis.org/analysis/closing-loop-enhancing-us-drone-capabilities-through-real-world-testing.

12 "Дельта | Новини МОУ," March 30, 2024, https://mod.gov.ua/news/shho-take-sistema-delta-i-yak-vona-zadae-trendi.

13 Joe Saballa and Joe Saballa, "NATO Eyes Intelligence Sharing With Ukraine on Russia's EW Capabilities," The Defense Post, June 10, 2024, https://thedefensepost.com/2024/06/10/nato-intelligence-sharing-ukraine/.

and allied forces have synchronised[14] their efforts to detect, track, and engage enemy targets in real time. This interoperability not only boosts collective defense but also illustrates the practical value of standardised C2 frameworks. As NATO members continue supplying advanced systems and intelligence, Ukraine's experience demonstrates how a cohesive technological and procedural environment accelerates decision-making and contributes to more effective mission outcomes.

Communications

In fact, a U.S. Space Force commander confirmed that Russia tried to jam Starlink and failed, largely due to its design and SpaceX's quick software updates to overcome interference.

The war in eastern Ukraine since 2014 exposed severe shortcomings in the Armed Forces of Ukraine's communications. At the outset of hostilities, Ukrainian units relied heavily on aging Soviet-era systems and improvised solutions, leaving communications insecure and disjointed.[15] Over the period 2014 to early 2022, Ukraine undertook significant efforts to modernise both tactical battlefield communications and its strategic command infrastructure. In addition, Ukraine's existing public and private digital infrastructure played a crucial role in sustaining operations during the initial days and months of the war, before military-grade systems were widely integrated across the Armed Forces. 79 percent of the population had internet access as of 2021. By that same year, 4G services reached 91.6 percent of the population, reflecting the country's extensive broadband coverage.[16]

This section analyses the upgrades of Ukrainian military communications—covering the technologies employed, their distribution and upgrades, major modernisation programs, and persistent challenges.

1. Resilient satellite communications are vital for maintaining connectivity under electronic and kinetic attack.

Ukraine's rapid adoption of satellite internet terminals provided vital connectivity when traditional networks failed under Russian attacks and EW.[17] Low-Earth orbit constellations, such as Starlink, gave the frontline units access to reliable internet connectivity that withstood intensive jamming and cyber attacks. In fact, a U.S. Space Force commander confirmed that Russia tried to jam Starlink and failed, largely due to its design and SpaceX's quick software updates to overcome interference.

In addition, Ukraine gained access to satellite communications through NATO-supported initiatives aimed at enhancing secure communications and force positioning.[18] The process

14 "U.S. Provided Intelligence That Helped Ukraine Sink Russian Warship," The Washington Post, May 5, 2022, accessed March 24, 2025, https://www.washingtonpost.com/national-security/2022/05/05/us-intelligence-ukraine-moskva-sinking/.

15 "NATO's Support of Ukraine's C4 Capabilities," AFCEA International, December 7, 2023, https://www.afcea.org/signal-media/defense-operations/natos-support-ukraines-c4-capabilities#:~:text=A%20targeted%20NATO%20trust%20fund,TechNet%20Transatlantic%20on%20December%207.

16 "Telecommunication in Ukraine," Worlddata.info, n.d., https://www.worlddata.info/europe/ukraine/telecommunication.php.

17 "Starlink and the Russia-Ukraine War: A Case of Commercial Technology and Public Purpose?," The Belfer Center for Science and International Affairs, March 9, 2023, https://www.belfercenter.org/publication/starlink-and-russia-ukraine-war-case-commercial-technology-and-public-purpose#:~:text=Just%20a%20few%20days%20into,a%20few%20hours%20for%20SpaceX.

18 "NATO's Support of Ukraine's C4 Capabilities," AFCEA International, December 7, 2023, https://www.afcea.org/signal-media/defense-operations/natos-support-ukraines-c4-capabilities.

began with the Enhanced Mobile Centralized System (EMCS), which leverages the Iridium satellite system to connect secure radios and GPS trackers, providing real-time force positioning and command-and-control communications. Initially adopted in 2018, the system saw increasing use by the Ukrainian Navy and Army, significantly improving situational awareness and secure information exchange. Building on this foundation, NATO expanded Ukraine's satellite communication capabilities through the Slingshot program, which integrates tactical combat radios with SATCOM, further strengthening command, control, and ISR capabilities across military operations.

