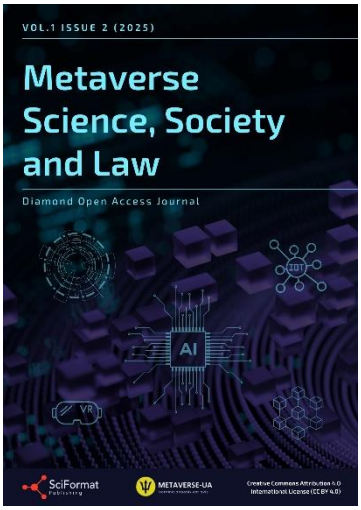

Metaverse Science, Society and Law

Vol. 1, Issue 2 (2025)

SciFormat Publishing

Publisher:
SciFormat Publishing Inc.

ISNI: 0000 0005 1449 8214
2734 17 Avenue Southwest, Calgary,
Alberta, Canada, T3E0A7

+15878858911
editorial-office@sciformat.ca

ARTICLE TITLE	AI-ENABLED DRONES: THE CASE OF THE RUSSO-UKRAINIAN WAR AND ITS FAR-REACHING CONSEQUENCES
DOI	https://doi.org/10.69635/mssl.2025.1.2.22
RECEIVED	26 July 2025
ACCEPTED	29 September 2025
PUBLISHED	13 October 2025
LICENSE	The article is licensed under a **Creative Commons Attribution 4.0 International License.**

AI-ENABLED DRONES: THE CASE OF THE RUSSO-UKRAINIAN WAR AND ITS FAR-REACHING CONSEQUENCES

Yulia Razmetaeva
Ph.D., Centre for Multidisciplinary Research on Religion and Society, Department of Theology, Uppsala University, Thunbergsvagen 3B, 752 38, Uppsala, Sweden; Department of Human Rights and Legal Methodology, Center for Law, Ethics and Digital Technologies, Yaroslav Mudryi National Law University, Hryhoriia Skovorody Street 77, 61024, Kharkiv, Ukraine.
ORCID ID: 0000-0003-0277-0554

ABSTRACT

The Russo-Ukrainian War has significantly accelerated the integration of artificial intelligence (AI) and drones (or unmanned aerial systems) into modern military operations, transforming security and defence. Traditional doctrines, centred on static, physical defences, have proven insufficient against the speed and adaptability of AI-enabled drone warfare. Drawing on recent operational evidence, this paper identifies three doctrinal shifts: the replacement of fixed defences with dynamic monitoring networks, based on collaborative human-AI decision-making; the decentralization of innovation through collaboration between military units and civilian actors; and the recognition of drones as inherently dual-use technologies requiring tailored policy frameworks. By analysing Ukraine's adaptive approach to limited resources, the study underscores the strategic advantages of proactive detection, predictive analytics, and rapid technological iteration. These findings suggest that states that integrate AI-driven anticipation and dual-use preparedness into their doctrines will be better positioned to safeguard the civilian population and critical infrastructure in an era of rapid technological diffusion and evolving threats.

KEYWORDS

Artificial Intelligence, AI-Enabled Drones, Decision-Making, Drones, Human-AI Collaboration, Russo-Ukrainian War, Security and Defence Doctrine, Warfare

CITATION

Yulia Razmetaeva (2025) AI-Enabled Drones: The Case of The Russo-Ukrainian War and Its Far-Reaching Consequences. *Metaverse Science, Society and Law*. Vol. 1, Issue 2. doi: 10.69635/mssl.2025.1.2.22

1. Introduction

The ongoing Russo-Ukrainian war has revealed a striking shift in the nature of military innovation. Conventional security and defence doctrines appear increasingly outdated in the face of asymmetric warfare and technological improvisation. When faced with limited resources, both sides – particularly Ukraine – have resorted to rapid, inventive solutions that have accelerated the development of emerging military technologies, especially AI-enabled drones.

The battlefield has become a dynamic testing ground for adaptive systems, providing invaluable empirical insights for security and defence research. In this context, prioritizing *proactive* detection and AI-based situational awareness over purely physical defensive measures has emerged as a critical necessity. The Russo-Ukrainian War may thus be seen as the first large-scale "drone war," analogous to how the First World War represented the birth of air combat (DeVore, 2023). If this marks the beginning of a global drone revolution, the long-standing correlation between economic capacity and military power could weaken significantly or even disappear (Calcara et al., 2022, p. 132).

Recent conflicts have demonstrated that drone technology, though often designed for civilian use, can be quickly adapted for military purposes. Caballero-Martin et al. (2024) highlight their widespread application in infrastructure inspection, disaster prevention, environmental monitoring, and precision agriculture – uses that translate easily into surveillance, targeting, and strike capabilities. Ukraine's reliance on rapid adaptation

stems from necessity: facing a better-equipped adversary, both military units and private innovators modify civil technologies and platforms into effective battlefield tools. This adaptability mirrors trends in earlier technological shifts, where wartime pressures accelerated innovation cycles and blurred the boundaries between civilian and military applications.

AI-enabled drones are apparently becoming crucial and indispensable for any defensive strategy. Some experts are sceptical about the disruptive impact of AI drones (Kirichenko, 2025), especially autonomous drone swarms (King, 2024), claiming that they have not yet changed the potential of offensive and defensive activities. Others argue that even simple, one-way attack drones "present new opportunities for a greater range of would-be attackers", and "have in essence diffused precision strike vertically and horizontally" (Plichta & Rossiter, 2024, p. 1009). Small drones already have had their greatest impact in less dramatic roles – serving as aerial scouts that help soldiers detect enemy positions and direct artillery fire, thereby improving the speed and accuracy of ground operations while reducing troop exposure to danger (Kunertova, 2023). The ability to manufacture and deploy such small uncrewed aerial systems on demand is likely to entail a reassessment of how military innovation is understood by scholars (Dawson & Nadal, 2024, p. 324), as well as of how the proper protection of population and infrastructure can be implemented.

According to Tweneboah-Koduah and Buchanan, critical infrastructure systems are becoming too complex and dynamic to predict due to their convergence with advanced technologies, while interdependencies blur system boundaries, making them harder to define. Despite the wide range of risk assessment methods available, the complexity and interdependencies of modern systems reduce their effectiveness. This calls for new approaches to handling risks, as no single universal solution can address all security challenges (Tweneboah-Koduah & Buchanan, 2018). The Russia–Ukraine conflict has underscored emerging hybrid threats to logistics infrastructure, including strikes on supply nodes, cyberattacks, underwater sabotage, and hard-to-trace asymmetric operations (Slusher, 2025). Evolving cyber threats are driving more sophisticated and targeted attacks against infrastructures that provide essential services across various sectors, including government, energy, healthcare, transportation, and telecommunications – high-risk assets vital to safety, efficiency, and reliability. Nations must identify and address all potential threats while developing strategies to maintain resilience (Roshanaei, 2021). The double complexity outlined above makes the task of elaborating protection strategies very far from trivial.

