Review of Contemporary Philosophy
ISSN: 1841-5261, e-ISSN: 2471-089X
Vol 24 (01), 2025
pp. 824 - 849

Advanced Technologies and Battlefield Transformation: A Legal and Ethical Reading of the Russia-Ukraine Conflict

[1] María Stephania Aponte García *, [2] Gabriel Andrés Arévalo-Robles, [3] Alexander Romero-Sánchez

[1] Doctoral candidate in Law at the Universidad Libre de Colombia, Master of Laws in Constitutional Law, Attorney. Full-time Professor at the Central University of Valle del Cauca (UCEVA), Tuluá, Valle del Cauca, Colombia. Email: maponte@uceva.edu.co. ORCID: https://orcid.org/0000-0003-2642-2896
Corresponding Author

[2] PhD in International Studies, University of the Basque Country/Euskal Herriko Unibertsitatea. Master's Degree in International Studies (UPV/EHU). Master's Degree in Decentralized International Cooperation (UPV/EHU). Lawyer, Universidad Libre. Sociologist, National University of Colombia. Currently serves as National Director of Research, Universidad Libre. Email: gabriel.arevalo@unilibre.edu.co ORCID: https://orcid.org/0000-0002-4389-5997

[3] Doctor of Business Administration from San Buenaventura University, Cali, Colombia. Master of Economics, Management, and Business Administration from the University of Salerno. Business Administrator. Vice-Rector of Research and Community Outreach and Full-Time Professor at the Central Unit of Valle del Cauca, Tuluá, Valle del Cauca, Colombia. Email: aromero@uceva.edu.co ORCID: https://orcid.org/0000-0003-1928-7315

Abstract:

Technological advancement is transforming the nature of contemporary armed conflicts. The war between Russia and Ukraine has highlighted the increasingly critical role of advanced technologies—such as artificial intelligence, cyber systems and autonomous weapons on the battlefield. This integration raises legal and ethical challenges within the framework of International Humanitarian Law, requiring an examination of its application and scope. This article first reviews the IHL regulatory frameworks applicable to the use of emerging technologies. It then identifies ethical dilemmas arising from drone attacks, digital sabotage operations and algorithmic disinformation practices. The methodology employed consists of a qualitative documentary approach that integrates sources from 2017 to 2025, including United Nations resolutions, reports from the International Committee of the Red Cross, UNESCO technical documents and analyses from specialized research centers. The corpus is organized into three analytical dimensions: IHL regulation, relevant technological characteristics and political-legal impacts. Through a thematic comparative method, normative standards are cross-referenced with case studies involving kamikaze drones, cyberattacks on critical infrastructure and artificial-intelligence-based facial recognition in military operations. The conclusions reveal regulatory gaps regarding meaningful human control, responsibility attribution, algorithmic transparency and the protection of civilian assets. The analysis shows that the conflict exposes substantive limitations within the current international framework and underscores the need to strengthen these mechanisms to address the challenges posed by disruptive military technologies.

Keywords: International Humanitarian Law, Artificial Intelligence, Autonomous Weapons, Cyberconflict, International Responsibility.

Received: 19 October 2025 **Revised:** 4 November 2025 **Accepted:** 26 November 2025

introduction

The armed conflict between Russia and Ukraine has become one of the most paradigmatic scenarios of contemporary warfare, not only because of its geopolitical impact, but also due to the intensity with which advanced military technologies have been incorporated into it. Artificial intelligence (AI) systems applied to targeting, emerging autonomous weapons, cyber operations against critical infrastructure, and algorithmic disinformation campaigns have redefined the way hostilities are planned and conducted, turning the Ukrainian theater into a true laboratory of war experimentation. In this context, the traditional categories of International Humanitarian Law (IHL) and the ethics of war are strained by practices and means of warfare that overflow the frameworks for which those norms were originally conceived.

The premise of the technological neutrality of IHL, according to which its principles apply to every form of war and every type of weapon, including those of the future, faces unprecedented challenges when lethal decisions are delegated to algorithms, cyberattacks unleash cascading effects on highly digitalized societies, and armed drones are used both as instruments of defense and as tools of terror against the civilian population. This compels us to question to what extent the principles of distinction, proportionality, and precaution can continue to ensure effective protection of civilians in the face of technologies that are increasingly autonomous, opaque, and difficult to attribute.

From a legal-ethical perspective, the Russia–Ukraine conflict not only reveals concrete violations of IHL, but also underlying regulatory gaps and moral dilemmas. Among these stand out the notion of "meaningful human control" over autonomous weapons, the attribution of responsibility for algorithmic decisions, the protection of civilian infrastructures and data in cyberspace, and the impact of automated information warfare on truth and human dignity. At the same time, the response of international organizations, States, humanitarian agencies, and technology companies has set in motion processes of normative reinterpretation and proposals for new rules to limit the use of these disruptive capabilities.

Based on this scenario, the article offers an integrated reading of the Russia–Ukraine conflict as a critical case for assessing the adequacy of the current humanitarian legal framework and for discussing the emerging ethical challenges posed by the technological transformation of the battlefield.

1. Methodology

This study adopts a qualitative design with a documentary-analytical approach, based on the systematic and critical review of secondary sources (Romero et al., 2024ª; Martínez, 2025) produced between 2017 and 2025, a period in which the use of advanced technologies in the Russia–Ukraine conflict intensified. Resolutions of the UN General Assembly and Security Council, reports from the Independent International Commission of Inquiry on Ukraine, statements by the International Committee of the Red Cross, and UNESCO technical documents on the ethics of artificial intelligence were examined. Additionally, reports from multilateral organizations, statements by CCW governmental expert groups on autonomous weapons, and analyses from specialized think tanks (RUSI, CSIS, Chatham House) were incorporated.

The documentary corpus was organized according to three analytical dimensions: (i) the applicable legal framework—International Humanitarian Law, international law, and the principles of distinction, proportionality, and precaution; (ii) emerging technologies in armed conflict—autonomous weapons, military AI, and cyber operations; and (iii) observable political-legal impacts on the conduct and regulation of the conflict. The analysis was carried out using a thematic comparative method aimed at cross-referencing legal-normative evidence with concrete case studies from the conflict (Aponte et al., 2025a).

The procedure included: identifying relevant documented events (Romero et al., 2024b; Martínez and Escobar, 2025) such as the use of kamikaze drones, cyberattacks on critical infrastructure, and the employment of AI systems for targeting and surveillance; extracting patterns of state or armed group behavior; and contrasting these with international standards found in the analyzed sources. Each case—cyberattacks on the electrical grid, drone attacks on civilians, deepfakes as an information weapon—was evaluated in light of IHL and emerging regulatory frameworks on autonomous weapons and AI, verifying compliance or infringement with humanitarian principles (Aponte Garcia et al., 2025b). Finally, a

triangulation process was applied among legal sources, technical reports, and available empirical evidence to strengthen interpretive validity and support the findings regarding the ethical, operational, and regulatory challenges identified in the contemporary conflict.

2. Results and discussion

IHL regulatory framework in relation to new technologies of war

The first issue to clarify is which international legal framework governs the use of advanced technologies—AI, cyber systems, and autonomous weapons—in armed conflict. A cardinal principle is that IHL is technologically neutral: its rules apply to "all forms of warfare and all types of weapons, including those of the future" (Aponte et al., 2020), according to the jurisprudence of the International Court of Justice (Winter, 2022; International Committee of the Red Cross, 2024 [ICRC], 2024). In other words, the fact that a weapon or method of warfare is new does not place it in a legal vacuum; on the contrary, it remains subject to existing IHL norms and principles (Gunawan et al., 2022; International Committee of the Red Cross and Red Crescent, 2024). Among these fundamental principles are distinction (prohibition of attacks against civilians or civilian objects), proportionality (avoiding attacks that cause excessive civilian harm relative to the anticipated military advantage), and precaution in attack (ICRC, 2024; Hamad, 2025). Thus, any new weapon system—whether an AI algorithm in a targeting system, an offensive computer virus, or an armed autonomous drone—must be capable of operating in compliance with these principles; otherwise, its use would be prohibited under IHL (Casey-Maslen, 2025). In this regard, the UN General Assembly, in response to Russia's invasion of Ukraine, explicitly urged all parties to "respect IHL and human rights," protect the civilian population (especially vulnerable groups), and refrain from attacks on civilians or civilian objects. This political-legal reaffirmation underscores that, even in the face of emerging war technologies, basic humanitarian standards remain fully in force in the conflict (Bratu & Freeland, 2026).

Autonomous weapons and artificial intelligence: obligations and regulatory gaps

Regarding lethal autonomous weapons—those capable of selecting and attacking targets without direct human control—there is still no specific international treaty regulating them (Aponte Garcia et al., 2025c). However, their development has been the subject of intense debate within the international community under the premise that applicable IHL (particularly norms on distinction, proportionality, and command responsibility) may be challenged by these weapons (Winter, 2022). In fact, multiple States and organizations, including the International Committee of the Red Cross (ICRC), question whether fully autonomous systems can meet IHL requirements due to the difficulty of programming them to correctly distinguish between combatants and civilians or to assess proportionality in real time (Perišić & Tomljenović, 2024). Additionally, the issue of legal responsibility arises: IHL attributes responsibility for acts to human combatants and commanders, so delegating life-or-death decisions to a machine blurs accountability (Copeland et al., 2023a).

In light of these concerns, general principles such as the Martens Clause have been invoked; under this clause, in the absence of specific rules, "the principles of humanity and the dictates of public conscience" continue to protect the population (International Committee of the Red Cross and Red Crescent, 2024). Moreover, Article 36 of Additional Protocol I of 1977 requires States to conduct legal reviews of all new weapons to ensure their conformity with IHL before use. This means that any AI-based or autonomous weapon must undergo prior scrutiny to verify that it is not inherently indiscriminate and does not cause "superfluous injury or unnecessary suffering" (Tsybulenko & Kajander, 2022; Copeland et al., 2023b).

In practice, given the absence of a binding treaty, States have turned to diplomatic forums to address this issue. Since 2014, within the framework of the UN Convention on Certain Conventional Weapons (CCW), a Group of Governmental Experts has discussed Lethal Autonomous Weapon Systems (LAWS). As a result of those deliberations, eleven guiding principles were agreed upon in 2019, including: that IHL fully applies to autonomous weapons, that humans "must retain responsibility for decisions concerning the use of weapons," and that machines remain subject to human control (Jackson, 2023). However, the lack of consensus has so far prevented progress toward a protocol or prohibition/restriction treaty. Military

powers such as Russia and the United States have opposed a total ban, favoring instead non-binding guidelines that preserve technological innovation (Bächle & Bareis, 2022).

Still, normative momentum has recently increased: in late 2024, the UN General Assembly adopted a resolution (166 votes in favor, 3 against, 15 abstentions) proposing negotiations for a legal instrument on autonomous weapons, combining a prohibition on certain LAWS with strict regulation of others (American Society of International Law, 2025). Notably, Ukraine was among the abstentions, possibly reflecting that, in the midst of war, its priorities center on immediate military effectiveness rather than imposing limits that could restrict potentially advantageous technologies (Human Rights Watch, 2024).