2. Securing battlefield communications requires both advanced equipment and disciplined operational procedures.

While efforts to standardise on military-grade systems were underway, civilian infrastructure remained a critical component—particularly in rear areas or newly contested zones.

In the early years of the war in Donbas, many Ukrainian units were equipped with analog Soviet radios or commercial walkie-talkies, which were extremely vulnerable to these attacks. Troops often resorted to using personal cell phones or unencrypted devices, which enabled Russian SIGINT units to intercept calls, triangulate positions, and in several well-documented cases, direct lethal artillery strikes.

As a response, Ukraine rapidly prioritised acquisition of secure, frequency-hopping radios, such as the U.S.-made Harris RF-7800V and Turkish Aselsan software-defined radios. These systems offered AES encryption and frequency agility, making them far more resilient to jamming and eavesdropping. Notably, even under heavy Russian EW pressure in Donbas, the Harris radios using SINCGARS waveforms were not degraded, validating the importance of NATO-grade radios.[19]

Ukraine also implemented communications discipline protocols, discouraging cell phone use near the front and training units in burst transmissions, directional antennas, and frequent channel switching. In 2021, Aselsan radios were even updated with a Digital Mobile Radio (DMR) mode to securely interoperate with the widespread Motorola systems still in use. These technical and procedural adaptations allowed Ukrainian forces to sustain communications under electronic attack, and to deny Russian forces a major EW advantage.

3. Public-private collaboration enhances communication resilience and flexibility in wartime.

Ukraine's extensive use of civilian telecom infrastructure illustrated how public-private partnerships can enable and improve battlefield communications. While efforts to standardise on military-grade systems were underway, civilian infrastructure remained a critical component—particularly in rear areas or newly contested zones. Civil telecom companies, sometimes with support from volunteers and civil society, quickly repaired damaged fiber lines, installed portable cell towers, and maintained 4G access under wartime conditions.[20] This infrastructure helped the Ukrainian military to leverage civilian messaging apps (such as

[19] Defense Security Monitor, "Life in the Old SINCGARS Waveform Yet!," May 20, 2022, https://dsm.forecastinternational.com/2022/05/17/life-in-the-old-waveform-yet/#:~:text=collection%20and%20communications%20jamming,suffered%20adversely%20from%20any%20jamming.

[20] "Rebuilding Ukraine's Telecoms Infrastructure Amid War," DCD, January 9, 2024, https://www.datacenterdynamics.com/en/analysis/rebuilding-ukraines-telecoms-infrastructure-amid-war/.

Telegram, Signal) for certain communications when appropriate.[21] The military worked with Ukraine's tech sector to develop secure messaging platforms (one example is "MilChat," a secure military messenger developed by volunteers).

This hybrid approach greatly increased communications redundancy and enabled faster decision-making on the ground. However, it also came with cybersecurity tradeoffs. Civilian platforms are more easily surveilled or disrupted, so Ukraine took steps to isolate sensitive channels, restrict usage by rank or location, and train soldiers on OpSec best practices when operating in mixed civilian/military systems.

4. Long-term NATO interoperability planning enabled seamless wartime integration of allied communications systems.

A crucial long-term success story in Ukraine's comms modernisation is its strategic focus on NATO interoperability, which began after 2014 and intensified through 2021.

A crucial long-term success story in Ukraine's comms modernisation is its strategic focus on NATO interoperability, which began after 2014 and intensified through 2021.[22] Ukraine deliberately adopted NATO-compatible encryption, waveforms, and protocols when selecting new radio systems. For example, both the Harris RF-7800V (used by U.S. forces) and Aselsan VRC/PRC radios (used by NATO allies like Turkey) were evaluated for encryption robustness and waveform compatibility, ensuring that joint operations would not require custom bridging or workarounds.

At the strategic level, Ukraine's Delta situational awareness system was built on NATO-standard data formats[23], including compatibility with Link 16 and other tactical data links, which allows real-time or near-real-time sharing of targeting data, sensor feeds, and positional updates between NATO and Ukrainian forces. As of late 2021, this meant that AWACS surveillance, ISR drone feeds, and satellite imagery could be piped into Ukrainian command networks with minimal friction.

At the procedural level, Ukraine also transitioned its command structures to NATO-style J-code staff models and adopted NATO communications security doctrines (including crypto key management and message classification procedures). This enabled smoother collaboration in exercises and laid the groundwork for rapid integration of allied systems in wartime.