As was shown in the Global Peace Index 2025, investments are increasingly channelled into cutting-edge areas such as AI, autonomous systems like drones and unmanned underwater vehicles, cyber warfare capabilities, space-based assets, advanced sensors, and sophisticated missile technology (Institute for Economics & Peace, 2025). Since 2022, all nuclear-armed states have maintained or expanded their arsenals, while great-power competition is driving an arms race in advanced technologies ranging from AI-enabled drones to counter-space systems (Institute for Economics & Peace, 2025). However, along with investments in cutting-edge systems, a review of key defence doctrines is needed, which would ensure an anticipative approach and maximize the effect of the technologies in question.

Ukraine's experience proves that three key doctrinal shifts need to be recognised: 1. A need for *transition from fixed defences to dynamic networks*. Instead of static protection, it has been shown that flexible, layered systems that combine electronic countermeasures, rapid-response strike capabilities, AI-assisted monitoring, and decision-making achieve the best results. 2. A need to *decentralize innovation*. Encouraging bottom-up adaptation from field units and civilian partners dramatically accelerates technological iteration and ensures relevance to battlefield realities. 3. A need for *dual-use policy planning*. Recognizing the inevitable overlap between civilian and military drone technology, states can be advised to prepare both legal frameworks and industrial policies to manage and exploit this duality. These principles align with historical precedents: as with the early days of air warfare, effective doctrine must evolve in parallel with technological possibilities, rather than lag behind them.

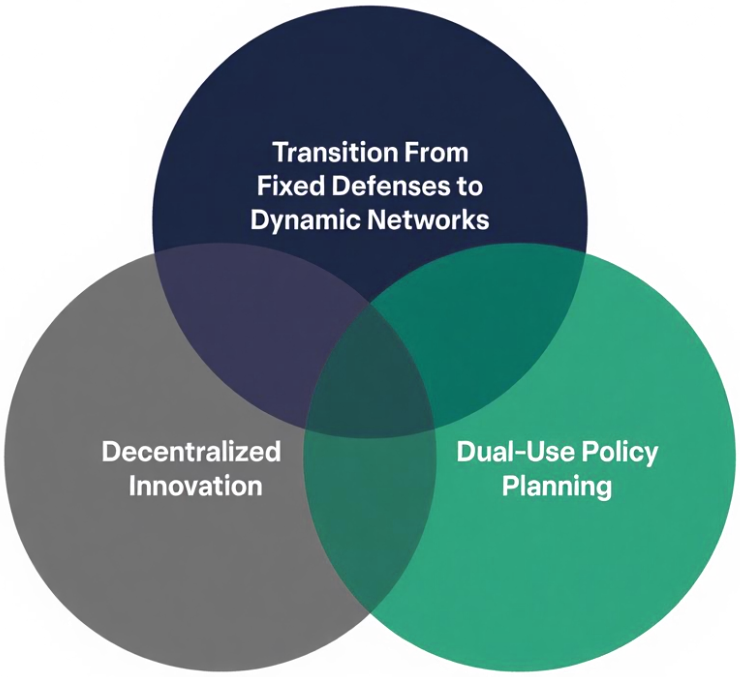

Fig. 1. *Key Doctrinal Shifts*

This paper intends to outline the current doctrine of security and defence against the backdrop of AI-enabled drone threats. It is based mainly on the lessons of the Russia–Ukraine war. Particular attention is paid to the shift in human-machine collaboration that is manifested in decision-making with the involvement of AI.

The theoretical framework of this article embraces the dual-use theory. This theory (See Atlas & Dando, 2006; Miller & Selgelid, 2007) is applied as a framework for understanding the ethical tension between the innovative potential of certain technologies for societal benefit and their capacity for misuse with applications, particularly across AI and military innovations domains (De Ágreda, 2020; Grinbaum & Adomaitis, 2024). The approach to human-AI interaction in collaborative decision-making was grounded in the concepts of trust in advanced technologies, including AI (Glikson & Woolley, 2020; Gillath et al., 2021; Choung et al., 2023), and the acceptance/unacceptance of AI in automated decision-making (Helberger et al., 2020; Araujo et al., 2020; Schaap et al., 2024).

2. AI-Enabled Drones in Modern Warfare: The Case of Russo-Ukrainian War

Unmanned aerial systems (UAS) have already reshaped modern warfare, and the integration of AI into drone technology promises to deepen this transformation. The Russo-Ukrainian war has marked a qualitative leap in both the development and operational use of diverse drone platforms. As Kunertova observes, the realisation of the value of deploying a wide variety of drones to accomplish military objectives has become a critical emerging technology lesson taught by the conflict (Kunertova, 2023).

The evolution of drones in Ukraine is multifaceted, patchy, and multi-directional, depending on the resources available, technical ingenuity, and the necessity to address the ever-changing battlefield requirements. According to Zaluzhnyi, the former Commander-in-Chief of the Armed Forces of Ukraine, low-cost maritime drones have driven the Russian Black Sea fleet out of its seemingly impenetrable Crimean harbour, while unarmed drones conduct continuous logistical and medical evacuation operations. He highlights that these drones are rarely proprietary products of traditional defence contractors; instead, they are largely assembled from commercially available hardware and open-source software, enabling cost-effective attrition warfare at scale (Zaluzhnyi, 2025).

Combat conditions have accelerated the enhancement of drones not originally designed for AI integration. In particular, Ukrainian innovations in electronic protection have improved short-range tactical strike systems, while both sides have expanded the use of first-person view (FPV) drones. Upgrades such as autonomous terminal guidance and wire-spool mechanisms have rendered FPVs resistant to electronic disruption. Tactical unmanned aerial vehicles (UAVs), despite their limitations, currently account for 60–70% of destroyed or damaged Russian

assets (Watling & Reynolds, 2025, p. 10). As of today, only a certain percentage of drones deployed are AI-enabled; however, this is and will be changing as better efficiency is needed.

Several types of AI-enabled drones, developed domestically and through international partnerships, are now in Ukrainian service, reflecting a strategy to secure a technological edge over Russian forces (Khomenko, 2024). In December 2024, Ukrainian forces for the first time executed an attack solely with ground-based and FPV drones, demonstrating a significant evolution in unmanned warfare tactics (Bendett & Kirichenko, 2025). The operation, conducted near Kharkiv, deployed a mix of machine-gun-equipped ground drones and kamikaze FPVs. While these platforms remained remotely controlled and required substantial human oversight, they represent an early step toward more autonomous combat systems. Notably, a ground robot was previously used in a September 2024 assault on a Russian trench in Kursk Oblast (Axe, 2024a).