At the same time, high-level international officials have spoken out: UN Secretary-General António Guterres has described the very idea of out-of-control "killer robots" as "morally repugnant" and has urged negotiating their prohibition (Solovyeva & Hynek, 2023). The ICRC, for its part, has since 2021 called for new binding norms that "impose clear prohibitions and restrictions" on autonomous weapons, including the absolute prohibition of unpredictable systems or those designed to operate against persons (e.g., lethal robots that select humans as targets) (Ferl, 2024; International Committee of the Red Cross and Red Crescent, 2024). For other autonomous systems, the ICRC advocates requiring "meaningful human control" in their use. These recommendations, supported by UNESCO and various NGOs (e.g., the Stop Killer Robots campaign led in part by Human Rights Watch), reflect an emerging ethical consensus: preserving human agency in lethal decisions and preventing military AI from undermining humanitarian protection and human dignity in war.

Cyber operations and armed conflict: IHL in cyberspace

Alongside AI, the other major technological dimension in this war is cyberspace. Russia's aggression against Ukraine has been waged not only with tanks and missiles but also through cyberattacks against critical systems, government networks, and large-scale digital disinformation. In this context, the question arises: how does IHL apply to cyber operations in an international armed conflict?

First, it must be reiterated that cyber operations in war "do not occur in a legal vacuum." By international consensus, the same rules governing traditional means and methods of warfare also govern hostilities in cyberspace (ICRC, 2024; Biggio, 2025). Thus, a cyberattack that meets the threshold of an "attack" under IHL (i.e., causing damage to objects, injury, or death) must respect the principles of distinction and proportionality just like a conventional kinetic attack (Khalil & Raj, 2024). For example, it is prohibited to deliberately launch a computer virus to disable the IT system of a civilian hospital or an electrical plant if doing so affects the civilian population; this would constitute an attack directed at civilian objects, which is forbidden under IHL. Likewise, an indiscriminate cyberattack that spreads uncontrollably and equally affects civilian and military systems would be unlawful (Sohail, 2022). These criteria are clearly established: "attacks against civilians and civilian objects are prohibited; […] indiscriminate and disproportionate attacks are prohibited; medical services must be respected and protected. These rules […] also apply in cyberspace" (ICRC, 2024).

However, the technical particularities of cyberspace raise certain gaps and grey areas in the application of IHL. For instance, there is debate over whether certain cyber acts without physical damage constitute "attacks" under humanitarian law. What happens if a hack deletes essential civilian databases or temporarily blocks critical services without destroying equipment or killing people? Some experts argue that the destructive alteration of essential data should be treated as an attack (because it can paralyze a hospital just as effectively as bombing it), while others contend that, lacking direct physical damage, such acts fall outside the strict IHL definition of attack (AL-Hawamleh, 2023; Biggio, 2025). The protection of civilian data as civilian objects remains under analysis. Another issue is the difficulty of attribution in cyberspace: identifying with certainty the author of a cyberattack (State or group) may take time or be impossible in the midst of conflict, hindering responsibility under international law (Prasad et al., 2025).

Despite these uncertainties, steps have been taken to clarify and develop norms. Several non-binding initiatives, such as the Tallinn Manual (an academic legal study), have interpreted how existing rules apply

to cyber scenarios. For example, a cyberattack that disables a civilian electrical grid in winter may violate the principle of humanity even without immediate deaths, due to the suffering inflicted on the population (ICRC, 2020; Biggio, 2025). Politically, the UN has established Groups of Governmental Experts and an Open-Ended Working Group on information security, which in 2021 reached a common understanding: international law—including the UN Charter and, in armed conflict, IHL—does apply to ICTs, and States must exercise due diligence not to allow unlawful cyber activities from their territory (United Nations, 2021). Additional voluntary norms were recommended, such as refraining from harming critical civilian infrastructure through cyber means during peacetime. Although these recommendations do not specifically address wartime, they reveal global concern (Aponte & Sanchez, 2024) over setting limits on hostile uses of cyberspace (Bace et al., 2024).

The ICRC has emphasized the importance of "reaching a common understanding of the legal limits applicable to cyber operations during armed conflicts." In a 2020 report, it warned of the "potential human cost" of cyber weapons and the need for IHL interpretation to also protect the digital infrastructure upon which modern civilian life depends (ICRC, 2020, 2024b). This position underscores that humanitarian protection must cover not only hospitals, schools, and power grids in their physical dimension but also their IT systems and data, increasingly integral to their functioning. In sum, although IHL provides a clear general framework for cyber operations (prohibition of attacks on civilians, etc.), rapid technological evolution requires ongoing clarification of how rules apply to unprecedented situations. For example, a massive hack causing economic chaos or widespread panic could be considered a form of psychological or information warfare, whose relationship with IHL is still debated (Абрашин, 2024).

Before closing this normative section, it should be noted that both Russia and Ukraine—as well as the vast majority of States—formally recognize the applicability of IHL to their military operations, whether kinetic or cyber (Organization for Security and Co-operation in Europe [OSCE], 2023). Ukraine, in repelling the aggression, has insisted that its actions fall within self-defense and that it seeks to comply with humanitarian norms, even in the digital realm (Khoirunnisa et al., 2025; Casey-Maslen, 2025). Russia, by contrast, has blocked normative advances at the international level, such as negotiations on new treaties regarding autonomous weapons, and has not publicly acknowledged responsibility for cyberattacks, maintaining the opacity typical of hybrid warfare. Nonetheless, the clear expectation of the international community, reflected in UN resolutions, is that both States strictly respect IHL regarding new means and methods of warfare (United Nations, 2024). Violations of these norms—whether through an autonomous drone carrying out mass civilian killings or malware depriving thousands of people of drinking water—constitute war crimes and entail both individual and State responsibility.

Emerging ethical challenges in the use of AI, cyberweapons, and autonomous weapons

Beyond legal norms, the incorporation of AI and autonomous systems into warfare gives rise to profound ethical dilemmas. Even when technically complying with IHL, these technologies raise questions about the morality of delegating lethal decisions to algorithms, the erosion of human judgment in combat, and the potential blurring of responsibility for acts of war (Guo, 2025). The main emerging ethical challenges are examined below:

(i) Dehumanization of the decision to kill: Delegating the decision to attack a target to a machine—whether an autonomous drone or a targeting software system—may violate the principle of human dignity. Traditionally, killing in war, although permitted under certain conditions, involves a human deliberative process and real-time moral judgment. If an algorithm makes that decision, there is a concern that human life may be reduced to a set of data to be processed, leaving no room for compassion, prudence, or doubt that a human soldier might experience (Renic & Schwarz, 2023). Various experts and organizations (including UNESCO in its Recommendation on the Ethics of AI, 2021) have emphasized the need to preserve meaningful human control over weapon systems for moral reasons (Engelhardt & Kessler, 2024; Jackson, 2023b; O'Connell, 2023). Human Rights Watch, for instance, refers to a "moral imperative" to prohibit killer robots before they erode fundamental humanitarian values (Docherty, 2018).

(ii) Accountability and the "responsibility gap": A crucial ethical-legal issue is: if an autonomous weapon

commits an atrocity (for example, mistakes civilians for combatants and kills them), who is accountable? The programmer of the algorithm? The commander who deployed the system? The operator who activated it? The military leadership as a whole? This indeterminacy threatens to create an impunity gap: no individual could be directly culpable if they can claim "the machine did it" (Verdiesen et al., 2021; Winter, 2021). Such a scenario contradicts the foundational notion of justice for war crimes. Ethically, it is unacceptable for responsibility to be obscured behind an algorithmic "black box" (Chomanski, 2023). Therefore, it is argued that there must always be a clearly defined chain of responsibility, with humans legally accountable for the actions of autonomous systems (Cools & Maathuis, 2024). Some countries have proposed strict state liability for harm caused by their autonomous weapons, combined with ex-ante human oversight obligations (Li, 2025). However, no global consensus exists on a specific liability regime, raising legitimate concerns among human rights organizations (Javed, 2025).

(iii) Unpredictability and risk of catastrophic errors: AI-based systems (especially those using machine learning) may behave unpredictably, particularly in complex and dynamic environments such as the battlefield (International Committee of the Red Cross and Red Crescent, 2024; Podar & Colijn, 2025). This unpredictability is ethically troubling: is it right to deploy an autonomous weapon knowing its behavior cannot be fully guaranteed? A misidentification error (e.g., confusing a school bus with a military target) could result in a massacre of civilians (Figueroa et al., 2023). IHL requires discernment in attacks; if AI cannot provide such certainty, an ethical tension arises between innovation and the duty of protection (O'Connell, 2023). Moreover, AI may amplify the scale and speed of operations beyond human control capacity, reducing the time available for ethical reflection in attack decisions (Reichberg & Syse, 2021). A hypothetical example is swarms of autonomous drones attacking multiple targets within seconds, leaving no possibility of human intervention in each case and posing a risk of cascading collateral damage. Traditional military ethics emphasize prudence and control; algorithmic warfare could undermine those safeguards.

(iv) Conflict escalation and lowering the threshold for war: The "psychological distance" afforded by remote technologies (remotely piloted drones, AI-guided precision missiles, anonymous cyberattacks) may make the use of force politically easier and accompanied by fewer moral reservations (Johnson, 2020; Simmons-Edler et al., 2024). If soldiers no longer risk their lives directly because robots or autonomous systems take their place, leaders may be more willing to employ force, lowering the ethical threshold for initiating or escalating hostilities (Wood, 2022). This presents a dilemma: protecting soldiers' lives through technology (a positive outcome) versus making war less costly and thus more likely (a negative outcome for peace). The Russia–Ukraine war offers clues: the Ukrainian side, facing a numerically superior enemy, has embraced autonomous solutions and drones to protect its soldiers, implementing a "robots-first" strategy in certain operations (Kunertova, 2023; Mewoh & Rahmadan, 2025). While understandable from an ethics-of-self-preservation perspective, this widespread trend could imply that future powers will fight conflicts with machine armies, perhaps with less pressure to seek peaceful solutions (Sotoudehfar & Sarkin, 2024). In cyberspace, the relative invisibility and deniability of cyberattacks can also incentivize their aggressive use without considering humanitarian consequences. Ethically, this undermines efforts to contain war (Niyitunga, 2022).

(v) Algorithmic bias and discrimination: AI inherits biases from its training data. In military contexts, an algorithm could mistakenly associate certain profiles (for example, young men of a particular ethnicity) with threats, increasing the risk of unjustified shootings against individuals who fit that profile. This would not only violate principles of equality and non-discrimination but could translate into crimes against specific groups (Bhila, 2024; Ojha, 2025). A hypothetical case is a computer-vision system trained mainly on images of white enemy soldiers, failing to identify ethnic-minority civilians correctly—or vice versa. The lack of transparency in many AI systems (black boxes) makes detecting and correcting such biases difficult, which is ethically troubling when lives are at stake (Nazeer, 2024). UNESCO and the European Union have advocated for "trustworthy," explainable AI; applied to warfare, this would require rigorous verification mechanisms ensuring that AI is not making decisions based on spurious or discriminatory correlations (Maphosa, 2024; Ortiz, 2024).