When the full-scale invasion began in 2022, this pre-existing technical and doctrinal compatibility allowed Ukraine to absorb Western support efficiently, maintain joint communications channels, and securely share intelligence, giving it a critical edge in agility and situational awareness from day one.

---

21 "Ukrainian Soldiers' Apps Increasingly Targeted for Spying, Cyber Agency Warns," The Record From Recorded Future News, April 19, 2024, https://therecord.media/ukraine-military-personnel-cyber-espionage-uac-0184.

22 "NATO's Support of Ukraine's C4 Capabilities," AFCEA International, December 7, 2023, https://www.afcea.org/signal-media/defense-operations/natos-support-ukraines-c4-capabilities.

23 Daryna Vialko, "First Time in History: Ukrainian Combat System DELTA Passes NATO Standards Test," *RBC-Ukraine*, July 17, 2024, https://newsukraine.rbc.ua/news/first-time-in-history-ukrainian-combat-system-1721243988.html.

Computers

In the context of C4ISR, computers include the information technology infrastructure and computational capabilities that underpin command and control. This category includes both hardware and software used for data processing, storage, and dissemination—ranging from servers and cloud computing platforms to battlefield management software, databases, and AI algorithms. These interconnected systems serve as the digital foundation of military operations by managing information flows, enabling automated processes, and supporting the operation of advanced weaponry.

Ukraine's Armed Forces have developed a comprehensive suite of software tools to manage operations across all levels, from individual troop mapping applications to advanced operational planning systems.

Similar to its approach in communications, the Ukrainian military used both civilian and military solutions, integrating technologies developed by volunteer groups directly into frontline operations while gradually formalizing them at the doctrinal level. Simultaneously, the adoption of NATO standards and initiatives in C4ISR—introduced after the war in Donbas and expanded before the full-scale invasion—played a crucial role in enhancing digital infrastructure and preparing personnel to effectively use and integrate these technologies into command and control. Based on this experience, the following lessons can be drawn:

1. A robust digital ecosystem for battlefield management accelerates coordination and decision-making at every operational level.

Ukraine's Armed Forces have developed a comprehensive suite of software tools to manage operations across all levels, from individual troop mapping applications to advanced operational planning systems. A key component of this digital infrastructure is the Delta system, officially adopted by the Ministry of Defense in 2023 as part of Ukraine's broader cyber capabilities. As a cloud-based platform,[24] Delta integrates multiple applications that enhance battlefield coordination and situational awareness. It includes Delta Monitor, which provides intelligence insights on a digital map; Vezha, which streams real-time drone footage; and Mission Control, which facilitates drone coordination to prevent friendly jamming and frequency conflicts. Beyond software applications, Delta also serves as a connective hub for various hardware components, linking, for example, drones, tablets, communication devices, and weapon systems to ensure seamless information flow between frontline operators and command centers and mission coordination.

Alongside official platforms, volunteer software engineers continuously develop and update tools that improve situational awareness and streamline fire-control processes. The Armor system improves indirect fire targeting for armored units, cutting coordination time from 20–25 minutes to just 5–7 minutes. Situational centers, operated by a non-government organisation Aerorozvidka, integrate intelligence, surveillance, and reconnaissance (ISTAR) data to enhance command efficiency, with eight centers supporting frontline operations.[25] These systems show a broader digital ecosystem that supports battlefield management in Ukraine, demonstrating how agile software development can enhance operational effectiveness by integrating real-time intelligence, automation, and user-driven feedback loops.

[24] Kateryna Bondar, "Does Ukraine Already Have Functional CJADC2 Technology?," January 21, 2025, https://www.csis.org/analysis/does-ukraine-already-have-functional-cjadc2-technology.

[25] "ISTAR | ГО Аеророзвідка," n.d. https://aerorozvidka.ngo/direction/istar.

2. Proactive cybersecurity and resilient infrastructure are indispensable for countering large-scale cyber threats.

Ukraine's experience shows the necessity of proactive cybersecurity measures and resilient infrastructure to withstand large-scale cyber threats. Within the first six months of the war, Russian cyber operations targeted Ukraine with over 1,100 attacks,[26] ranging from website defacements and power grid disruptions to the large-scale Viasat satellite hack on the first day of the invasion. Anticipating and reacting to such threats, international technology companies played a key role in strengthening Ukraine's digital defenses. For example, Microsoft assisted in relocating Ukrainian government data centers abroad even before the war and with the beginning of full scale invasion.

