IRMO BRIEF

12
2025

21st Century Warfare: How Drones, Cyber Operations and AI Are Changing Combat

By Viktor Trumbetaš

Introduction

In the past three years, global warfare has undergone an accelerated transformation not yet seen since the end of the Cold War and Operation Desert Storm. The conflicts in Ukraine, the Middle East, and a series of smaller regional crises have produced several new ways in which warfare has changed. Technological advances, shifts in doctrine, and adaptation to new forms of threats have become crucial factors on the modern battlefield. While conventional military weaponry such as tanks, artillery, and air forces remain significant, their role is increasingly intertwined with unmanned, cyber, and autonomous systems. The first key trend is the explosion in the use of unmanned systems and asymmetric tactics. From cheap commercial drones converted into improvised weapons to sophisticated kamikaze platforms and swarms of

autonomous aircraft, unmanned technology has changed the pace and manner of conducting operations. The second important element is the expansion of cyber and electronic warfare as an integral part of almost every contemporary conflict. Attacks on infrastructure, disruption of communications, hacking of military networks, and manipulation of information are now just as important as physical strikes on the ground. The third feature is the introduction of artificial intelligence and autonomous systems into strategic, tactical, and logistical processes. AI algorithms analyse the vast amounts of data in real time, predict the movement of enemy forces, optimize supply lines, and even take control of armed platforms. These three changes; the proliferation of unmanned systems, the integration of the cyber and electronic battlefield, and the growing role of artificial intelligence show that the world has entered a new era not only of technical innovations but also of cardinal shifts in military strategies, international security policy, and legal norms. Therefore, the dynamics of these emerging phenomena and changes require timely adaptation of defence policies and international security arrangements.

Drones

One of the most striking changes in modern warfare over the past five years has been the dominance and proliferation of unmanned systems (better known as "drones"). Although they have been present on battlefields for more than 40 years, never before have drones - primarily aerial, but also maritime - played such a prominent role as they do today. The first war in which drones came to wider use and larger-scale deployment was the Second Karabakh War in 2020. In just a month and a half, the Azerbaijani military decisively defeated the Armenian para-state, the so-called "Republic of Artsakh."

First war in which drones came to wider use was the Second Karabakh War in 2020.

In this conflict, the Azerbaijani forces made extensive use of second-generation combat drones, most notably the already well-known Turkish Bayraktar TB-2, as well as loitering munitions (Orbiter 1K and Harop). These systems devastated Armenian positions without risking the loss of expensive conventional aircraft or pilots' lives. The world watched with immense interest as drone footage captured the destruction of Armenian trenches, trucks, tanks, infantry units, and other equipment—something reminiscent of the U.S. "Desert Storm" in 1990, only this time through the lenses of robots operated remotely by specialists hundreds of kilometres away. However, the biggest leap, better say a quantum leap, in the exploitation of drones occurred during the Russo-Ukrainian War that began in 2022. Learning from the Azerbaijani experience, the Ukrainians initially used their Bayraktar TB-2 drones to inflict losses on the Russian army and slow its operations. Most notable of their actions include the flights during the Battle of Kyiv, the slowing of the infamous 64-km Russian convoy, and the liberation of Snake Island. To boost morale, the Ukrainians even created a song dedicated to this drone.

Biggest leap in exploitation of drones occurred during Russo-Ukrainian War that began in 2022.

Over time, however, it became clear that larger military drones like the Bayraktar struggle to survive in modern conventional warfare. They were soon withdrawn from the front lines, primarily because the Russian military became increasingly effective at neutralizing them using various air-defence systems (both gun and missile) and electronic-warfare units. The next step was the mass use of ordinary commercial hobby (COTS) drones, which were at first used for reconnaissance and later modified for dropping grenades. The Russians, for their part, began using Iranian Shahed drones as a substitute for depleted stocks of cruise missiles and as an alternative to risky aircraft bombing missions. This use of drones born out of sheer necessity on both sides has completely transformed the modern battlefield. Asymmetric warfare has been most evident in this conflict precisely through these actions. On the Ukrainian side, it has been shown that relatively inexpensive drones can shift the balance of power and carry out destructive attacks on key targets. Thousands of pieces of Russian military equipment were destroyed by COTS drones that were hundreds of times cheaper (average cost per unit is between $500 and $1,000), blunting the striking power of the Armed Forces of the Russian Federation and giving Ukrainians crucial time to defend themselves. A single drone can destroy a tank only if it hits an open hatch, but in most cases it takes around ten drones or more drones to destroy one tank—showing that tanks can still survive on the battlefield. However, if we look at the cost-to-effect ratio, the calculation is favourable on the side of the drones. The cost-effectiveness of their attacks on the open battlefield is much higher.