Expectedly, AI integration extends beyond strike platforms. Ukraine's DELTA battlefield management system utilizes AI to rapidly process data and provide commanders with a comprehensive operational picture, including target repositories for kinetic or cyber strikes. Enhanced data-sharing and unmanned command-and-control centres have evolved to meet the war demands, subsequently embedding the data, AI, and drones into the norm (Zaluzhnyi, 2025). These capabilities are crucial given Ukraine's significant manpower disadvantage along the war's 1,200-kilometer front.

It is still debatable whether fully autonomous weapons are in use. Ukrainian military discourse often conflates "autonomous" with "unmanned" systems or those featuring limited autonomous functions such as navigation and targeting (Bondar, 2025b). Nonetheless, some analysts warn that "a dystopian future in which swarms of killer drones hunt for human targets is drawing closer" (Chapple, 2024). Others believe that predictions of an imminent AI drone revolution remain premature as of June 2025. Both Russia and Ukraine require additional time, testing, and investment before AI-enabled drones can be deployed at scale. AI/ML-enabled drones are unlikely to replace the mass of tactical FPV drones in the near future due to the latter's lower cost and adaptability to current battlefield conditions (Stepanenko, 2025).

At the same time, the conflict has produced several historical firsts: a drone-on-drone aerial engagement between Russian and Ukrainian systems (Hambling, 2022); the destruction of a Russian helicopter by an FPV drone (Axe, 2024b); the sinking of a Russian aircraft by an uncrewed surface vessel (Newdic, 2024); delivery of blood for transfusion to a critically wounded Ukrainian soldier at the front line (Kushnikov, 2025); the capture of Russian troops by drones (Zoria, 2025); the development of an AI-enabled "mother drone" capable of carrying two AI-guided FPV strike drones over up to 300 kilometres (Fratsyvir, 2025); the first autonomous missions of the AI-enabled mothership drone "GOGOL-M" (Hambling, 2025b) – and the list goes on. These breakthroughs illustrate not only technical progress in drone development but also the creativity of battlefield applications.

Innovations like the above have serious implications for security and defence. In the future, attacks may be designed in ways that are harder to anticipate and refute. In a hypothetical situation, for instance, a drone seemingly filming a wedding near a sensitive facility could be covertly collecting targeting data. AI could later process this data to identify vulnerabilities. Ultimately, a pizza deliveryman's motorcycle will stop near the facility, three small drones with explosives emerging out of their bag, instantly hitting the targets.

AI-enabled or not, drones may exert serious effects on the protection of the civil population and critical infrastructure both in peacetime and in times of warfare. As Calcara et al. (2022) point out, their size and design enable them to evade detection more effectively than traditional aircraft, facilitating penetration of enemy air defences and favouring offensive operations. Second, their relative affordability and technical simplicity lower barriers to advanced military capabilities, thereby reducing asymmetries in power and potentially empowering weaker actors (Calcara et al., 2022, p. 131).

Several key lessons can be extracted from the Russo-Ukrainian conflict. It has been demonstrated that unmanned systems dramatically extend operational reach while reducing risk to personnel. They enable engagement at greater distances, often beyond the range of direct-fire weapons, and have fundamentally altered tactical and operational planning (Slusher, 2025). According to DeVore (2023), two clear lessons emerge despite limited data about the present war: "the centrality of attrition rates and cost factors, and the importance of rapid adaptation cycles over exquisitely engineered weapons" (DeVore, 2023). The war is driving drone proliferation and confirming trends toward greater stealth, speed, lethality, and accessibility for more actors (Kunertova, 2023). Other insights from Ukraine's rapid drone innovation include fast and easy testing, frontline-localized research and development, and strong local representation in development (Bondar, 2024).

Three shifts manifested by the Russo-Ukrainian war appear to be crucial for the effective defensive activity in the new epoch. *Adaptation* and *decentralized innovation* have proven decisive. The rapid adaptation of solutions and their continuous testing on the battlefield helped to partially level the asymmetry in the resources of the warring

parties. The decentralization of innovations, largely grounded in the deployment of numerous independent initiatives, has made it easier for Ukrainian developers to modify AI-enabled drones quickly.

Ukraine's approach empowers individual units and workshops to experiment, modify, and deploy solutions quickly. In contrast, Russia's more centralized and hierarchical model has hindered agility (DeVore, 2023). Civilian and private initiatives have played a central role in Ukraine's drone development, with commercial platforms repurposed for combat. One of Ukraine's most significant institutional innovations, according to Schmid and Mueller (2025), has been the creation of Brave1, a program linking front-line requirements with domestic and foreign technology developers. Brave1 has issued over 400 grants totalling more than UAH 800 million (approximately USD 19 million) and has supported projects such as the Swarmer drone and the Griselda intelligence system (Schmid & Muller, 2025).

One important threat appears to be underestimated by policy-makers: the *dual use of AI-enabled drones*. The recent developments in the civil sphere have produced a wide variety of technologies initially designed for non-military applications; technologies that appear innocent and harmless. The many modern applications them include drones autonomously optimizing trajectories and routes to improve delivery efficiency, enabling tasks like precision farming, monitoring, and autonomous field operations, conducting autonomous inspections, monitoring and real-time threat detection, drones undertaking missions in remote or inaccessible areas, acting as aerial nodes to extend connectivity in areas with poor internet access, dynamically adapt their routes in complex environments (Caballero-Martin et al., 2024). However, most of these peaceful applications could be adapted in order to affect the civil population and critical infrastructure. For instance, with small modifications, what is used to save forests from the threats of climate change or lives during disasters can be used to destroy sensitive objects.

These potential developments challenge existing regimes of designing, deploying, and using AI-enabled drones. As it was rightly noted, the lessons of Ukraine highlight the need for adaptive measures, including military and dual-use export controls, to keep pace with rapidly evolving drone capabilities (Kunertova, 2023). Experiences of drone wars in the Caucasus and Libya underscore how the political supply of military UAS exacerbates instability and the supply of technologies to non-state actors exacerbates the manifest threats, while the relaxation of commercial drone regulations post-COVID-19 may create further vulnerabilities (Rogers, 2021).

In this constantly changing environment, multi-sectoral innovation, civil–military collaboration, continuous AI solutions testing, and adaptability are essential for protecting people and infrastructure. The dual-use nature of AI-enabled drones underscores the urgency of developing robust legal, ethical, and regulatory frameworks that can keep pace with technological change. Without recognition of such shifts, it would be relatively easy to use the same capabilities that enable humanitarian aid, environmental monitoring, and disaster relief to target the civil population and critical infrastructure with unprecedented precision and unpredictability. Besides, sole reliance on physical protection is insufficient in modern conflict. AI-enabled threat anticipation, pattern recognition, and real-time analysis offer a more resilient approach by enabling forces to detect, track, and neutralize threats before they materialize. This proactive model demands integrating drone surveillance with predictive analytics to map enemy movement patterns, identify potential attack vectors, and allocate defences dynamically. As the Ukrainian example demonstrates, the integration of AI with drone reconnaissance reduces reaction times, optimizes resource allocation, and enhances both strategic and tactical decision-making.