(vi) Intensification of informational and psychological warfare: The use of AI is not limited to physical weapons but also extends to information as a weapon. In the current war, we have seen deepfakes, automated social-media campaigns, and algorithmically targeted propaganda. AI can generate highly persuasive fake content (fabricated videos of leaders, manufactured news) that erodes truth and intensifies hatred (Gilbert & Gilbert, 2024; Alanazi et al., 2025). Ethically, this "cognitive cyberwarfare" poses enormous challenges: manipulating the perception of civilian populations and soldiers can prolong conflicts and justify atrocities (Kazić, 2025). Algorithmically amplified harmful discourse spreads faster than ever and carries "dangerous real-world consequences," as the president of the ICRC warned (ICRC, 2025). An unsettling example was the deepfake video of the Ukrainian president calling for surrender in 2022, briefly circulated on social media. Although quickly debunked, it demonstrated AI's potential to undermine the morale of an entire country (Roković, 2024). From an ethical standpoint, such tactics erode public trust and can incite violations of IHL (e.g., a soldier influenced by dehumanizing propaganda may be more prone to commit abuses). Regulating informational warfare is complex, but it is ethically imperative to distinguish between legitimate use of information (e.g., countering enemy propaganda) and disseminating lies that endanger civilians or encourage cruelty (Aslam, 2025).

The ethical challenges that emerge with AI and autonomous weapons in conflicts involve preserving humanity in war, ensuring clear responsibility for machine actions, preventing unpredictable harm, and safeguarding truth and human dignity (Engelhardt & Kessler, 2024; Marsili, 2024). These concerns complement the legal framework: even if a technological action complies with the letter of IHL, it may still be morally problematic (Ojha, 2025). For this reason, many experts argue that not only legal solutions are needed but also ethical codes and operational doctrines to guide the military in using these tools with prudence, humanity, and accountability (Ahmad et al., 2025).

Advanced technologies in the Russia–Ukraine conflict: cases and lessons

The conflict in Ukraine has been regarded as a laboratory in which cutting-edge military technologies are tested and used on a large scale. Both Russia and Ukraine, each with its own motivations, have incorporated drones, autonomous systems, cyberattacks and even AI applications into their operations (Akhtar, 2025; Kunertova, 2023b). This section analyzes reported or alleged cases of the use of such technologies in this war, drawing lessons about their practical and humanitarian impact (Pandey, 2025).

Use of armed drones and autonomous systems on the battlefield

Illustration of a military drone chasing a civilian in a devastated urban area, reflecting the dangers these technologies pose to the civilian population. Drone operations have acquired unprecedented prominence in Ukraine. From unmanned aerial vehicles (UAVs) for reconnaissance to loitering munitions, both sides have exploited these platforms (Minculete & Păstae, 2023). Although many drones are remotely piloted by humans, the line toward autonomy is blurry: some models can identify targets or guide themselves automatically once launched (Bwana, 2023).

Russia, for example, has deployed Shahed-136 kamikaze drones (of Iranian manufacture) for long-range attacks against Ukrainian infrastructure (Bouks, 2023; Sotoudehfar & Sarkin, 2024). These drones are capable of autonomous flight preprogrammed toward GPS coordinates and fly in swarms; their intensive use from late 2022 onwards devastated power grids in Ukrainian cities in the middle of winter, causing massive blackouts (Boşneagu, 2024). Although the Shahed-136 does not select targets through AI (the target is fixed in advance), its autonomous navigation qualifies it as a simple autonomous weapon. Ukraine has denounced that such swarming attacks with Iranian drones were intended to spread terror among the civilian population, as they were directed at power plants rather than immediate military objectives, in violation of IHL (Human Rights Watch, 2025).

For their part, Ukrainian forces have also innovated with autonomous systems, mainly low-cost combat drones. The well-known Turkish Bayraktar TB2s—remotely piloted armed drones—destroyed columns of Russian armored vehicles at the beginning of the war. Over time, Ukraine began to produce or adapt commercial drones to drop munitions on enemy trenches. A Ukrainian commander stated that "drones play

a very big role on the battlefield, more than anything else," marking the beginning of a strategy that prioritizes robots over tanks (Kunertova, 2023b; Plakoudas & Sofitis, 2023).

In 2023, the "Army of Drones" initiative emerged, supported by volunteers and Western technology companies, providing UAVs for surveillance and attack. The "Avenger" platform was even announced, integrating AI to assist in target selection and drone coordination (Spansvoll, 2024). The strategic objective of Ukraine, according to its officers, is to minimize the exposure of its soldiers by replacing them with "unmanned systems" wherever possible (Nazirah et al., 2024). This need—born of numerical inferiority and a will to protect its troops—has driven rapid innovation. However, it also raises immediate ethical concerns: according to reports, combat pressure led some Ukrainian units to adjust their drone-use protocols to treat them almost as "shoot first, ask questions later." Operators were trained to treat "ambiguous targets" as threats, increasing the likelihood that automated drones might attack non-combatants or hors de combat soldiers by mistake (Sotoudehfar & Sarkin, 2024).

One documented case illustrating the misuse of drones against civilians occurred in the city of Kherson (southern Ukraine) during 2023–2024. Human Rights Watch investigated numerous incidents in which Russian forces used armed drones—mainly commercial quadcopters adapted to drop explosives—to deliberately attack civilians on streets, in evacuation centers and in car convoys (Human Rights Watch, 2025). These ad hoc drone attacks, low-cost but with high tactical precision, "appear designed to spread terror among the civilian population," according to the Human Rights Watch report (3 June 2025). HRW documented at least 45 Russian drone attacks against civilians in Kherson in 2024, including the bombing of ambulances, medical teams and even the dropping of banned antipersonnel mines over residential neighborhoods (Human Rights Watch, 2025).

The evidence—drone videos with mocking inscriptions shared on pro-Russian Telegram channels—indicates a clear intent to terrorize. These acts constitute serious violations of IHL (indiscriminate or direct attacks against civilians) and even crimes against humanity as part of a systematic attack on the population (Human Rights Watch, 2025). What is troubling is how easily available this tactic was: Russia simply adapted Chinese civilian drones (DJI, Autel) by equipping them with explosives (Human Rights Watch, 2025). The accessibility of commercial technology allowed Russia to perpetrate war crimes in a way previously reserved for specialized weaponry. This exposes a challenge: how to control the proliferation of civilian drones that can be used as weapons? The manufacturers themselves stated that such use violates their policies, but acknowledging it reveals the impotence of these voluntary mechanisms in the face of malicious military uses (Human Rights Watch, 2025).

Another technological front is unmanned ground and naval systems. Russia has tested some robotic ground vehicles (UGVs) in urban combat, though with limited success due to technical difficulties. Ukraine, by contrast, surprised observers in 2023 with its use of unmanned naval drones to attack Russian vessels in the Black Sea and bases in Crimea—a tactic documented by defense analysts as a milestone in the evolution of autonomous maritime warfare (Clark, 2024). These so-called "naval kamikaze drones," fast boats loaded with explosives and remotely directed, damaged at least one Russian landing ship and opened a new domain: autonomous war at sea (Bosneagu, 2024).

At the same time, both sides have used loitering munitions—suicidal roaming drones, such as the Russian Lancet or the Polish Warmate—equipped with algorithms to detect electronic or visual signatures and dive onto targets. Recent studies emphasize that these systems "border on lethal autonomy," operating with minimal human intervention (Bwana, 2023). The war in Ukraine has demonstrated their lethality against tanks and radars, with no confirmed reports of catastrophic misidentification, although the possibility of errors remains an ethical and legal concern under International Humanitarian Law (Czerwiński & Balcerzak, 2024).

The legacy of this proliferation of drones in Ukraine is ambivalent. On the one hand, they have been crucial defensive tools for Ukraine and have proven to be inexpensive "force multipliers," redefining land warfare (for example, allowing artillery to adjust its fire in near real time thanks to drone observation) (Borsari & Davis, 2023; Kirichenko, 2025). On the other hand, their indiscriminate use by Russia against civilians

shows their darkest side: investigations by Human Rights Watch and the Independent International Commission of Inquiry on Ukraine document systematic drone attacks against the civilian population, characterized as serious violations of international humanitarian law and even crimes against humanity (Human Rights Watch, 2025; Independent International Commission of Inquiry on Ukraine, 2025). International observers warn that many of these tactics and technologies, "tested and refined in Ukraine," will soon appear in other conflicts around the world (Kirichenko, 2025). Indeed, Western countries have already accelerated their drone programs (including autonomous systems), learning from Ukraine's experience, as reflected in the sharp increase in British investment in unmanned systems and Germany's development of the AI-enabled loitering drone Virtus/OWE-V (Reuters, 2024; Brizard, 2025). Some diplomats have even described events in Ukraine as our generation's "Oppenheimer moment," warning that the proliferation of autonomous weapons could transform warfare in a way comparable to the introduction of the atomic bomb and force an international regulatory response (Kirichenko, 2025; Robins-Early, 2024).

The cyber front: attacks and digital operations

Parallel to the physical combat, the Russia–Ukraine war has been intensely waged in the cyber domain. Russia, even before the open invasion of 2022, had been using cyberattacks against Ukraine as part of its hybrid aggression: recall the massive 2017 "NotPetya" malware attack (apparently launched against Ukrainian infrastructure, which ended up causing billions in global damage) (Greenberg, 2018; U.S. Department of Justice, 2020) or the power outages caused by Russian hackers in Kyiv in 2015–2016 (Zetter, 2016). Since February 2022, this campaign intensified through attempts to disrupt Ukraine's defenses and society. One of the first acts of the invasion was a cyberattack on the Viasat satellite network, which deprived Ukrainian units of military communications and incidentally affected civilian services across Eastern Europe (Mura et al., 2024). Destructive malware (wipers) was also detected in Ukrainian ministries and banks, designed to erase data and sow chaos in the rear (EU Agency for Cybersecurity, 2023). Although these attacks did not cause direct deaths, they clearly sought to weaken critical civilian and military functions, violating the rule prohibiting attacks against civilian infrastructure. In fact, the European Union and the United States publicly attributed these cyberattacks to Russia, calling them irresponsible and contrary to international norms (Council of the European Union, 2022).