Thousands of pieces of Russian military equipment were destroyed by COTS drones.

The Russian armed forces have also integrated themselves into this form of warfare quite successfully, although somewhat later, as demonstrated by the halting of the Ukrainian counteroffensive in 2023, the battles for Sudzha and the Kursk region in 2024/25, and the battles for Pokrovsk in 2025. Alongside artillery, the "god of war", drones have become a new instrumental weapon. They are being used more than ever for assault operations, reconnaissance and surveillance, assassinations, and even logistics. As of 2025, military experts estimate that around 80% of military casualties on both sides on Ukrainian battlefield, both personnel and equipment, are caused by drones (predominantly FPV, first-person view, video piloting drones). With the evolution of affordable FPV *kamikaze* drones, unmanned systems have risen to such importance that many countries around the world, following the examples of Ukraine and Russia, are establishing their own drone units (for example Croatia in the EU), or even entire new branches of the armed forces composed of unmanned systems. This trend has also influenced other branches of the military. In the Ukrainian war, for instance, both sides actively use naval drones (which have wreaked

havoc on the Russian Black Sea Fleet) as well as ground combat robotic systems. The trend of robotizing warfare continues, and automated combat systems and weapons are in high demand. Artificial intelligence is an additional factor accelerating the development of such weaponry.

Cyber Warfare

With the development of digital technologies and the digitization of both military and civilian systems, especially over the past 20 years, cyber warfare has become another key and unavoidable domain of modern warfare. Cyber operations are now used alongside traditional military actions, and their scope is multifaceted. They are considered to be an integral part of so-called "hybrid warfare," because in modern conflicts cyberattacks have become an essential element combined with other "classical" methods of aggression such as direct attacks, sieges, and sabotage. From a Western perspective (and vice versa), potential adversaries use cyber activities and campaigns to weaken critical infrastructure, disrupt government services, gather intelligence, steal intellectual property, and hinder military operations. Confrontational rhetoric and disinformation can also be added to this list as another form of "hybrid warfare." All of these activities share a common goal: to jeopardize system security, destabilize states or organizations, and obtain sensitive information that may hold strategic value. Such attacks often involve data theft, the installation of malicious software, the use of phishing techniques, and the hacking of user accounts to gain control over important information.

Cyberspace has become crucial because digitalization has made the world dependent on digital infrastructure.

Cyberspace has become crucial because digitalization has made the world, including armed forces, largely dependent on digital infrastructure. For this very reason, cyberspace has become indispensable, as digitalization has made both civilian and military systems tightly bound to and inseparable from digital infrastructure. The war in Ukraine has shown to what extent cyber activities have become a defining feature of modern conflicts. With a single click, attacks such as sabotage or the disruption of key systems can be carried out paralysing opponent's defence. The most active actors in cyber confrontations are Western states and NATO on one side, and Russia and China on the other, although many other actors are also involved in cyber warfare, such as North Korea, Iran, Turkey, and even smaller informal hacker groups. In 2024, for example, cyberattacks on Ukraine increased by nearly 70%, with more than 4,300 attacks on critical infrastructure, including government services, the energy sector, and defence entities. Data from Ukraine's cybersecurity agency indicates that these attacks often targeted the theft of sensitive information and the disruption of operations through techniques such as malware distribution, phishing, and account compromise. A similar situation occurred in Taiwan, where cyberattacks by Chinese groups rose to 2.4 million attempts per day in 2024, targeting government systems and telecommunications companies. Cyberattacks also targeted government entities

in Pakistan, India, and other parts of the world, demonstrating the global nature of this issue.

In 2024 cyberattacks on Ukraine increased by nearly 70%.

In December 2024, Russian hackers successfully compromised the systems of a Pakistani hacking group, repurposing the group's digital infrastructure to reach confidential data that had been stolen from various South Asian governmental and military entities. Cyberattacks on Indian government entities has also increased by 138% between 2019 and 2023, rising from 85,797 incidents in 2019 to 204,844 in 2023, according to India's Ministry of Electronics and IT. In November 2024, the United Kingdom's National Cyber Security Centre reported a threefold increase in significant cyberattacks compared to the previous year, providing support in response to 430 incidents, 89 of which were classified as "nationally significant." Chinese, Russian, Iranian, and North Korean threats were described as "real and enduring threats."

In Taiwan, cyberattacks by Chinese groups rose to 2.4 million attempts per day in 2024.