Within the first six months of the war, Russian cyber operations targeted Ukraine with over 1,100 attacks, ranging from website defacements and power grid disruptions to the large-scale Viasat satellite hack on the first day of the invasion.

Meanwhile, there is an example of effective cyber resilience,[27] which was provided by Cisco. The company developed custom-built industrial Ethernet switches to counter Russian electronic warfare targeting Ukraine's power grid. Designed to function independently of GPS, these switches maintained synchronisation between substations despite persistent jamming attempts. Following successful testing, Cisco—supported by the U.S. government—delivered dozens of these devices to Ukrenergo, enhancing the grid's ability to withstand cyber and electronic disruptions. This case demonstrated the importance of integrating smart, hardware-and software-based solutions alongside traditional cybersecurity measures to ensure operational continuity in contested environments.

3. Digitised logistics and cloud-based planning ensure agile and sustainable military operations under extreme conditions.

Ukraine's experience highlights the crucial role of digital logistics in sustaining military operations under wartime conditions. Supported by NATO advisers, Ukraine is implementing automated supply chain management to track inventories, optimise resupply, and quickly adapt to frontline needs.[28] A key advancement was the Ministry of Defense's adoption of System Analysis Program Development (SAP), a NATO-standard platform used by 28 member states. SAP replaces paper-based processes, centralises warehouse inventories, streamlines procurement, and enhances accountability in tracking international military aid.

This integration of logistics into C4ISR improves both operational agility and sustainment. When military systems proved slow, Ukrainian logisticians leveraged commercial tools like Google Sheets and WhatsApp for rapid coordination, while cloud-based collaboration enabled planners to work remotely. With full SAP Ukraine will achieve complete automation of military logistics, offering a scalable model for NATO and allied forces seeking more efficient, digitally-driven logistics management.

---

26 Nino Kubinidze et al., "Interim Assessment on Damages to Telecommunication Infrastructure and Resilience of the ICT Ecosystem in Ukraine," December, 2022, https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Interim%20assessment%20on%20damages%20to%20telecommunication%20infrastructure%20and%20resilience%20of%20the%20ICT%20ecosystem%20in%20Ukraine%20-2022-12-22_FINAL.pdf.

27 Lance Luo, "Tech Giant Cisco Built Special Device to Help Kyiv Ward off Cyberattacks on Power Grid," *The Kyiv Independent*, November 26, 2023, https://kyivindependent.com/tech-giant-cisco-built-special-device-to-help-kyiv-ward-off-cyberattacks-on-power-grid/.

28 "Міністерство Оборони України," Telegram, January 12, 2024, https://t.me/ministry_of_defense_ua/8622.

Intelligence, Surveillance, and Reconnaissance (ISR)

The battlefield in Ukraine differs significantly from previous full-scale conflicts, primarily due to the unprecedented proliferation of sensors, the widespread deployment of unmanned systems, and the exponential growth in data generation. These factors, combined with advanced data processing and analysis capabilities, contribute to an autonomous operational paradigm where real-time situational awareness enables machines to interpret and respond effectively to the battlefield environment.

The Ukrainian military processes tens of terabytes of intelligence daily, including video, photo, acoustic, and text data streams. Once analysed, this information is sent back to the front line as a detailed operational picture, displaying enemy locations, equipment, movements, and activities on digital maps. This processed intelligence is accessible to unit commanders and even individual warfighters via phones and tablets, ensuring near-instantaneous situational awareness and decision-making at all levels. Such a considerable improvement in situational awareness provides following takeaways:

The Ukrainian military processes tens of terabytes of intelligence daily, including video, photo, acoustic, and text data streams.

1. Software innovations in ISR automate data analysis, significantly reducing human workload and speeding intelligence cycles.

AI integration has streamlined ISR workflows, enabling rapid data fusion from multiple sensors. UAVs equipped with AI-assisted analysis tools can transmit already analysed information to the operator or command center. AI-enabled tools within Delta system can autonomously process video streams, prioritise actionable intelligence, and integrate findings into command systems. Automated acoustic reconnaissance systems like Zvook complement ISR by detecting enemy drone and missile threats through sound analysis, covering approximately 20,000 square kilometers[29] of Ukraine's airspace with a 12-second response time. These AI-driven ISR capabilities have significantly improved the speed and accuracy of intelligence processing, reducing the risk of information overload on human operators.