3. Human-AI Interaction and Collaborative Decision-Making

3.1. Adaptability in the human-AI collaborative decisions

While fusion between human and machine is seen by many as problematic, especially in the context of public decision-making (e.g., Levy et al., 2021; Alon-Barkat & Busuioc, 2023; Decker et al., 2025), in the operational decision-making needed for the protection of the civil population and critical infrastructure, the *collaborative model* might prove very beneficial.

The line between human and automated agents is becoming increasingly indistinct as AI tools improve and are integrated into various stages of the decision-making process. The difficulty of determining the "decision point" – a common concern in AI-assisted decision-making (Crompton, 2021) – suggests that this line will be further eroded. However, in urgent contexts, it might be beneficial to facilitate a rapid transfer of control between human and AI agents. This flexibility can be vital in many security and defence scenarios, where operational control may need to shift quickly from humans to AI and back.

In particular, protecting critical infrastructure in peacetime requires rapid responses to emerging threats, including those posed by AI-enabled drones. In wartime, such protective measures may extend into hostile territory, which may, by contrast, require not defensive actions against drones but their active use. Human-AI interaction within decision-making processes enhances adaptability in responding to threats, giving rise to collaborative decision-making models.

A notable example from the Russo-Ukrainian war is Operation "Spiderweb", in which AI-enabled drones were employed by Ukraine to strike Russian airfields located thousands of kilometres away (Mazhulin et al., 2025). For the operation, the AI had been trained using old aircraft from an open-air museum in Ukraine to maximize targeting accuracy. Throughout the mission, control shifted repeatedly between human operators and the AI system. A hybrid control loop in Spiderweb where pilots flew the FPV drones over Russia's LTE network (Bondar, 2025a), and if/when the link degraded or jammed, onboard autonomy (including AI vision/target-assist) took over to keep the mission on track. When the link recovered, humans resumed manual control – sometimes handing back to AI for a terminal lock-on/dive. Drones also employed backup AI targeting, which in some instances successfully guided the drone to its target aircraft (Hambling, 2025a). Besides, in the case of a temporary loss of the control signal, some drones switched to using AI to complete their mission (Panella, 2025).

Another case of collaboration could be the use of AI control in the 'last mile'. According to a Brave1 spokesperson interviewed by Radio Free Europe/Radio Liberty, drones equipped with AI-assisted targeting modules operate without a continuous link to the operator during the engagement phase. Once the operator locks onto a target, the AI assumes control of targeting autonomously, making the process resistant to enemy electronic warfare measures (Chapple, 2024). These examples show that in wartime, human-machine close interaction emerges as a natural course of events, prompted by urgent necessity.

However efficient, AI-assisted decision-making raises several well-founded and fair concerns. Chief among these is accountability – a topic discussed in detail later – along with issues of bias, opacity, and public trust. Ng and Gray (2022) note that claims of AI delivering 'objective' judgments, particularly in judicial contexts, are questionable; such assertions are reminiscent of earlier debates about whether utilitarian or economic legal theories could produce mathematically precise and justifiable decisions (pp. 667–668). Similarly, Buchelt et al. (2024) observe that the most advanced machine learning models are often so complex, high-dimensional, and non-linear that they defy meaningful interpretation, making it nearly impossible to reconstruct how a given result was reached. Buchelt further suggests that explainable AI (XAI) could improve trust and safety by providing decision-making transparency, supporting liability assessments, and enabling more precise operations. In domains such as environmental monitoring and forest management, XAI could enhance impact analysis and operational efficiency. Applied to drones, an XAI-based approach would guarantee an understanding of why an AI system selected a particular route or action, informing both safety procedures and system improvements.

At the same time, turning to a human-AI collaborative decision-making model will require sustained public trust. The latter in human-AI collaboration for protecting the civil population and critical infrastructure is closely linked to perceptions of AI's role in decision-making more broadly. Haesevoets et al. (2024) find that people generally prefer AI to play an advisory role rather than share or hold primary decision-making authority. Nonetheless, the trend toward increasing AI integration in decision-making makes greater human-machine collaboration likely.

Schlicker et al. (2021) report that interpersonal justice perceptions are higher when humans, rather than AI, make decisions, and that explanations from human agents tend to improve informational justice perceptions – whereas explanations from automated systems have no such effect. Research on public acceptance of government-deployed algorithms emphasizes that these systems operate within specific socio-technical contexts. Citizens' acceptance depends heavily on how they perceive the importance of the problems the algorithm addresses and on their trust in the deploying organization (Wenzelburger et al., 2024). Interestingly, Horowitz et al. (2024) find that familiarity with AI has little impact on support for AI-enabled military applications – and that opposition to such uses has slightly increased over time. Yet, a greater presence of AI in decision-making related to military matters may be more acceptable to society in wartime than, for example, its presence in public decision-making.

Holzinger et al. (2023) highlight that the availability of large, high-quality datasets and the growth in computing power remain central drivers of AI development. Since AI already surpasses human cognitive capacity in certain processes, defending the population and infrastructure against emerging threats will increasingly require technological solutions.

In operational contexts – whether preventing threats in peacetime or responding to aggression during wartime – a collaborative human-AI decision-making model proves very effective. Even though 'slow-paced' decisions, such as those in litigation, may suffer from reduced human involvement, 'fast-paced' operational decisions can benefit significantly from such collaboration. The replacement of static defences with dynamic monitoring networks based on collaborative human-AI decision-making may significantly contribute to the protection of the civil population and critical infrastructure in the background of new threats.

3.2. Accountability in human-AI interactions

Human-AI collaboration plays a critical role at every stage of the decision-making process: from the initial situational assessment and preliminary analysis to the subsequent implementation of security and defence measures, their adjustment as needed, post-evaluation, and final explanation. It must be noted that throughout the process, it is essential to maintain an appropriate balance between system autonomy and human control.

One of the most contentious issues in AI-assisted decision-making concerns the deployment of autonomous weapons – particularly when lethal decisions occur outside of direct human oversight. Recent advances in AI have significantly facilitated the integration of autonomy into weapons systems, increasing the probability of such systems independently determining lethal targets. A 2021 United Nations Security Council report noted that a drone endowed with this capability may have been used during the Libyan civil war (UN Security Council, 2021).