Ukraine responded not only by strengthening its cyberdefense but also by mobilizing an "IT Army" of volunteers and global hacktivists to digitally harass Russia (Burgess, 2022). This "voluntary cyber force," tacitly backed by the Ukrainian government, has conducted DDoS attacks against Russian government websites, intrusions to leak data from Russian state agencies, and even manipulations of Russian television to broadcast real images of the war (Canadian Centre for Cyber Security, 2022; Soesanto, 2022). Although Ukraine maintains that these actions focus on legitimate military or propaganda-related targets, the blurred line between civilians and combatants in cyberspace poses a dilemma: many of these hackers are foreign civilians whose active participation could classify them as directly involved in hostilities, thus losing protection (Byczyński, 2024; International Committee of the Red Cross, 2023). IHL was not designed for global digital volunteers, making this an area where reality has surpassed the traditional framework (International Committee of the Red Cross, 2023).

Among emblematic cases is the foiled April 2022 cyberattack on the Ukrainian power grid (Greenberg, 2022). The Russian hacker group known as Sandworm (linked to the GRU military intelligence) introduced malware dubbed "Industroyer2" into a power company, with the apparent intention of causing a massive blackout in Kyiv (Greenberg, 2022). Fortunately, the rapid response of CERT-UA (Ukraine's Computer Emergency Response Team) neutralized the attack before it caused damage (Greenberg, 2022). Nonetheless, had it succeeded, hundreds of thousands of civilians would have been left without electricity, heating and water (Greenberg, 2022; Gisel et al., 2020; ICRC, 2020). This would have constituted a deliberate attack on essential civilian infrastructure, prohibited by IHL (Gisel et al., 2020; ICRC, 2020; ICRC, 2023). The incident demonstrates both the real threat posed by cyberattacks during war and the importance of strengthening cyber defenses (in this case, Ukraine had support from Western technology companies to monitor its networks) (Microsoft, 2022). It also highlights the difficulty of proportionality:

Sandworm may have intended to compromise military command systems interconnected with the electrical grid, but given digital interdependence, isolating the effects is nearly impossible (Gisel et al., 2020; ICRC, 2023). In practice, a broad cyberattack will almost always produce civilian consequences, making it intrinsically problematic under IHL unless used with extreme precision (Gisel et al., 2020; ICRC, 2020, 2023).

Another front was the sabotage of satellites and communications. Beyond the Viasat hack, Russia has attempted to interfere with GPS and satellite signals to disorient Ukrainian forces (Council of the European Union, 2022; Slusher, 2025; Smith, 2022). There were even concerns that Russia could physically attack satellites used by Ukraine (for example, Starlink communications satellites) (Slusher, 2025; Smith, 2022). The militarization of outer space, though beyond the scope of this chapter, also intersects with IHL: destroying a civilian satellite providing internet to hospitals could be considered an illegal attack on civilian objects, demonstrating the need to update legal interpretations for new domains.

Finally, information warfare on social media and digital platforms—though not a "technical cyberattack"—has been intensified by digital technologies (Iskoujina et al., 2024; Mejova et al., 2025). Russia deployed an extensive disinformation apparatus to justify its invasion (false narratives of "denazification," denial of atrocities such as Bucha by calling them staged, etc.), supported by bot farms and automated accounts spreading propaganda (Brusylovska & Maksymenko, 2023; Prysiazhniuk, 2025). Ukraine responded effectively in the global information sphere, also using social networks (though mostly with verified information and awareness campaigns, which fall under legitimate information warfare) (Prysiazhniuk, 2025; Iskoujina et al., 2024). A notable case was Ukraine's use of facial recognition technology: the Ukrainian Ministry of Defense admitted to using an AI platform (Clearview AI) to identify the faces of Russian soldiers killed in combat, in order to notify their families in Russia and even to detect infiltrators (Bhuiyan, 2022; Bergengruen, 2023). This application of AI—bordering on issues of privacy and the dignity of the dead—was justified as a psychological tactic to undermine Russia's hidden narrative of its casualties (Bergengruen, 2023). Although it does not directly violate IHL, it raises ethical concerns about the limits of using biometric data in war (Madziwa, 2024; Rosenzweig & Pacholska, 2025).

In sum, the cyber and informational dimension of the Russia–Ukraine conflict teaches us that digital operations can have effects as real and devastating as bullets or bombs (ICRC, 2019, 2020; Kerr, 2023). IHL provides guiding principles, but gaps emerge in its concrete implementation when facing malware and algorithmic propaganda (ICRC, 2020). The need to develop better mechanisms for protecting civilians in the digital sphere is evident: for instance, the ICRC has proposed agreements to refrain from attacking basic civilian digital infrastructure, similar to protections for medical infrastructure (ICRC, 2019, 2020). Likewise, collaboration with the technology sector is crucial: companies such as Microsoft, ESET and Starlink have acted as informal participants in this war, helping to defend or, in some cases, having their products used for attacks (Microsoft, 2022). This opens the debate on corporate co-responsibility in conflicts: should companies like Meta or DJI implement safeguards to prevent their platforms from being weaponized? (Renic & Christensen, 2024). Human Rights Watch has urged governments to "work with commercial drone manufacturers to develop safeguards that prevent their unlawful military use" (Human Rights Watch, 2025). A key lesson from Ukraine is that a USD 1,000 drone can become a weapon of terror; preventing this may require combinations of regulation (banning exports to armies that will use them against civilians), technology (geofencing in specific airspace), and, of course, strict enforcement of criminal accountability when abuses occur (Human Rights Watch, 2025; Renic & Christensen, 2024).

Applied artificial intelligence and information systems on the ground

AI applied to military intelligence has been another feature of this war (Rickli & Mantellassi, 2024). Ukraine, with support from its allies, has used advanced algorithms to process satellite and drone imagery, speeding up the identification of Russian movements and selecting targets with greater precision (Kunertova & Herzog, 2024). Western companies have provided big-data and AI platforms (such as Palantir) to help coordinate combat and logistics in real time (Jones et al., 2023; Re-Russia, 2023; The Washington Post, 2023). These uses of AI, though less visible, likely contributed to Ukraine's ability to repel attacks and

optimize the use of its scarce resources (Jones et al., 2023). From a humanitarian perspective, well-trained AI could even reduce collateral damage by enabling more refined targeting that avoids civilians (ICRC, 2020). However, there is also a risk of over-reliance on algorithmic recommendations: military AI is not error-free, and if a commander delegates critical judgment to a system that mistakenly flags an ambulance as a "valid target," they could commit a violation of IHL while hiding behind the supposed infallibility of the machine (ICRC, 2020).

A noteworthy development is the creation of databases and large-scale recognition systems to document war crimes. Ukraine, supported by international organizations, has collected millions of data points (camera footage, satellite images, intercepts) on incidents in the conflict. AI is used to filter and analyze this enormous volume of information with a view to future criminal prosecutions (Chlevickaitė, 2025). UNESCO has also contributed to projects that use AI to analyze 3D images and monitor the destruction of cultural heritage in Ukraine, in order to preserve evidence (Giannini, 2023; UNESCO & UNOSAT, 2023; UNESCO, 2024). This facet demonstrates a constructive use of technology: strengthening post-conflict accountability. Although not free of dilemmas (e.g., ensuring the accuracy and chain of custody of alterable digital evidence), it may be crucial for justice (Jančárková et al., 2024).

The emergence of generative AI also merits attention. During the conflict, deepfakes have circulated (not only the aforementioned video of Zelensky, but also fake audio recordings of commanders, etc.) (Kuźnicka-Błaszkowska, 2025; Pauwels, 2024). The accessibility of these tools creates an environment where distinguishing truth from deception is difficult, putting journalistic ethics, public credibility and even security to the test (UNESCO, 2025; Ahmed et al., 2024; Pauwels, 2024). The international community still lacks mechanisms to halt these tactics beyond countering them quickly with truthful information (Allen, 2022; Kuźnicka-Błaszkowska, 2025).

Finally, AI has even appeared in weapons supplied to Ukraine. For example, it has been reported that sniper scopes equipped with AI (for automatic calculation of wind and distance) have been delivered, and that modernized Ukrainian tanks incorporate targeting systems with target-recognition algorithms (Jones et al., 2023; New Strategy Center, 2025). Although these uses are essentially technical enhancements (they do not imply full autonomy), they demonstrate the trend toward integrating AI at all levels of the military art (Jones et al., 2023; Rickli & Mantellassi, 2024). Each integration entails the need to train operators to understand its limitations and avoid blind trust. Ethically, soldiers must remain aware that the final decision is theirs, not the AI chip's (Davison, 2017; Asaro, 2012; ICRC, 2021, 2025).

In sum, the Russia–Ukraine conflict offers multiple cases of high-tech use: civilian drones turned into terror weapons, semi-autonomous swarms, cyberattacks on power grids, algorithms analyzing intelligence, deepfakes in information warfare, among others. This combined reality has forced the international community to update its technical and legal analyses (ICRC, 2024). Bodies such as the UN and the ICRC have closely followed these developments, not only to condemn violations (e.g., the UN has created a Commission of Inquiry that also documents the use of indiscriminate weapons, including technology) but also to draw regulatory lessons (Independent International Commission of Inquiry on Ukraine, 2022, 2024, 2025; ICRC, 2024). Defense think tanks (Chatham House, CSIS, RUSI, etc.) have published reports assessing how these technologies have affected strategic stability (de Deus Pereira, 2025; Slusher, 2025). For example, a CSIS report identifies five transformative areas in this war: autonomous systems, information operations, electronic warfare, cyber defense and precision missiles, concluding that the synergy among them is redefining the conduct of modern warfare (Slusher, 2025). Likewise, analyses from the European Parliament highlight that the war in Ukraine has "demonstrated the critical role of AI in intelligence gathering, autonomous systems and cyber operations," accelerating a global arms race in military AI. All these assessments feed reflection on how to strengthen norms and ethics before these technologies spread even further.

Mechanisms of accountability and governance: assessing the international response

In light of the panorama described, the question arises: what mechanisms currently exist to ensure accountability for the misuse of AI, cyberweapons and autonomous weapons, and how is their governance being addressed at the international level? The answer, for now, is fragmented: traditional mechanisms of responsibility for violations of international law are combined with nascent efforts to develop specific norms and encourage responsible self-regulation (Aponte et al., 2025c).

As for accountability, the main framework remains International Criminal Law as applied to war crimes and crimes against humanity. If an advanced technology is used in such a way that it commits an IHL crime (for example, a commander launches a deliberate cyberattack against the civilian population, or deploys an autonomous weapon knowing it will cause indiscriminate deaths), that commander and those who ordered or participated can face criminal prosecution (Al-Billeh, 2025; AL-Hawamleh et al., 2023). In the case of Ukraine, initiatives have already begun in this regard: the International Criminal Court has opened an investigation into crimes committed in the conflict and, although it has so far focused on conventional atrocities (killings, deportations, etc.), there is no obstacle to considering cyber or drone attacks as war crimes in the future if they meet the requisite elements (intentional attack against civilians, etc.) (Orr, 2023).