In June 2025, Ukraine's military intelligence claimed to have breached the Russian aerospace company Tupolev, stealing confidential data concerning strategic bomber programs. In October 2025, North Korea's Lazarus APT group targeted three European defence companies in an attempt to steal sensitive information about drone components and manufacturing processes. Using social engineering, attackers sent fake job offers embedded with remote-access trojans. The targeted companies supply military equipment to Ukraine and possess specialized knowledge of advanced single-rotor drones that North Korea is actively developing. It was also discovered that an Iranian intelligence group maintained persistent access to Kurdish and Iraqi government networks for eight years, using custom implants and backdoors to spy on officials and maintain strategic positions in both regions. In May 2025 it was uncovered that Russian hackers conducted an espionage campaign against educational, governmental, and research entities in Tajikistan using an HTML application to implant malware, while a Turkish espionage group exploited a vulnerability in a messaging app to spy on Kurdish military forces in Iraq, using a zero-day flaw to access Kurdish military communications.

Cyberattacks on Indian government entities has increased by 138% between 2019 and 2023.

Given the growing number and increasing sophistication of cyberattacks, it is becoming clear that in modern conflicts, cyber operations are not merely an additional threat but a key dimension of warfare that requires the

development of new protection strategies and response mechanisms. In this context, the use of artificial intelligence (AI) in cyberattacks is becoming increasingly prominent. Cybercriminals now use AI to enhance existing offensive techniques. The application of large language models enables the mass distribution of false narratives through social networks, articles, photos, and manipulated videos, making the spread of disinformation easier than ever. Deep-fake technology and other forms of AI-generated images or audio have become almost indistinguishable from reality, making information manipulation more dangerous and harder to detect. These attacks introduce additional challenges to global security and require rapid adaptation in defensive methods in order to minimize negative effects on societies, political systems, and international relations.

Artificial Intelligence

If 2020's brought drones and cyber warfare to more prominence, then for the artificial intelligence this decade is a major breakthrough. According to the European Commission, "Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. US Government and NASA are defining AI as the computer systems that can perform complex tasks normally done by human-reasoning, decision making, creating, etc. In an essence, it is an artificial system designed to think or act like a human, including cognitive architectures and neural networks. Consequently, as much as AI has been exploited within the civilian domain that much it was found to be applicable within the military domain. Applications of AI within the military are multiple: unmanned systems are rapidly evolving, with aerial and ground-based drones advancing from traditional reconnaissance roles to sophisticated strike platforms that feature increasing levels of autonomy.

Breakthroughs in autonomous navigation are enhancing operational flexibility and effectiveness.

At the same time, breakthroughs in autonomous navigation, particularly in GPS-denied environments and drone swarm coordination are greatly enhancing operational flexibility and effectiveness. Artificial intelligence is also transforming situational awareness, command, and control by delivering real-time intelligence and decision-support tools that strengthen battlefield strategy and leadership. In post-strike operations, AI assists with damage analysis and assessment, enabling more accurate recovery planning and cost estimation. Furthermore, AI-powered demining technologies are improving the speed and safety of landmine clearance, significantly reducing risks to both soldiers and civilians. Finally, AI-driven training and simulation systems are creating highly realistic, adaptive combat scenarios tailored to individual learning needs, resulting in more effective and responsive military training programs. The current use of artificial intelligence in military applications remains limited in scope, primarily

enhancing specific functions and resolving selected operational challenges rather than enabling complete system autonomy. AI serves as a critical enabling technology in the evolution from automated systems those that follow predefined, human-programmed instructions to truly autonomous systems capable of independently determining how best to achieve assigned objectives. Autonomy is defined by the U.S. military as a system's ability to accomplish goals independently or with minimal supervision in complex and unpredictable environments. As such, it is not yet present on the contemporary battlefields. The primary reason for this is that the necessary technology, AI in particular, has not reached the required level of development, required to support fully autonomous military operations.

Russian Ministry of Defense uses AI primarily to support data collection and analysis.

The strategies towards using AI on contemporary battlefields can be the best observed by looking on the Russian and Ukrainian army's strategies towards AI and usage on the battlefield. According to analyses and public statements, the Russian Ministry of Defense uses AI primarily to support data collection and analysis as part of the transition from current digital warfare systems, with AI serving as a decision-making support tool for operators, commanders, and deployed forces. This also implies the use of AI in information and cyber operations as well as the hybrid warfare. Russian government and military's approach towards AI development and implementation is more centralized and the Russian government is promoting stronger integration between its military and civilian sectors to accelerate advancements in artificial intelligence. Alongside with the information and cyber warfare domains, Russian armed forces are equipping loitering munitions, aerial drones, and select ground-based robotic platforms with enhanced, AI-driven functionalities. At the same time, Moscow is expected to increasingly rely and depend on China for both technological innovation and policy collaboration in the field of AI, as mounting U.S. and international sanctions continue to restrict Russia's access to foreign technology partnerships, procurement channels, and other resources essential to its domestic AI research and development efforts.