Rogers (2021) argues that ethical controversies from the early era of drone warfare have intensified with the proliferation of remotely operated lethal robotics. The difficulty of attributing responsibility for drone-related atrocities – whether deliberate or accidental – creates a condition of "plausible deniability" with significant political, legal, and strategic consequences. In environments where similar or identical systems are employed by numerous and disparate actors, holding perpetrators accountable or responding effectively becomes increasingly complex. This second 'drone age' carries broader implications for global security, stability, and great-power relations.

Determining the precise scope of AI 'accountability' still represents a central difficulty (See, e.g., Busuioc, 2021; Cobbe et al., 2023; Cheong, 2024). Commonly recognised goals guiding policy-makers' understanding of accountability in AI governance include compliance, reporting, oversight, and enforcement. These ensure that agents act within ethical and legal bounds, document their actions and justify their conduct, allow for review and evidence collection, and determine consequences, such as sanctions, authorisations, or prohibitions, based on the findings (Novelli et al., 2024, p. 1882). Busuioc (2021, p. 827) conceptualises 'meaningful accountability' as a three-stage process: the provision of information, the offering of explanation or justification, and the possibility of consequences.

Within this framework, creating explainable AI becomes a central component of the justification phase in human-AI collaboration. As it was rightly pointed out, when an AI system produces decisions misaligned with its intended purpose or harmful to specific groups, understanding the reasoning behind those decisions is essential for corrective intervention (Holzinger et al., 2023). In unforeseen events or accidents, XAI's capacity to clarify a drone's behaviour is invaluable for assigning liability, ensuring regulatory compliance, and maintaining ethical standards. By uncovering the rationale behind actions, specialists can fine-tune AI systems to improve performance over time (Buchelt et al., 2024).

To date, the key safeguard for maintaining oversight and mitigating the most severe risks in collaborative decision-making is the 'human-in-the-loop' approach. This principle entails integrating human judgment and direction into AI development and operations to ensure effective and efficient human-machine cooperation toward shared objectives (Holzinger, 2023). However, there is an important caveat: humans are inherently biased, and their judgments tend to be influenced by AI outputs. Some studies have shown that when AI systems make errors, human overseers may blindly accept AI's suggestions, showing that human judgment declines in accuracy when participants receive incorrect algorithmic support, especially before giving their own perspective (Agudo et al., 2024), which leads to automation bias. This phenomenon can result in the amplification of AI mistakes rather than their correction. Since strategic security and defence projects often require large-scale solutions, the above problems are likely to be further augmented, adding to the known scalability issues connected with human-in-the-loop systems.

On the other hand, certain defence scenarios will necessitate substantial AI autonomy. Tucker (2024) notes that one of the main lessons from the war in Ukraine is the rapid pace of battlefield developments. Policies regarding lethal autonomy differ across nations and may shift quickly in response to frontline

conditions. As adversaries become more effective at disrupting the connections of humans and drones, the demand for greater autonomous capability is likely to grow.

In sum, while human-AI collaborative decision-making may require greater trust in algorithms than other AI-assisted processes, this trust must not come at the expense of accountability. Essential components of such accountability include keeping humans in the loop while preventing the loss of skill and expertise, and curbing automation bias; maintaining the capacity to swiftly transfer operational control between human and AI agents, and ensuring decision explainability.

4. A New Security and defence Doctrine

The integration of AI-enabled drones into modern warfare – across both offensive and defensive operations – necessitates a fundamental reassessment of security and defence doctrine. It should prioritize the principles of *proactivity, adaptability in decision-making*, *accountability*, *public trust*, *human oversight and control,* and *involvement of private and/or civil initiatives*. This renewed and properly balanced doctrine must also acknowledge that traditional concepts of security and defence are no longer sufficient.

Fig. 2. *Core Principles of the New Security and defence Doctrine*

The threats created by the use of AI-enabled drones are proving this insufficiency. Even though AI-enabled drones still face developmental limitations, such as visual occlusions, background interference, restricted sensor resolution, and operational challenges, including limited battery capacity, susceptibility to weather conditions, alongside gaps in standardization and publicly available datasets, their combined potential remains considerable (Aliane, 2025). There is no reason to assume that the mentioned limitations won't be overcome in the foreseeable future, aggravating the threats.

Public trust – a principle that might not seem obvious when it comes to security and defence strategies – is gaining in importance as AI technologies become increasingly complex. Not only will people's credence depend on transparent governance and citizen feedback mechanisms, but also on raising awareness of AI's capabilities, particularly those of AI-enabled drones. Educating citizens on how to utilize AI for state defence,

both military and civil, could build trust and encourage broader participation in its defence. According to Bondar (2025b), training civilians to operate AI-assisted drones, especially in emergencies, may further enhance public engagement. Drone training programs increasingly integrate autonomous navigation and targeting features, enabling operators to master AI-supported modes within a short time frame, often less than a day, thereby expanding the pool of qualified personnel and improving operational readiness (Bondar, 2025b).

Major challenges in security and defence, especially in the case of the protection of critical infrastructure, include governance and security management, secure network architecture design, self-healing systems, modeling and simulation capabilities, large-scale situational awareness, forensic analysis, trust management, and privacy protection (Alcaraz & Zeadally, 2015). To ensure confidence in ICT systems managing sensitive infrastructure data, these systems must meet requirements such as high availability, resilience, fault tolerance, scalability, autonomy, and interoperability, as well as the ability to collaborate across heterogeneous environments during abnormal or threatening events (Alcaraz & Zeadally, 2015). Adaptability in decision-making, crucial in cases of emergency, should be added to this list.

Effective security and defence strategies also depend on robust public-private partnerships. According to Yusta et al. (2011), such partnerships are especially important in the protection of interconnected infrastructure. These should facilitate the exchange of incident reports, threat intelligence, and vulnerability assessments among stakeholders, including infrastructure owners, industry representatives, government agencies, intelligence services, advisory bodies, and local or regional authorities (Yusta et al., 2011). As Roshanaei (2021) notes, future improvements in critical infrastructure protection frameworks should incorporate standardized performance assessment systems using shared metrics, enabling consistent evaluation of action plans and security measures. The proper assessment might require the involvement of independent civil initiatives.

Historically, many security and defence strategies have relied on risk management principles. For example, in the United States (U.S.), the National Infrastructure Protection Plan stands out as a leading example, guiding other nations in establishing committees, task forces, and working groups tasked with scenario planning, risk evaluation, and early warning systems – often in collaboration between civil and military authorities (Yusta et al., 2011). In the modern context, a risk-based approach requires vigorous proactive prevention, which, in turn, may require human-AI collaboration.