Indeed, in its resolution ES-11/5 of November 2022, the UN General Assembly recognized the need for Russia to "be held accountable for its violations of international law in Ukraine" and recommended the creation of an international mechanism to register the damage caused, laying the groundwork for reparation claims (Zhabchyk, 2025). This includes damage resulting from any unlawful means used, whether a missile, a drone or a computer virus. The resolution in question affirms the obligation to repair the harm from all wrongful acts, implying that, for instance, Ukrainian victims of a blackout caused by a cyberattack could in theory claim compensation from Russia in a future mechanism (Futerinska-Orzhynska, 2024).

However, bringing individuals to justice faces particular challenges when advanced technologies are involved. The aforementioned difficulty of attribution in cyber operations can hinder the identification of the perpetrator. It is well known that Russia often masks its cyberattacks through proxy groups; proving the chain of command up to higher levels can be difficult using digital evidence (Tsagourias & Farrell, 2020; Kolodii, 2024). Another challenge is the lack of specific regulations: as long as no treaty clearly classifies certain uses of AI or robotics as unlawful per se, prosecutors must fit them into existing criminal categories. For example, could a prosecutor charge someone with "use of prohibited means of warfare" for employing an autonomous weapon? Although there is no treaty banning autonomous weapons (unlike, say, chemical weapons), it might be argued that if a weapon is indiscriminate by nature, its use violates customary law and thus constitutes a crime (Boutin, 2023; Gaeta, 2024; Ojha, 2025). This is novel ground that will likely be tested in coming years.

Another layer of accountability is State responsibility. Ukraine has brought legal actions against Russia in international forums (ICJ, European Court of Human Rights) over its aggression and its attacks. While these actions do not address technology per se, they do seek a ruling on overall State responsibility (Milanovic & Shah, 2023; Suarez Ortiz et al., 2023). Additionally, the UN Human Rights Council established a Commission of Inquiry that has documented patterns of violations; its reports mention, for instance, the use of explosive weapons in populated areas and indiscriminate attacks (categories in which kamikaze drones against cities would fit) (Głogowska-Balcerzak, 2024; Ilić & Ilić-Kosanović, 2023). These records will serve to publicly attribute responsibility and exert pressure for justice (Qiao, 2024).

In the realm of preventive governance, as already discussed, the international community is in the process of developing new norms and frameworks; in particular, negotiating a treaty on autonomous weapons is emerging as a crucial step to fill the existing regulatory gap (De Stercke, 2022; Jackson, 2023). Broad support in the UN General Assembly to begin negotiations (with Russia's notable opposition) indicates that most States see the need to impose international limits on these technologies (Nadibaidze, 2022). Likewise, driven by the European Parliament, the European Union has adopted a principled stance in favor of banning lethal autonomous systems without human control, and is integrating that perspective into its defense

policies (Filipović, 2023).

Although the future convention will take years to materialize, experts suggest it could be modeled on the already mentioned "two-tier" approach: banning particularly dangerous categories (e.g., unpredictable autonomous weapons or those designed to target humans) and strictly regulating the rest (e.g., requiring constant human supervision or limiting their use to environments where there are no civilians). It is worth noting that, even before a treaty, some countries have adopted political commitments: for example, 30 States (Latin America as a bloc, along with some European and African countries) have signed joint statements calling for a ban on "killer robots." The civil society campaign itself has gradually created a stigma around these weapons, comparable to the stigma that preceded the bans on anti-personnel mines and cluster munitions (Rosert & Sauer, 2019).

As for the governance of cyber warfare, this remains one of the slipperiest areas of international law. There is still no specific treaty regulating cyberattacks in armed conflict, partly because major powers, including Russia, are reluctant to limit their offensive capabilities in this domain (Pandey, 2025). Nonetheless, UN forums have at least managed to agree that International Humanitarian Law (IHL) applies to cyberspace and have recommended responsible behavior among States (Bogdan, 2024).

A relevant proposal has been the idea of a "Digital Geneva Convention," initially promoted by Microsoft and later taken up in academia, which seeks to protect civilian users from State-sponsored digital aggression (Casey-Maslen & Mwale, 2021; Kumar & Niranjan, 2025). Although non-binding, such ethical calls help generate normative and reputational pressure on States to moderate their actions.

In practice, after Russian cyberattacks against Ukrainian infrastructure, several States and multilateral bodies, including NATO, warned that a devastating cyberattack could be considered an unlawful use of force or even an armed attack, which would open the door to collective defense under Article 5 of the North Atlantic Treaty (Radu, 2023). This possibility acts as a deterrent, reinforcing a form of governance through classic deterrence adapted to cyberspace.

An innovative component of technological governance in conflicts is the role of private companies and corporate self-regulation. For example, after becoming indirectly involved in the war when its drones were used for military purposes, DJI implemented no-fly zones in Ukraine and suspended sales to both sides to prevent their military use, setting a precedent for corporate ethical responsibility (Kajander, 2023; Bender & Staggs, 2023). Although these measures had limited effectiveness, they represent progress toward applied ethics by private actors in war scenarios.

On the social media side, platforms such as Meta and Twitter were forced to adjust their policies to combat Russian disinformation and influence operations, indirectly cooperating with Ukrainian cyber defense efforts (Schroeder et al., 2025). This type of intervention illustrates how multi-stakeholder governance, in which States, international organizations and tech companies collaborate, is essential to address the ethical and security challenges of modern technology. Tech ethics experts also suggest developing "guardrails" or algorithmic safety barriers built directly into systems: for example, target-verification algorithms or automatic locks when there is a risk of harm to civilians (Lexman & Krishna, 2025). This technical and ethical approach aims to minimize collateral damage and strengthen the accountability of autonomous systems, aligning innovation with humanitarian principles.

From the standpoint of International Humanitarian Law, existing mechanisms to ensure compliance—such as Protecting Powers, ex officio investigations, or sanctions for grave breaches—need to adapt to new technological realities; the ICRC has urged an expanded discussion on how to monitor respect for IHL in the digital domain (Giovannelli, 2024). Some proposals include creating a UN body to monitor cyberattacks against civilian infrastructure, issuing real-time alerts and publicly naming those responsible—a sort of virtual equivalent of conventions protecting cultural or medical property, but for computer systems (Jiang, 2019). Another idea is to foster bilateral agreements during war, just as humanitarian ceasefires are agreed to, in order to exclude certain systems (for example, not interfering with hospitals via cyberattacks or not using drones in populated areas) (Biggio, 2025).

The war in Ukraine has also revived discussion of political responsibility. Russia has faced diplomatic isolation precisely because of the condemnation of its methods of warfare (Eichensehr et al., 2022). Its suspension from the UN Human Rights Council in 2022, decided by the General Assembly due to systematic violations, is an example of political sanction for breaching international norms, sending the message that atrocities entail loss of international prestige and privileges (Fonju, 2022).

Additionally, economic sanctions regimes have been widely used: the European Union and the United States have sanctioned companies and individuals linked to providing technological components, chips, Iranian drones and other items used to sustain Russia's war machine and its violations of IHL (Hofer, 2023). These sanctions seek to limit Russia's access to advanced technology and, at the same time, punish technical assistance to the Kremlin's abuses, consolidating a new regime of international political and economic responsibility.

Current mechanisms of accountability and governance regarding the use of AI, cyber systems and autonomous weapons in armed conflicts are evolving rapidly, driven largely by the lessons of the Russia–Ukraine war (Sotoudehfar & Sarkin, 2023). Although significant gaps remain—such as the absence of a specific treaty on autonomous weapons or the difficulty of legally classifying certain cyberattacks—the direction is clear: the international community recognizes the problem and is taking initial steps (Bode et al., 2023).

The effectiveness of these measures will depend on the political will of States, especially major technological powers, to yield in favor of our shared humanity (Ojha, 2025). As the ICRC noted in 2025, "without limits, the rise of autonomous weapons risks crossing lines that humanity has agreed must not be crossed" (ICRC, 2024). Ensuring that law and ethics evolve in step with military technology is perhaps one of the greatest challenges for International Humanitarian Law in the twenty-first century (Onderco, 2025; Maathuis, 2024). The case of Ukraine warns us of the dangers, but also offers crucial lessons for strengthening the humanitarian-legal framework before the next generation of smart weapons once again tests the limits of our conscience and our norms.

3. Conclusions

The Russia–Ukraine conflict constitutes the first real and systematic laboratory for the large-scale deployment of autonomous drones, semiautonomous systems, and loitering munitions, revealing both their transformative capacity and their high humanitarian risk. Documented cases, such as Russia's use of Shahed-136 drones against the power grid in the middle of winter, show that these systems, even without full lethal autonomy, can produce devastating strategic effects and strike essential civilian objects, exceeding the capacity of International Humanitarian Law (IHL) to contain their impacts. This situation highlights a significant regulatory gap, since navigational autonomy and pre-programmed routes enable wide-spectrum attacks without direct human control.

The conflict demonstrates that cyber operations have become a domain of warfare with effects comparable to kinetic force, where malware, digital sabotage and satellite interference can paralyze critical services. The hacking of the Viasat satellite network, wiper attacks on Ukrainian ministries, and the attempted sabotage of the power grid via Industroyer2 confirm that cyberattacks can deprive millions of civilians of water, electricity, or communications, amounting to direct violations of the IHL principle of distinction. The difficulty of isolating military effects without impacting civilian infrastructure shows that proportionality is almost impossible to guarantee in cyber warfare.

The integration of technology companies into digital defense and the provision of critical infrastructure makes the private sector a decisive actor in the conflict, with legal implications that remain unresolved. Ukraine's defense depended to a large extent on the technical support of companies such as Microsoft, ESET, and Starlink; at the same time, commercial technologies such as DJI drones were used as improvised weapons. This ambivalent participation reveals the urgent need to clarify the shared legal responsibility of

private actors in war scenarios, since their products and operational decisions directly influence the conduct of the conflict.

The information war and the use of AI for facial recognition introduced new forms of psychological pressure and social manipulation, expanding the war beyond the battlefield. Ukraine's use of Clearview AI to identify Russian corpses and notify their families raises profound ethical implications regarding digital privacy, the dignity of the dead, and the limits of using biometric data in wartime. At the same time, Russia's disinformation machinery, operated through bots, algorithms and false narratives, showed how the cognitive dimension of the conflict can alter global perceptions and hinder the verification of atrocities, putting international accountability mechanisms to the test.

The conflict highlights the emergence of new arenas of confrontation—autonomous maritime, outer space, and the cognitive domain—for which IHL does not yet have robust guidelines, as illustrated by the use of naval kamikaze drones, interference with civilian satellites, and growing risks of the militarization of outer space. These scenarios extend the geography of the conflict beyond traditional combat zones and introduce widespread vulnerabilities for civilian populations and globally interconnected infrastructure. The absence of specific regulation makes it necessary to reinterpret classic IHL rules in domains where the line between civilian and military objects is extremely thin.

The case shows that digitalized warfare tends to blur the line between civilians and combatants, especially with the participation of volunteer hacktivists in offensive cyberattacks. Ukraine's "IT Army," composed in part of international civilians, demonstrates that distributed cyber operations can turn thousands of individuals into direct participants in hostilities without a clear understanding of the legal consequences, eroding traditional IHL protections. This challenge requires updating the criteria for direct participation in hostilities to include hybrid and decentralized dynamics.