Moscow is expected to increasingly rely and depend on China in the field of AI.

In contrast, Ukraine has adopted a more flexible and decentralized approach. Since 2014 and the beginning of the first War in Donbass, numerous non-profit and volunteer organizations have emerged and progressively evolved towards greater decentralization. This structure has provided distinct advantages, particularly in attracting and retaining skilled drone engineers and AI innovators. Early distribution networks benefited from reliable and transparent feedback informed by frontline soldiers and their experience. Recognizing the technical expertise of these organizations, the Ukrainian government actively sought to collaborate with them. Following the onset of the full-scale war in

2022, Ukrainian private enterprises and volunteer groups played a pivotal role in pioneering the deployment of first-person-view (FPV) drones and introducing AI-assisted equipment to frontline units and command posts—often leveraging personal connections with soldiers and field units. Following the early upheaval of the invasion and subsequent counteroffensives in 2022 and 2023, the Ukrainian government renewed its push to advance AI innovation in the defence sector, giving its development still more decentralization and developmental freedom that it is compared to the Russian approach, but still showing the incentive that this development of the AI gets in the essence state institutional backing.

Ukrainian private enterprises and volunteer groups played a pivotal role in introducing AI-assisted equipment to frontline.

Current most prominent military action reportedly involving AI is the well-known "Operation Spider web" from June 2025, in which swarms of truck launched FPV *kamikaze* drones wreaked havoc on dozens of aircraft of the Russian strategic bomber fleet on airfields across Russia. According to open-source intelligence and reports, members of the Ukrainian SBU intelligence service studied construction and visual profiles of the targeted aircraft including Tu-95MS, Tu-22M3, and A-50 models, which are preserved in Ukrainian aviation museum such as the Poltava Museum of Long-Range and Strategic Aviation, to identify precise weak points. While there has been no official confirmation that the drones conducted AI-assisted autonomous strikes, it is likely that the mentioned incorporation of AI-driven object recognition within their control systems enhanced operators' capacity to identify and target specific vulnerabilities on enemy aircraft. In practice, these drones functioned as precision-guided weapons, remotely manually piloted, yet potentially capable of performing final targeting manoeuvres with computational support. How far will the AI development and military application go, it is yet to be seen.

Conclusion

It is definite that 2020's are bringing us the reemergence of the active warfare and the developments in the military technologies. Drones, both of the medium-altitude long-endurance (MALE) and commercial off-the-shelf (COTS) classes, have become and are becoming more than ever the essential parts of the modern armed and police forces. Once considered as a „poor man's air force," commercial drones have proved as very cost effective weapon against both heavy armor and infantry as well as large stationary objects such as airbases or industrial/energetic infrastructure. Their simplicity and price made them one of the essentials of the industrialized warfare production, like Ukrainian or Russian ones, and also useful for non-state actors, such as the narco cartels in Latin America. Consequently, the anti-drone warfare is also evolving to address the need for precise, effective, and cost-efficient responses to swarms of these inexpensive yet lethal aircraft. Cyber and electronic warfare have become essential, as data theft provides critical intelligence for

adversaries and a single piece of malware can disable or shut down an adversary's defenses and equipment. Cyberspace has therefore become indispensable, as digitalization has made the world and consequently, the military dependent on and inseparable from digital infrastructure. The war in Ukraine has demonstrated the extent to which cyber activities are defining the modern conflicts.

The escalating weaponization of the artificial intelligence made the domain of combat and decision making much quicker and lethal than before. Autonomous systems, predictive analytics, and AI-assisted targeting have reduced human workload, while increasing precision and adaptability across all domains of warfare. The rise of AI has expanded cyber operations, disinformation campaigns, and automated decision-making systems. A key question is whether fully autonomous combat systems represent the next stage of AI evolution and to what extent they will be deployed, given concerns over morality, control, and accountability. The international community and lawmakers continue to struggle with regulating AI-enabled weapons, which introduce new ethical and strategic risks, including escalation and reduced human oversight. One is for sure; the landscape of modern warfare is rapidly changing due to the evolving technologies. Ongoing conflicts such as the war in Ukraine and active geopolitical conflict hotspots in the Middle East are serving as testing grounds for a new military-industrial revolution, just like it was in past during both world wars.

Viktor Trumbetaš is an analyst and military historian who deals with geopolitical and military issues, currently working at the European Parliament in Brussels.

DISCLAIMER: The views presented in this paper are solely of the authors and do not represent an official position of the Institute for Development and International Relations (IRMO).

IRMO
Institut za razvoj i međunarodne odnose
Institute for Development and International Relations

Lj. F. Vukotinovića 2, Zagreb, Croatia
www. irmo.hr