2. AI-enabled target recognition expands ISR effectiveness by reducing human error in identifying hostile assets.

Automatic target recognition systems onboard drones and reconnaissance platforms have drastically reduced human error in target identification. Ukrainian-developed AI models can now recognise and classify Russian vehicles and personnel up to 2 km away, even in degraded visual conditions. Such systems like ZIR and other AI-powered autonomy kits have enabled drones to lock onto targets with greater precision, particularly in GPS-jammed environments. These advancements have enhanced the effectiveness of Ukraine's drone warfare strategy, enabling precise targeting while minimizing collateral damage.

[29] Fedorchuk Sergii, "Штучний Інтелект У ЗСУ: Сержант Сил ППО Розкрив Деталі Роботи Інноваційних Систем Zvook," Прямий (blog), August 1, 2024, https://prm.ua/shi-v-ukrainskomu-viysku-serzhant-zsu-rozkryv-detali-roboty-innovatsiynykh-system-ppo/#google_vignette.

3. Real-time ISR integration into situational awareness systems is critical for distributed, high-speed decision-making.

ISR data is only as valuable as its integration into decision-making frameworks. Ukrainian forces have mandated that all unmanned and reconnaissance systems feed directly into shared situational awareness and fire correction platforms. Even foreign manufacturers, such as Skydio, have integrated their drones with Ukraine's Delta system to ensure seamless data sharing. This real-time ISR network enables distributed decision-making, improving Ukraine's ability to track enemy movements, anticipate attacks, and coordinate fire missions with unparalleled speed.

4. Crowdsourced ISR and civilian participation provide strategic advantages by broadening intelligence sources.

These systems demonstrate that ISR does not need to be limited to traditional military assets—AI-driven civilian participation has created a force multiplier effect for Ukraine's intelligence operations.

Ukraine has successfully leveraged civilian ISR contributions through applications like ePPO, which allows verified users to report missile and drone threats. With over 600,000 downloads and 200,000 active users,[30] this crowdsourced air defense network provides real-time intelligence on incoming threats, significantly improving response times. Similarly, AI-powered text analysis platforms such as Griselda process intercepted Russian communications and battlefield reports, automatically extracting key intelligence. These systems demonstrate that ISR does not need to be limited to traditional military assets—AI-driven civilian participation has created a force multiplier effect for Ukraine's intelligence operations.

5. AI-driven ISR strengthens decision superiority in multi-domain operations by providing actionable insights in near real time.

The fusion of AI-enhanced ISR across land, air, and cyber domains has provided Ukraine with a real-time operational picture that enhances decision-making across all levels of command. AI algorithms synthesise ISR data and in near future will be able to recommend prioritised targets, predict enemy logistics movements, and assess battlefield vulnerabilities. The increasing demand for AI-powered ISR solutions suggests that NATO and allied forces should focus on integrating autonomous data processing and decision-support tools to maintain operational superiority in future conflicts.

6. AI Integration in ISR is more effective through curation of standard datasets and small AI models for specific tasks

Ukraine's approach to integration AI into ISR is based of standardisation of data curation and the development of specialised AI models for targeted operational tasks. Rather than relying on centralised efforts conducted by the Ministry of Defense only, military and private-sector teams collaboratively structure and label datasets—ranging from drone feeds to satellite imagery. This standardised approach improves efficiency, allowing AI models to quickly

[30] Valerii Bilyk, "The Ministry of Defense Announced the Significant Effectiveness of the "ePPO" Application in Protecting the Ukrainian Sky," Новини ФАКТ, November 25, 2024, https://fact-news.com.ua/en/the-ministry-of-defense-announced-the-significant-effectiveness-of-the-eppo-application-in-protecting-the-ukrainian-sky/.

process relevant intelligence while filtering out unnecessary data. Additionally, Ukraine has prioritised smaller, task-specific AI models over large, generalised systems. These focused models, trained on curated subsets of ISR data, enhance precision and adaptability. This modular approach to AI ensures faster deployment, greater flexibility, and higher accuracy in intelligence processing.

Conclusion

The key takeaway is that success in high-intensity conflict relies on continuous learning, agile procedures, and an operational culture that encourages creative problem-solving and immediate feedback loops.