The accelerated proliferation of autonomous technologies during the war has generated a global multiplier effect, driving the development of autonomous weapons programs in several States. Diplomats and experts describe this phenomenon as an "Oppenheimer moment," indicating that the precedent set by Ukraine may trigger a military technological race without adequate international regulation. The empirical experience shows that the absence of prior regulatory frameworks leads to the unrestricted adoption of increasingly autonomous systems, with a disruptive potential comparable to that of historical strategic weapons.

This article is developed within the framework of the doctoral research project entitled: The Impact of the 4.0 Revolution on International Law and the Regulation of Arms: Technological Advances, Autonomous Weapons, Artificial Intelligence and Cyberwarfare (2016-2024) as part of the academic requirements of the Doctorate in Law of the Free University of Colombia.

4. References

1. Ahmad, I., Ahmad, L., Irshad, N., & Talha, M. (2025). Artificial Intelligence in Autonomous Weapon Systems: Legal Accountability and Ethical Challenges. *Journal of Engineering, Science and Technological Trends*, *2*(1). https://doi.org/10.48112/jestt.v2i1.9
2. Ahmed, S., et al. (2024). *Deepfakes and the crisis of knowing: Public perceptions and vulnerability to synthetic media*. UNESCO. https://www.unesco.org/en/articles/deepfakes-and-crisis-knowing
3. Akhtar, A. (2025). The Role of AI in U.S. and Russian Military Operations and Its Implications on Ukraine's Cyber and National Security. *Journal of Regional Studies Review*, *4*(1), 516-525. https://doi.org/10.62843/jrsr/2025.4a097
4. Al-Billeh, T., Al-Mudanat, J., Almamari, A., Khashashneh, T., & Al-Hailat, O. (2025). The International Framework for Cyber-Attacks Under the Rules of International Humanitarian Law. Journal of Human Rights, Culture and Legal System, 5(2), 412-441. https://doi.org/10.53955/jhcls.v5i2.534

5. AL-Hawamleh, A. M. (2023). Predictions of Cybersecurity Experts on Future Cyber-Attacks and Related Cybersecurity Measures. *International Journal of Advanced Computer Science and Applications (IJACSA)*, *14*(2). https://doi.org/10.14569/IJACSA.2023.0140292

6. Alanazi, S., Asif, S., Caird-daley, A., & Moulitsas, I. (2025). Unmasking deepfakes: A multidisciplinary examination of social impacts and regulatory responses. *Human-Intelligent Systems Integration*. https://doi.org/10.1007/s42454-025-00060-4

7. Allen, D. (2022). *Deepfake fight: AI-powered disinformation and perfidy under the Geneva Conventions*. *Notre Dame Journal on Emerging Technologies*. https://doi.org/10.2139/ssrn.3958426

8. American Society of International Law. (2025). *Lethal Autonomous Weapons Systems & International Law: Growing Momentum Towards a New International Treaty | ASIL*. https://www.asil.org/insights/volume/29/issue/1

9. Aponte García, C. A., Martínez Barrios, H. E., Romero-Sánchez, A., Aponte García, M. S., & García Valdés, M. del P. (2025a). Governance and regulation of autonomous weapons and cybersecurity (2016–2024): The influence of states, international organizations, and civil society on international humanitarian law. Contemporary Readings in Law and Social Justice. https://doi.org/10.52783/crlsj.537

10. Aponte García, M. S., Arévalo-Robles, G. A., & Romero-Sánchez, A. (2025). Evolution of the Industrial Revolutions and International Law: From mechanization to the regulatory challenges of the 4.0 Revolution. *Contemporary Readings in Law and Social Justice, 17*(1), 904–932. https://doi.org/10.52783/crlsj.612

11. Aponte García, M. S., Romero-Sánchez, A., Aponte García, C. A., Urriago Fontal, J. C., & García Valdés, M. del P. (2025b). The impact of Revolution 4.0 on international law and arms regulation (2016–2024). Review of Contemporary Philosophy. https://doi.org/10.52783/rcp.1150

12. Aponte, M. S., Aponte, C. A., & Romero, A. (2020). Derecho internacional público, justicia global y modelos transicionales. En M. Aponte (Comp.), *Derechos humanos, conflicto armado y construcción de paz* (pp. 12-50). Uceva. https://repositorio.uceva.edu.co/bitstream/handle/20.500.12993/1942/Derechos-humanos-conflicto-construccion-paz. pdf?sequence=1&isAllowed=y

13. Aponte, M. S., Aponte, C. A., & Romero, A. (2020). La reparación de las víctimas en el modelo de justicia transicional colombiano. En M. Aponte (Comp.), *Derechos humanos, conflicto armado y construcción de paz* (pp. 51-72). Uceva. https://repositorio.uceva.edu.co/bitstream/handle/20.500.12993/1942/Derechos-humanos-conflicto-construccion-paz. pdf?sequence=1&isAllowed=y

14. Aponte, M., & Sanchez, S. (2024). Globalization, human rights and Colombian armed conflict. Migration Letters, 21(S5), 1237–1251.https://doi.org/10.59670/ml.v21iS6.8109

15. Asaro, P. (2012). On banning autonomous weapon systems: Human rights, automation, and the dehumanization of lethal decision-making. *International Review of the Red Cross, 94*(886), 687–709. https://international-review.icrc.org/sites/default/files/irrc-886-asaro.pdf

16. Aslam, H. A. (2025). AI Driven Cyber Warfare Between China and India and Its Impact on Pakistan's National Security. *Journal of Regional Studies Review*, *4*(1), 424-432. https://doi.org/10.62843/jrsr/2025.4a089

17. Bace, B., Gökce, Y., & Tatar, U. (2024). Law in orbit: International legal perspectives on cyberattacks targeting space systems. *Telecommunications Policy*, *48*(4), 102739. https://doi.org/10.1016/j.telpol.2024.102739

18. Bächle, T. C., & Bareis, J. (2022). "Autonomous weapons" as a geopolitical signifier in a national

power play: Analysing AI imaginaries in Chinese and US military policies. *European Journal of Futures Research*, *10*(1), 20. https://doi.org/10.1186/s40309-022-00202-w

19. Bender, C., & Staggs, J. (2023). Leveling the Playing Field: Equipping Ukrainian Freedom Fighters with Low-Cost Drone Detection Capabilities. 2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon), 287-312. https://doi.org/10.23919/CyCon58705.2023.10181421

20. Bergengruen, V. (2023, 14 de noviembre). *Ukraine's "secret weapon" against Russia is Clearview AI*. *Time*. https://time.com/6334176/ukraine-clearview-ai-russia/

21. Bhila, I. (2024). Putting algorithmic bias on top of the agenda in the discussions on autonomous weapons systems. *Digital War*, *5*(3), 201-212. https://doi.org/10.1057/s42984-024-00094-z

22. Bhuiyan, J. (2022, 24 de marzo). *Ukraine uses facial recognition software to identify Russian soldiers killed in combat*. *The Guardian*. https://www.theguardian.com/technology/2022/mar/24/ukraine-facial-recognition-identify-russian-soldiers

23. Biggio, G. (2025). Regulating non-kinetic effects of cyber operations: The 'Loss of Functionality' approach and the military necessity-humanity balance under International Humanitarian Law. *Journal of Conflict and Security Law*, *30*(2), 241-263. https://doi.org/10.1093/jcsl/kraf008

24. Bode, I., Huelss, H., Nadibaidze, A., Qiao-Franco, G., & Watts, T. F. A. (2023). Prospects for the global governance of autonomous weapons: Comparing Chinese, Russian, and US practices. *Ethics and Information Technology*, *25*(1), 5. https://doi.org/10.1007/s10676-023-09678-x

25. Borsari, F., & Davis, G. B. (2023). *An urgent matter of drones: Lessons for NATO from Ukraine*. Center for European Policy Analysis (CEPA).

26. Boşneagu, R. (2024). Russia-Ukraine War of Drones – Strategic Impact, Tactics, and Implications. The Drones Dropped in Romania during the Russia-Ukraine War. *Romanian Military Thinking*, *2024*(4), 504-521. https://doi.org/10.55535/RMT.2024.4.33

27. Bouks, B. (2023). *The Iranian Involvement in the War in Ukraine and its Implication on Broader Arenas as the Middle-East—The Test Case of Unmanned Drones
(Volume 24, No. 3, 2023.)*. https://doi.org/10.37458/nstf.24.3.7

28. Boutin, B. (2023). State responsibility in relation to military applications of artificial intelligence. Leiden Journal of International Law, 36(1), 133-150. https://doi.org/10.1017/S0922156522000607

29. Bratu, I., & Freeland, S. (2026). Winner takes all? Legal implications of autonomous weapons systems and the militarization of outer space. *Acta Astronautica*, *238*, 803-814. https://doi.org/10.1016/j.actaastro.2025.09.031

30. Brizard, L. (2025, 15 de abril). Russian FPV drones have killed 121 civilians in Kherson since beginning of war, prosecutor reports. *UNITED24 Media*. https://united24media.com/latest-news/russian-fpv-drones-have-killed-121-civilians-in-kherson-since-beginning-of-war-prosecutor-reports-7618

31. Brusylovska, O., & Maksymenko, I. (2023). Analysis of the media discourse on the 2022 war in Ukraine: The case of Russia. *Regional Science Policy & Practice, 15*(1), 222–236. https://doi.org/10.1111/rsp3.12579

32. Burgess, M. (2022, 27 de febrero). *Ukraine's volunteer "IT Army" is hacking in uncharted territory*. *WIRED*. https://www.wired.com/story/ukraine-it-army-russia-war-cyberattacks-ddos/

33. Bwana, R. (2023). Kicking Man Out of the Loop: The Case of Loitering Munitions and Implications

for International Humanitarian Law. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4383978

34. Byczyński, M. (2024). The legal status of "civilian hackers" under international humanitarian law. *Acta Universitatis Lodziensis. Folia Iuridica*. https://czasopisma.uni.lodz.pl/Iuridica/

35. Canadian Centre for Cyber Security. (2022, 14 de julio). *Cyber threat activity related to the Russian invasion of Ukraine*. Government of Canada. https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-threat-activity-related-russian-invasion-ukraine

36. Casey-Maslen, S. (2025). Autonomous Weapons Systems Under International Law. En K. Talves & D. Spreen (Eds.), *Artificial Intelligence in Military Technology: Sociological, cultural and ethical perspectives* (pp. 161-179). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-95578-5_10

37. Chlevickaitė, G. (2025). Documenting conflict-related crimes in Ukraine. *Journal of International Criminal Justice*. https://doi.org/10.1093/jicj/mqaf020

38. Chomanski, B. (2023). A Moral Bind? — Autonomous Weapons, Moral Responsibility, and Institutional Reality. *Philosophy & Technology*, *36*(2), 41. https://doi.org/10.1007/s13347-023-00647-2