Military innovation experiences also offer lessons for improved protection of the civil population and critical infrastructure. As it was demonstrated by Dawson and Nadal in the case of the Royal Air Force (RAF) in the United Kingdom (UK), this structure's growing willingness to take risks – spurred in part by the war in Ukraine – could help streamline change and foster broader organisational adaptability. Yet, as the earlier case of experimenting with weaponised small uncrewed aerial systems reveals, a strong culture of risk aversion still remains (Dawson & Nadal, 2024, p. 346). Context is highly important, however, as it was rightly pointed out by Schmid and Mueller (2025): Ukraine's processes, organisational structures, and regulations cannot simply be transplanted into the U.S. or other nations. Still, Ukraine's experience offers two valuable lessons: (1) adopt commercial technologies more aggressively; (2) use innovation bodies like Brave1, which connects front-line needs to tech developers, to accelerate weapons acquisition in conflict. This strategy of leveraging commercial technology can be particularly advantageous when fighting is ongoing, capability gaps emerge suddenly, and the urgency of the situation rules out conventional procurement channels (Schmid & Mueller, 2025).

Change often faces resistance, driven in part by organisational inertia. However, the fundamental changes listed above must be recognized and, in turn, implemented into national security and defence doctrines, policy, and legislative frameworks to ensure resilience in an evolving threat environment.

5. Conclusions

The future of security and defence increasingly depends on the development of artificial intelligence. The reality of widespread use of AI in drones requires a new framework, a new security and defence doctrine that must be adapted to explore this uncharted territory. The Russo-Ukrainian War offers a preview of future conflicts, in which AI-enabled drones will play a central role in both offensive and defensive operations. The lessons extend beyond Ukraine: in an era where technological diffusion is rapid and barriers to entry are low, protection of the civil population and critical infrastructure will face growing vulnerability.

The global proliferation of drones, much like the spread of aircraft a century ago, is reshaping the very foundations of strategic power, which means that the states that adapt earliest will set the standards for the conflicts of tomorrow. To navigate this landscape, security and defence doctrine must go beyond physical protection, embracing AI-driven anticipation, resilient human–AI collaboration, and dual-use innovation. At

the same time, governance frameworks and international norms are urgently needed to address ethical risks and accountability in autonomous operations. States that adapt early, by combining technological foresight with robust policy and civil–military cooperation, will not only set the standards for future conflict but also safeguard critical infrastructure and civilian populations more effectively in an era of accelerating change.

Author Contributions

Yulia Razmetaeva is essentially responsible for all aspects of the research, including conception and writing.

Acknowledgements and Funding

The research in this paper is funded by the Wallenberg Foundations by the Wallenberg AI, Autonomous Systems and Software Program – Humanities and Society (WASP-HS) program within the project "The Artificial Public Servant" (2022–2026).

Data Availability: Not applicable.
Declarations: No conflict of interest.

REFERENCES

1. Agudo, U., Liberal, K. G., Arrese, M., Matute, H. (2024). The impact of AI errors in a human-in-the-loop process. *Cognitive Research: Principles and Implications*, 9, 1. https://doi.org/10.1186/s41235-023-00529-3.
2. Alcaraz, C., & Zeadally, S. (2025). Critical infrastructure protection: Requirements and challenges for the 21st century. *International journal of critical infrastructure protection*, 8, 53–66. https://doi.org/10.1016/j.ijcip.2014.12.002.
3. Aliane, N. (2025). Drones and AI-Driven Solutions for Wildlife Monitoring. *Drones*, 9, 455. https://doi.org/10.3390/drones9070455.
4. Alon-Barkat, S., & Busuioc, M. (2023). Human–AI interactions in public sector decision making: "automation bias" and "selective adherence" to algorithmic advice. *Journal of Public Administration Research and Theory*, 33(1), 153–169. https://doi.org/10.1093/jopart/muac007.
5. Araujo, T., Helberger, N., Kruikemeier, S., & De Vreese, C. H. (2020). In AI we trust? Perceptions about automated decision-making by artificial intelligence. AI & society, 35(3), 611–623. https://doi.org/10.1007/s00146-019-00931-w.
6. Atlas, R. M., & Dando, M. (2006). The dual-use dilemma for the life sciences: perspectives, conundrums, and global solutions. *Biosecurity and bioterrorism: biodefence strategy, practice, and science*, 4(3), 276–286.
7. Axe, D. (2024a). Ukraine's Gun-Armed Ground Robot Just Cleared A Russian Trench In Kursk. Forbes. September 19, 2024. https://www.forbes.com/sites/davidaxe/2024/09/19/ukraines-gun-armed-ground-robot-just-cleared-a-russian-trench-in-kursk/.
8. Axe, D. (2024b). A Two-Pound Ukrainian Drone May Have Shot Down A 12-Ton Russian Helicopter. Forbes. July 31, 2024. https://www.forbes.com/sites/davidaxe/2024/07/31/a-two-pound-ukrainian-drone-just-shot-down-a-12-ton-russian-helicopter/.
9. Bathaee, Y. (2018). The Artificial Intelligence Black Box and the Failure of Intent and Causation. *Harvard Journal of Law & Technology*, 31(2), 889–938.
10. Bendett, S. & Kirichenko, D. (2025). Battlefield Drones and the Accelerating Autonomous Arms Race in Ukraine. January 10, 2025. https://mwi.westpoint.edu/battlefield-drones-and-the-accelerating-autonomous-arms-race-in-ukraine/#:~:text=Both%20Ukraine%20and%20Russia%20are,reducing%20risks%20to%20human%%2020live.
11. Bondar, K. (2024). Closing the Loop: Enhancing U.S. Drone Capabilities through Real-World Testing. Center for Strategic and International Studies. August 21, 2024. https://www.csis.org/analysis/closing-loop-enhancing-us-drone-capabilities-through-real-world-testing.
12. Bondar, K. (2025a). How Ukraine's Operation "Spider's Web" Redefines Asymmetric Warfare. June 2, 2025. https://www.csis.org/analysis/how-ukraines-spider-web-operation-redefines-asymmetric-warfare.
13. Bondar, K. (2025b). Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare. Report of CSIS. Wadhwani AI Center. March 6, 2025. https://www.csis.org/analysis/ukraines-future-vision-and-current-capabilities-waging-ai-enabled-autonomous-warfare.
14. Buchelt, A., et al. (2024). Exploring artificial intelligence for applications of drones in forest ecology and management. *Forest Ecology and Management*, 551, 121530. https://doi.org/10.1016/j.foreco.2023.121530.
15. Busuioc, M. (2021). Accountable artificial intelligence: Holding algorithms to account. *Public administration review*, 81(5), 825–836. https://doi.org/10.1111/puar.13293.