Ukraine's wartime innovations in C4ISR show how armed forces, even under severe resource constraints, can achieve rapid and sometimes unexpected advantages by fusing commercial technologies, AI-driven intelligence, and adaptable command structures. The key takeaway is that success in high-intensity conflict relies on continuous learning, agile procedures, and an operational culture that encourages creative problem-solving and immediate feedback loops. In other words, the Ukrainian experience shows that technological sophistication alone is insufficient without the right balance of skilled personnel, procedural flexibility, and cross-domain synergy. Given the lessons learned from the war in Ukraine, NATO allies should consider the following recommendations to be implemented:

1. Formalise public-private and international collaboration

Traditional defense procurement cycles lag behind the rapid innovation seen in the commercial sector. To keep pace, militaries and alliances like NATO should forge formal partnerships with private technology firms and international allies. Such collaborations allow a quick co-development of solutions and faster transitions from prototype to field use. This process also benefits from frequent, iterative testing under realistic conditions, enabling immediate refinements. Success here depends on ensuring that personnel at all levels understand how to work effectively with external partners—whether they are domestic telecom companies, multinational defense contractors, or allied military forces. Strong and clear frameworks for knowledge exchange, legal agreements, and intellectual property rights help maintain momentum and trust.

2. Standardise data protocols and interoperability measures

Seamless information sharing is paramount in coalition operations, yet it is often hampered by incompatible data formats, closed systems or numerous new systems, which are not integrated into existing data management and data analysis platforms. To overcome these barriers, NATO members and partners should implement universal data standards and commit to frequent joint exercises that test and refine interoperability. This standardisation allows real-time intelligence feeds to flow unimpeded across different platforms and national forces, expediting decision-making under pressure. Technically, standardised protocols simplify integration with advanced surveillance assets, while operationally, they ensure that personnel can interpret and act on shared intelligence without losing critical time. A standing team or Centre of Excellence devoted to these standards can help monitor compliance and rapidly address emerging technical issues.

3. Adopt modular, task-focused AI for ISR and decision-support

Given the sheer volume of battlefield data in contemporary conflicts, human analysts can easily be overwhelmed. Smaller, specialised AI models designed for discrete tasks—such as identifying specific vehicle types or analyzing particular radio frequencies—offer a more agile and accurate alternative to monolithic, general-purpose systems. These task-focused models can be rapidly retrained and redeployed based on lessons learned in the field, creating a continuous feedback loop. Crucially, personnel must be trained not only to operate these AI tools but also to understand their limitations, ensuring that human judgment complements rather than cedes entirely to machine recommendations.

4. Invest heavily in EW countermeasures and secure communications

Modern battlefields are saturated with electronic warfare threats, from signal jamming to interception of sensitive communications. To counter these challenges, NATO forces should adopt a dual strategy of advanced technology acquisition and disciplined operational procedures. On the hardware side, radios with robust encryption standards guard against eavesdropping and interference. Equally crucial is the human dimension: regular training drills on communication discipline—such as minimising transmission time and switching frequencies frequently—bolster preparedness. Taken together, these measures ensure that militaries can maintain cohesive command and control even when facing sophisticated EW attacks.

By actively seeking partnerships with Ukrainian startups, research centers, and military technologists, NATO can tap into a reservoir of field-tested solutions.

5. Expand direct collaboration with Ukrainian defense innovators

Ukraine's defense sector has acquired a wealth of practical combat experience under the most demanding conditions. By actively seeking partnerships with Ukrainian startups, research centers, and military technologists, NATO can tap into a reservoir of field-tested solutions. Joint R&D projects, short pilot deployments, and fast-track contracting can rapidly bring these innovations to a broader set of allied forces. At the same time, Ukrainian partners gain new resources and insights from NATO's organisational and technological depth, creating a virtuous cycle of mutual benefit.

By systematically revisiting the key challenges Ukraine encountered, its continuous learning cycle, and the balanced integration of technology, people, and procedures, NATO can fortify its own C4ISR architecture to stay agile and effective in future conflicts.

The Hague Centre
for Strategic Studies

HCSS
Lange Voorhout 1
2514 EA The Hague

Follow us on social media:
@hcssnl

The Hague Centre for Strategic Studies
Email: info@hcss.nl
Website: www.hcss.nl