39. Clark, B. (2024). Sea Drones in the Russia-Ukraine War Inspire New Tactics: Military Strategists See a Possible Means of Defending Taiwan. IEEE Spectrum, 61(10), 28-33. https://doi.org/10.1109/MSPEC.2024.10705385

40. Comisión Internacional Independiente de Investigación sobre Ucrania. (2025, 28 de mayo). *UN Commission concludes that Russian armed forces' drone attacks (…) amount to crimes against humanity*. Oficina del ACNUDH. https://www.ohchr.org/en/press-releases/2025/05/un-commission-concludes-russian-armed-forces-drone-attacks-against-civilians

41. Comité Internacional de la Cruz Roja (CICR). (2020). International humanitarian law and cyber operations during armed conflicts: ICRC position paper submitted to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, November 2019. *International Review of the Red Cross*, *102*(913), 481-492. https://doi.org/10.1017/S1816383120000478

42. Comité Internacional de la Cruz Roja (CICR). (2024a, marzo 19). *Las ciberoperaciones durante los conflictos armados | COMITÉ INTERNACIONAL DE LA CRUZ ROJA*. https://www.icrc.org/es/derecho-y-politicas/las-ciberoperaciones-durante-los-conflictos-armados

43. Comité Internacional de la Cruz Roja (CICR). (2025, septiembre 8). *ICRC president: «IHL only as strong as leaders' will to uphold it» | ICRC*. https://www.icrc.org/es/declaracion/presidenta-cicr-fortaleza-derecho-internacional-humanitario-depende-voluntad-lideres-respetarlo

44. Comité Internacional de la Cruz Roja y la Media Luna Roja. (2024). *Armas y derecho internacional humanitario*. https://rcrcconference.org/app/uploads/2024/04/CoD24-Background-doc-Weapons-and-IHL-ES.pdf

45. Cools, K., & Maathuis, C. (2024). Trust or Bust: Ensuring Trustworthiness in Autonomous Weapon Systems. *MILCOM 2024 - 2024 IEEE Military Communications Conference (MILCOM)*, 182-189. https://doi.org/10.1109/MILCOM61039.2024.10773908

46. Copeland, D., Liivoja, R., & Sanders, L. (2023b). The Utility of Weapons Reviews in Addressing Concerns Raised by Autonomous Weapon Systems. *Journal of Conflict and Security Law*, *28*(2), 285-316. https://doi.org/10.1093/jcsl/krac035

47. Council of the European Union. (2022, 10 de mayo). *Russian cyber operations against Ukraine: Declaration by the High Representative…*. https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/

48. Davison, N. (2017). *Autonomous weapon systems under international humanitarian law*. ICRC. https://www.icrc.org/sites/default/files/document/file_list/autonomous_weapon_systems_under_international_humanitarian_law.pdf

49. de Deus Pereira, J. (2025, 19 septiembre). *From drones to data: Private contractors and cyber mercenaries*. Royal United Services Institute. https://www.rusi.org/explore-our-research/publications/commentary/drones-data-private-contractors-and-cyber-mercenaries

50. De Stercke, C. (2022). To ban or not to ban. Analyzing the banning process of autonomous weapon systems. Journal of Science Policy & Governance, 21(01). https://doi.org/10.38126/JSPG210102

51. Docherty, B. (2018). Atender la llamada. *Human Rights Watch*. https://www.hrw.org/es/report/2018/08/21/atender-la-llamada/un-imperativo-moral-y-legal-prohibir-los-robots-asesinos

52. Eichensehr, K., Camia, E., Meyer, K., Pazhwak, M., Rutherford, A., & Wade, K. (2022). Russia Invades Ukraine. *American Journal of International Law*, 116, 593 - 604. https://doi.org/10.1017/ajil.2022.26.

53. Engelhardt, W., & Kessler, V. (2024). The ethical debate about the use of autonomous weapon systems from a theological perspective. *Verbum et Ecclesia*, *45*(1), 9. https://doi.org/10.4102/ve.v45i1.3176

54. ENISA — European Union Agency for Cybersecurity. (2023). *ENISA Threat Landscape 2023: Russia–Ukraine cyber operations*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

55. Ferl, A.-K. (2024). Imagining Meaningful Human Control: Autonomous Weapons and the (De-) Legitimisation of Future Warfare. *Global Society*, *38*(1), 139-155. https://doi.org/10.1080/13600826.2023.2233004

56. Figueroa, M. D., Orozco, A. H., Martínez, J., & Jaime, W. M. (2023). The risks of autonomous weapons: An analysis centred on the rights of persons with disabilities. *International Review of the Red Cross*, *105*(922), 278-305. https://doi.org/10.1017/S1816383122000881

57. Filipović, A. (2023). Lethal Autonomous Weapon Systems (LAWS): Towards global regulation or indiscriminate employment? Politička Revija, 75(1), 211-232. https://doi.org/10.5937/polrev75-43187

58. Fonju, Dr. N. K. (2022). The Roots of Russian Naked Aggression (RRNA) Versus Unjust Shortsighted Support to Ukrainian Secessionists (USSUS): Constituent Tools of Re-Emerging to the Position of New International Hyper Hegemonic Power (NIHHP) in the Unipolar World of 1991-2022. South Asian Research Journal of Humanities and Social Sciences, 4(4), 269-290. https://doi.org/10.36346/sarjhss.2022.v04i04.009

59. Freedberg, S. J. Jr. (2024, febrero 20). *The revolution that wasn't: How AI drones have fizzled in Ukraine (so far)*. *Breaking Defense*. https://breakingdefense.com/2024/02/the-revolution-that-wasnt-how-ai-drones-have-fizzled-in-ukraine-so-far/

60. Gaeta, P. (2024). Who Acts When Autonomous Weapons Strike? Journal of International Criminal Justice, 21(5), 1033-1055. https://doi.org/10.1093/jicj/mqae001

61. Gianinni, T. (2023). Global cultural conflict and digital identity. *Heritage, 6*(2), 107. https://www.mdpi.com/2571-9408/6/2/107

62. Gilbert, C., & Gilbert, M. A. (2024). Leveraging Artificial Intelligence (AI) by a Strategic Defense against Deepfakes and Digital Misinformation. *International Journal of Scientific Research and Modern Technology*, *3*(11), 62-78. https://doi.org/10.38124/ijsrmt.v3i11.76

63. Giovannelli, D. (2025). Handling cyberspace's state of intermediacy through existing international law. International Review of the Red Cross, 107(928), 96-139. https://doi.org/10.1017/S1816383124000390

64. Gisel, L., Rodenhäuser, T., & Dörmann, K. (2020). Twenty years on: IHL and protection of civilians from cyber operations. *International Review of the Red Cross, 102*(913), 1119–1160.

65. Greenberg, A. (2018). *The untold story of NotPetya*. WIRED. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

66. Greenberg, A. (2022, 12 abril). Russia's Sandworm hackers attempted a third blackout in Ukraine. *WIRED*. https://www.wired.com/story/sandworm-russia-ukraine-blackout-gru/

67. Gunawan, Y., Aulawi, M. H., Anggriawan, R., & Putro, T. A. (2022). Command responsibility of autonomous weapons under international humanitarian law. *Cogent Social Sciences*, *8*(1), 2139906. https://doi.org/10.1080/23311886.2022.2139906

68. Guo, J. (2025). The ethical legitimacy of autonomous Weapons systems: Reconfiguring war accountability in the age of artificial Intelligence. *Ethics & Global Politics*, *18*(3), 27-39. https://doi.org/10.1080/16544951.2025.2540131

69. Hamad, B. (2025). The Impact of Digital Technology on International Humanitarian Law: Ethical and Legal Implications of Autonomous Weapons Systems. *European Journal of Law and Political Science*, *4*(4), 1-14. https://doi.org/10.24018/ejpolitics.2025.4.4.182

70. Hofer, A. (2023). The EU's 'Massive and Targeted' Sanctions in Response to Russian Aggression, a Contradiction in Terms. Cambridge Yearbook of European Legal Studies, 25, 19-39. https://doi.org/10.1017/cel.2023.9

71. Human Rights Watch. (2024, diciembre 5). *Robots asesinos: La votación de la ONU debería impulsar las negociaciones del tratado | Human Rights Watch*. https://www.hrw.org/news/2024/12/05/killer-robots-un-vote-should-spur-treaty-negotiations

72. Human Rights Watch. (2025, 3 de junio). *Ucrania: Rusia utiliza drones para atacar la población civil*. Human Rights Watch. https://www.hrw.org/es/news/2025/06/03/ucrania-rusia-utiliza-drones-para-atacar-la-poblacion-civil

73. Human Rights Watch. (2025, junio 3). *Ucrania: Rusia utiliza drones para atacar a la población civil | Human Rights Watch*. https://www.hrw.org/es/news/2025/06/03/ucrania-rusia-utiliza-drones-para-atacar-la-poblacion-civil

74. Human Rights Watch. (2025). *Hunted from above: Russia's use of drones to attack civilians in Kherson, Ukraine*. https://www.hrw.org/report/2025/06/03/hunted-from-above/russias-use-of-drones-to-attack-civilians-in-kherson-ukraine

75. International Committee of the Red Cross (ICRC). (2019). *International humanitarian law and cyber operations during armed conflicts*.

76. International Committee of the Red Cross (ICRC). (2020). *International humanitarian law and cyber operations during armed conflicts* (Position paper). https://www.icrc.org/sites/default/files/document/file_list/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf

77. International Committee of the Red Cross (ICRC). (2023). *Cyber operations during armed conflict: The principle of distinction*. https://www.icrc.org/sites/default/files/wysiwyg/war-and-

law/03_distinction-0.pdf

78. International Committee of the Red Cross (ICRC). (2023). *International humanitarian law and the growing involvement of civilians in cyber operations…* https://reliefweb.int/report/world/international-humanitarian-law-and-growing-involvement-civilians-cyber-operations-and-other-digital-activities-during-armed-conflict

79. Iskoujina, Z., Gnatchenko, Y., & Bernal, P. (2024). *Social media as an information warfare tool in the Russia-Ukraine war*. Carnegie Mellon University.

80. Jackson, J. (2023). Mapping the Lethal Autonomous Weapons Debate: An Introduction. Ethics & International Affairs, 37(3), 254-260. https://doi.org/10.1017/S0892679423000345

81. Jančárková, T., et al. (2024). *Seeing through the fog: The impact of information operations on war crimes investigations in Ukraine*. UC Berkeley Human Rights Center.