16. Caballero-Martin, D., Lopez-Guede, J. M., Estevez, J., & Graña, M. (2024). Artificial Intelligence Applied to Drone Control: A State of the Art. *Drones*, 8, 296. https://doi.org/10.3390/drones8070296.
17. Calcara, A., Gilli, A., Gilli, M., Marchetti, R., Zaccagnini, I. (2022). Why drones have not revolutionized war: The enduring hider-finder competition in air warfare. *International Security*, 46(4), 130–171.
18. Chapple, A. (2024). Swarm Wars: The Shaky Rise Of AI Drones In Ukraine. Radio Free Europe/Radio Liberty. August 14, 2024. https://www.rferl.org/a/drone-ai-technology-russia-ukraine-war/33078798.html.
19. Choung, H., David, P., & Ross, A. (2023). Trust in AI and its role in the acceptance of AI technologies. International Journal of Human–Computer Interaction, 39(9), 1727–1739. https://doi.org/10.1080/10447318.2022.2050543.
20. Cheong, B. C. (2024). Transparency and accountability in AI systems: safeguarding wellbeing in the age of algorithmic decision-making. *Frontiers in Human Dynamics*, 6, 1421273. https://doi.org/10.3389/fhumd.2024.1421273.
21. Cobbe, J., Veale, M., & Singh, J. (2023). Understanding accountability in algorithmic supply chains. In Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency (FAccT '23). Association for Computing Machinery, New York, NY, USA, 1186–1197. https://doi.org/10.1145/3593013.3594073.
22. Crompton, L. (2021). The decision-point-dilemma: Yet another problem of responsibility in human-AI interaction. *Journal of Responsible Technology*, 7–8, 100013. https://doi.org/10.1016/j.jrt.2021.100013.
23. Dawson, A., Nadal, A. (2024). Concept to Combat: The Royal Air Force, Small Drones and the War in Ukraine. *European Review of International Studies*, 11 (3), Special issue: European Military Innovation in the wake of Russia's invasion of Ukraine, 321–357.
24. De Ágreda, Á. G. (2020). Ethics of autonomous weapons systems and its applicability to any AI systems. *Telecommunications Policy*, 44(6), 101953. https://doi.org/10.1016/j.telpol.2020.101953.
25. Decker, M., Wegner, L., & Leicht-Scholten, C. (2025). Procedural fairness in algorithmic decision-making: the role of public engagement. *Ethics and Information Technology*, 27, 1. https://doi.org/10.1007/s10676-024-09811-4.
26. DeVore, M. R. (2023). "No end of a lesson:" observations from the first high-intensity drone war. *defence & Security Analysis*, 39(2), 263–266. https://doi.org/10.1080/14751798.2023.2178571.
27. Fratsyvir, A. (2025). Ukraine's AI-powered 'mother drone' sees first combat use, minister says. The Kyiv Independent. May 29, 2025. https://kyivindependent.com/ukraines-ai-powered-mother-drone-sees-first-combat-use-minister-says/.
28. Gillath, O., Ai, T., Branicky, M. S., Keshmiri, S., Davison, R. B., & Spaulding, R. (2021). Attachment and Trust in Artificial Intelligence. *Computers in Human Behavior*, 115, 106607. https://doi.org/10.1016/j.chb.2020.106607.
29. Glikson, E., & Woolley, A. W. (2020). Human trust in artificial intelligence: Review of empirical research. Academy of management annals, 14(2), 627–660.
30. Grinbaum, A., & Adomaitis, L. (2024). Dual use concerns of generative AI and large language models. *Journal of Responsible Innovation*, 11(1). https://doi.org/10.1080/23299460.2024.2304381.
31. Haesevoets, T., Verschuere, B., Van Severen, R., & Roets, A. (2024). How do citizens perceive the use of Artificial Intelligence in public sector decisions? *Government Information Quarterly*, 41(1), 101906, https://doi.org/10.1016/j.giq.2023.101906.
32. Hambling, D. (2022). Ukraine Wins First Drone Vs. Drone Dogfight Against Russia, Opening A New Era Of Warfare (Updated). October 14. Forbes. https://www.forbes.com/sites/davidhambling/2022/10/14/ukraine-wins-first-drone-vs-drone-dogfight-against-russia-opening-a-new-era-of-warfare/.
33. Hambling, D. (2025a). Moving Targets: Implications of the Russo-Ukrainian War for Drone Terrorism. Combating Terrorism Center at West Point. July 2025. https://ctc.westpoint.edu/moving-targets-implications-of-the-russo-ukrainian-war-for-drone-terrorism/.
34. Hambling, D. (2025b). Ukraine Drone Carriers Launch First Long-Range Autonomous Strikes. Forbes. May 26, 2025. https://www.forbes.com/sites/davidhambling/2025/05/26/ukraine-drone-carriers-launch-first-long-range-autonomous-strikes/.
35. Helberger, N., Araujo, T., & de Vreese, C. H. (2020). Who Is the Fairest of Them All? Public Attitudes and Expectations Regarding Automated Decision-making. *Computer Law & Security Review*, 39, 105456. https://doi.org/10.1016/j.clsr.2020.105456.
36. Holzinger, A., Keiblinger, K., Holub, P., Zatloukal, K., Müller, H. (2023). AI for life: Trends in artificial intelligence for biotechnology. *New biotechnology*, 74, 16-24. https://doi.org/10.1016/j.nbt.2023.02.001.
37. Horowitz, M. C., Kahn, L., Macdonald, J., & Schneider, J. (2024). Adopting AI: How Familiarity Breeds Both Trust and Contempt. *AI and Society*, 39, 1721–1735.
38. Hambling, D. (2025). Ukraine Drone Carriers Launch First Long-Range Autonomous Strikes. Forbes. May 26, 2025. https://www.forbes.com/sites/davidhambling/2025/05/26/ukraine-drone-carriers-launch-first-long-range-autonomous-strikes/.
39. Institute for Economics & Peace. Global Peace Index 2025: Identifying and Measuring the Factors that Drive Peace, Sydney, June 2025. Available from: http://visionofhumanity.org/resources (accessed 30 July 2025).

40. Khomenko, I. (2024). How Ukraine Is Using AI Drones to Outsmart Russia on the Battlefield. United 24 Media. November 19, 2024. https://united24media.com/latest-news/how-ukraine-is-using-ai-drones-to-outsmart-russia-on-the-battlefield-3833.
41. King, A. (2024). Robot wars: Autonomous drone swarms and the battlefield of the future. *Journal of Strategic Studies*, 47(2), 185–213. https://doi.org/10.1080/01402390.2024.2302585.
42. Kirichenko, D. (2025). Why Ukraine's AI drones aren't a breakthrough yet. The Strategist. Australian Strategic Policy Institute. 19 June 2025. https://www.aspistrategist.org.au/why-ukraines-ai-drones-arent-a-breakthrough-yet/.
43. Kunertova, D. (2023). The war in Ukraine shows the game-changing effect of drones depends on the game. *Bulletin of the Atomic Scientists*, 79(2), 95–102. https://doi.org/10.1080/00963402.2023.2178180.
44. Kushnikov, V. (2025). Azov Brigade Drones Deliver Blood to Critically Wounded Soldier at Front Line. Militarnyi. February 21, 2025. https://militarnyi.com/en/news/azov-brigade-drones-deliver-blood-to-critically-wounded-soldier-at-front-line/.
45. Levy, K., Chasalow, K. E., Riley, S. (2021). Algorithms and decision-making in the public sector. *Annual Review of Law and Social Science*, 17(1), 309–334.
46. Mazhulin, A., Holmes, O., Swan, L., Boulinier, L., & Hecimovic, A. (2025). Operation Spiderweb: a visual guide to Ukraine's destruction of Russian aircraft. The Guardian. 2 June 2025. https://www.theguardian.com/world/2025/jun/02/operation-spiderweb-visual-guide-ukraine-drone-attack-russian-aircraft?ref=hackernoon.com.
47. Miller, S.; Selgelid, M. (2007). Ethical and Philosophical Consideration of the Dual-Use Dilemma in the Biological Sciences. *Science and Engineering Ethics*, 13(4), 523–580. https://doi.org/10.1007/s11948-007-9043-4.
48. Newdick, T. (2024). Ukraine Claims Its Drone Boat Shot Down A Russian Mi-8 Helicopter With A Surface-To-Air Missile. December 31, 2024. https://www.twz.com/sea/ukraine-claims-its-drone-boat-shot-down-a-russian-mi-8-helicopter-with-a-surface-to-air-missile.
49. Ng, Y.-F., Gray, S. (2022). Disadvantage and the Automated Decision. *Adelaide Law Review*, 43(2), 641–677.
50. Novelli, C., Taddeo, M., Floridi, L. (2024). Accountability in artificial intelligence: What it is and how it works. *AI & Society*, 39(4), 1871–1882.
51. Panella, C. (2025). The AI drone revolution isn't here yet, but Ukraine and Russia are laying the groundwork in battle. Business Insider. June 9, 2025. https://www.businessinsider.com/ai-drone-boom-isnt-here-ukraine-russia-setting-stage-researchers-2025-6.
52. Plichta, M., & Rossiter, A. (2024). A one-way attack drone revolution? Affordable mass precision in modern conflict. *Journal of Strategic Studies*, 47(6–7), 1001–1031. https://doi.org/10.1080/01402390.2024.2385843.
53. Rogers J. (2021). Future threats: Military UAS, terrorist drones, and the dangers of the second drone age. InDrone Warfare: Trends and emerging issues (pp. 481–505). The Joint Air Power Competence Centre.
54. Roshanaei, M. (2021). Resilience at the core: critical infrastructure protection challenges, priorities and cybersecurity assessment strategies. *Journal of Computer and Communications*, 9(8), 80–102.
55. Schaap, G., Bosse, T., & Hendriks Vettehen, P. (2024). The ABC of algorithmic aversion: Not agent, but benefits and control determine the acceptance of automated decision-making. AI & society, 39(4), 1947–1960. https://doi.org/10.1007/s00146-023-01649-6.
56. Schlicker, N., Langer, M., Ötting, S. K., Baum, K., König, C. J., & Wallach, D. (2021). What to expect from opening up 'black boxes'? Comparing perceptions of justice between human and automated agents. *Computers in Human Behavior*, 122, 106837, https://doi.org/10.1016/j.chb.2021.106837.
57. Schmid, J., Mueller, E. (2025). What the Pentagon Might Learn from Ukraine About Fielding New Tech. Rand. Commentary. February 14, 2025. https://www.rand.org/pubs/commentary/2025/02/what-the-pentagon-might-learn-from-ukraine-about-fielding.html.
58. Shneiderman, B. (2020). Human-Centered Artificial Intelligence: Reliable, Safe & Trustworthy. *International Journal of Human–Computer Interaction*, 36(6), 495–504.
59. Slusher, M. (2025). Lessons from the Ukraine Conflict: Modern Warfare in the Age of Autonomy, Information, and Resilience. Center for Strategic and International Studies. Report. May 2, 2025. https://www.csis.org/analysis/lessons-ukraine-conflict-modern-warfare-age-autonomy-information-and-resilience.
60. Stepanenko, K. (2025). The Battlefield AI Revolution Is Not Here Yet: The Status of Current Russian and Ukrainian AI Drone Efforts. Special report. Institute for the Study of War. June 2, 2025. https://understandingwar.org/backgrounder/battlefield-ai-revolution-not-here-yet-status-current-russian-and-ukrainian-ai-drone.
61. Tucker, P. (2024). New AI-powered strike drone shows how quickly battlefield autonomy is evolving. defenceOne. October 10, 2024. https://www.defenceone.com/technology/2024/10/new-ai-powered-strike-drone-shows-how-quickly-battlefield-autonomy-evolving/400179/.
62. Tweneboah-Koduah, S., Buchanan, W. J. (2018). Security risk assessment of critical infrastructure systems: A comparative study. *The Computer Journal*, 61(9), 1389–1406. https://doi.org/10.1093/comjnl/bxy002.
63. UN Security Council. (2011). Final report of the Panel of Experts on Libya established pursuant to Security Council resolution 1973 (2011). 8 March 2021. S/2021/229. https://docs.un.org/en/S/2021/229.

64. Watling, J., Reynolds, N. (2025). Tactical Developments During the Third Year of the Russo–Ukrainian War. The Royal United Services Institute for Defence and Security Studies. Report. February 2025. https://static.rusi.org/tactical-developments-third-year-russo-ukrainian-war-february-2205.pdf.
65. Wenzelburger, G., König, P. D., Felfeli, J., Achtziger, A. (2024). Algorithms in the public sector. Why context matters. *Public Administration*, 102(1), 40–60.
66. Yusta, J. M., Correa, G. J., Lacal-Arántegui, R. (2011). Methodologies and applications for critical infrastructure protection: State-of-the-art. *Energy policy*, 39(10), 6100–6119. https://doi.org/10.1016/j.enpol.2011.07.010.
67. Zaluzhnyi, V. (2025). How drones, data, and AI transformed our military—and why the US must follow suit. Defence One. April 10, 2025. https://www.defenceone.com/ideas/2025/04/how-drones-data-and-ai-transformed-our-militaryand-why-us-must-follow-suit/404444/.
68. Zoria, Y. (2025). First battlefield capitulation to robots: Ukrainian drones force Russian surrender and seize fortified position (video). Euromaidan Press. February 9, 2025. https://euromaidanpress.com/2025/07/09/first-battlefield-capitulation-to-robots-ukrainian-drone-unit-takes-positions-and-prisoners-with-zero-troops-video/#google_vignette.