82. Javed, M. N. (2025). Artificial Intelligence and Autonomous Weapons: Ethical and Political Dilemmas in Global Security. *IJFMR - International Journal For Multidisciplinary Research*, *7*(1). https://doi.org/10.36948/ijfmr.2025.v07i01.35182

83. Jiang, Z. (2019). Regulating the Use and Conduct of Cyber Operations through International Law: Challenges and Fact-finding Body Proposal. LSE Law Review, 5, 59-88. https://doi.org/10.61315/lselr.42

84. Johnson, J. (2020). Artificial Intelligence, Drone Swarming and Escalation Risks in Future Warfare. *The RUSI Journal*, *165*(2), 26-36. https://doi.org/10.1080/03071847.2020.1752026

85. Jones, G., Egan, J., & Rosenbach, E. (2023, 31 julio). *Advancing in adversity: Ukraine's battlefield technologies and lessons for the U.S.* Belfer Center, Harvard.

86. Kajander, A. (2023). Russian Invasion of Ukraine 2022: Time to Reconsider Small Drones? 2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon), 313-327. https://doi.org/10.23919/CyCon58705.2023.10181494

87. Kazić, T. (2025). Digital propaganda and disinformation generated via artificial intelligence:The Israel/ Palestine conflict and the fall of Bashar al-Assad in Syria case studies. *Politika nacionalne bezbednosti*, *28*(1), 101-122. https://doi.org/10.5937/pnb28-56408

88. Kerr, J. A. (2023). *Assessing Russian cyber and information warfare in Ukraine*. CNA. https://www.cna.org/reports/2023/11/Assessing-Russian-Cyber-and-Information-Warfare-in-Ukraine.pdf

89. Khalil, A., & Raj, S. A. K. (2024). Challenges to the Principle of Distinction in Cyber Warfare Navigating International Humanitarian Law Compliance: The Principle of Distinction in Cyber Warfare. *PRAWO i WIĘŹ*, *2*, 109-131. https://doi.org/10.36128/PRIW.VI49.769

90. Khoirunnisa, K., Matthew, B., Jubaidi, D., & Nugroho, A. Y. (2025). The Ukraine-Russia conflict: An international humanitarian law review of the involvement of foreign fighters. *Social Sciences & Humanities Open*, *11*, 101340. https://doi.org/10.1016/j.ssaho.2025.101340

91. Kirichenko, D. (2025, 27 mayo). *How AI is eroding the norms of war*. AI Frontiers.

92. Kolodii, R. (2024). Unpacking Russia's Cyber-Incident Response. Security Studies, 33(4), 640-669. https://doi.org/10.1080/09636412.2024.2391757

93. Kumar, S., Niranjan, M., Nagar, G., Peddoju, S. K., & Tripathi, K. (2025). Humanizing Cyber War: A Geneva Conventions-based Framework for Cyber Warfare. International Conference on Cyber Warfare and Security, 20(1), 179-187. https://doi.org/10.34190/iccws.20.1.3324

94. Kunertova, D. (2023a). Drones have boots: Learning from Russia's war in Ukraine. *Contemporary Security Policy*, *44*(4), 576-591. https://doi.org/10.1080/13523260.2023.2262792

95. Kunertova, D. (2023b). 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

96. Kunertova, D., & Herzog, S. (2024). Emerging and disruptive technologies… In P. Forsström (Ed.). Finnish National Defence University.

97. Kuźnicka-Błaszkowska, D. (2025). Emerging need to regulate deepfakes in international law. *Journal of Cybersecurity, 11*(1). https://doi.org/10.1093/cybsec/tyaf008

98. Lexman, R. R., Krishna, A., & Sam, M. P. (2025). AI guardrails in business and education: Bridging minds and markets. Development and Learning in Organizations: An International Journal. https://doi.org/10.1108/DLO-01-2025-0001

99. Li, J. (2025). The Responsibility Gap in Militarized Application of AI and the Construction of Global Accountability Mechanism. *Lecture Notes in Education Psychology and Public Media*, *88*(1), 122-127. https://doi.org/10.54254/2753-7048/2025.22438

100. Llano Franco. (2025). CONSTITUTIONS AND CITIZENS: EXCLUSION AND INCORPORATION IN 19TH-CENTURY LATIN AMERICA. *International Journal of Applied Mathematics*, *38*(6s), 1350-1366. https://doi.org/10.12732/ijam.v38i6s.661

101. Madziwa, Z. (2024). Advancing honour and dignity in death… *International Review of the Red Cross, 106*(926), 760–794.

102. Maphosa, V. (2024). The Rise of Artificial Intelligence and Emerging Ethical and Social Concerns. *AI, Computer Science and Robotics Technology*. https://doi.org/10.5772/acrt.20240020

103. Marsili, M. (2024). Lethal Autonomous Weapon Systems: Ethical Dilemmas and Legal Compliance in the Era of Military Disruptive Technologies. *International Journal of Robotics and Automation Technology*, *11*, 63-68. https://doi.org/10.31875/2409-9694.2024.11.05

104. Martínez, H. E. (2025). Fundamentos filosóficos del conocimiento científico: gnoseología, epistemología, paradigmas y enfoques de investigación. En *Filosofia, essência e existência: questões fundamentais e reflexões filosóficas* (pp. 117–149). Atena Editora. https://doi.org/10.22533/AT.ED.7501125240310

105. Martínez Barrios, H. E., & Escobar Brochero, A. R. (2025). *Literature review in scientific research: Foundations, scope, and methodological guidelines for its preparation*. **International Journal of Applied Mathematics, 38**(10s), (pp 915 – 922). DOI: 10.12732/ijam.v38i10s.1005

106. Mewoh, G., & Rahmadan, Y. (2025). Russia's Use of Autonomous Weapon Systems: An Analysis of Offensive Military Policy in the 2022–2024 Russia-Ukraine War. *Politeia : Journal of Public Administration and Political Science and International Relations*, *3*(4), 237-252. https://doi.org/10.61978/politeia.v3i4.684

107. Microsoft. (2022). *Defending Ukraine: Early lessons from the cyber war*. Microsoft.

108. Milanovic, M., & Shah, S. (2023). Ukraine and the Netherlands v. Russia, Merits Amicus Curiae Brief Submitted on behalf of the Human Rights Law Centre of the University of Nottingham. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4427214

109. Minculete, G., & Păstae, V. (2023). Essential approaches to the use of combat drones. Specific elements of the armed conflict in Ukraine. *BULLETIN OF «CAROL I» NATIONAL DEFENCE UNIVERSITY*, *12*(4), 208-224. https://doi.org/10.53477/2284-9378-23-58

110. Mura, A. et al. (2024). *Analysis of the Cyber-Attack Against Viasat (February 2022)*. University of Bologna.

111. Naciones Unidas (Ed.). (2021). *Group of Governmental Experts on Advancing Responsible State*

Behaviour in Cyberspace in the Context of International Security: Note. UN. https://digitallibrary.un.org/record/3934214

112. Naciones Unidas. (2024, diciembre 10). *Principles relating to emerging technologies in the area of lethal autonomous weapons systems, including in the framework of the Convention on Certain Conventional Weapons. UN General Assembly*. United Nations. https://docs.un.org/es/a/res/79/62

113. Nadibaidze, A. (2022). Great power identity in Russia's position on autonomous weapons systems. Contemporary Security Policy, 43(3), 407-435. https://doi.org/10.1080/13523260.2022.2075665

114. Nazeer, M. (2024). Algorithmic Conscience: An In-Depth Inquiry into Ethical Dilemmas in Artificial Intelligence. *International Journal of Research and Innovation in Social Science*. https://doi.org/10.47772/IJRISS.2024.805052

115. Nazirah, N., Zaini, A., & Suseto, B. (2024). Implementation of Revolution in Military Affairs in the Russian and Ukrainian Wars. *Formosa Journal of Applied Sciences*, *3*(11), 4469-4480. https://doi.org/10.55927/fjas.v3i11.11889

116. New Strategy Center. (2025). *The impact of artificial intelligence in the drones' war in Ukraine*. https://newstrategycenter.ro/wp-content/uploads/2025/02/The-Impact-of-Artificial-Intelligence-in-the-Drones-War-in-Ukraine.pdf

117. Niyitunga, E. B. (2022). Armed drones and international humanitarian law. *Digital Policy Studies*, *1*(2), 18-39. https://doi.org/10.36615/dps.v1i2.2278

118. O'Connell, M. E. (2023). Banning Autonomous Weapons: A Legal and Ethical Mandate. *Ethics & International Affairs*, *37*(3), 287-298. https://doi.org/10.1017/S0892679423000357

119. Ojha, Y. (2025). Artificial Intelligence in Armed Conflict: Perspectives from International Humanitarian Law. *Unity Journal*, *6*(1), 34-47. https://doi.org/10.3126/unityj.v6i1.75547

120. Onderco, M. (2025). Navigating the AI frontier: Insights from the Ukraine conflict for NATO's governance role in military AI. Journal of Strategic Studies, 48(3), 602-626. https://doi.org/10.1080/01402390.2025.2463451

121. Organization for Security and Co-operation in Europe (OSCE). (2023). *The legal framework applicable to the armed conflict in Ukraine*. https://www.osce.org/files/f/documents/d/4/548614.pdf

122. Orr, Z. R. (2023). Redress for Unlawful Cyber-Attacks During Armed Conflict: The Limits of the International Criminal Court and How Human Rights Bodies Can Help Close the Gap. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4422358

123. Ortiz, I. A. (2024). Balcerzak, Michal and Julia Kapelańska-Pręgowska, eds. 2024. Artificial Intelligence and International Human Rights Law. Developing Standards for a Changing World. *Deusto Journal of Human Rights*, *14*, 377-384. https://doi.org/10.18543/djhr.3200

124. Pandey, A. (2025). Application of International Humanitarian Law in Changing Dimensions of Armed Conflict vis-à-vis Cyber Warfare. *Unity Journal*, *6*(1), 284-296. https://doi.org/10.3126/unityj.v6i1.75698

125. Pauwels, E. (2024). *Generative AI: A revolution for information warfare?* CIGI.

126. Perišić, P., & Tomljenović, M. (2024). Legal Permissibility of Autonomous Weapon Systems, with Specific Reference to the Principles of International Humanitarian Law. *Zbornik Radova Pravnog Fakulteta u Splitu*, *61*(4), 531-555. https://doi.org/10.31141/zrpfs.2024.61.154.531

127. Plakoudas, S., & Sofitis, V. (2023). Explaining the Bayraktar Paradox. *The RUSI Journal*, *168*(6), 42-52. https://doi.org/10.1080/03071847.2023.2285752

128. Podar, H., & Colijn, A. (2025). *Technical Risks of (Lethal) Autonomous Weapons Systems* (No. arXiv:2502.10174). arXiv. https://doi.org/10.48550/arXiv.2502.10174

129. Prasad, N., Diro, A., Warren, M., & Fernando, M. (2025). A survey of cyber threat attribution: Challenges, techniques, and future directions. *Computers & Security*, *157*, 104606. https://doi.org/10.1016/j.cose.2025.104606

130. Prysiazhniuk, M. (2025). Strategic narratives and information warfare. *Culture. Society. Economy. Politics, 5*(1), 88–108.

131. Qiao, Y. (2024). Assessing War Crimes Accountability Through Just War Theory: A Comparative Legal Analysis of the Russia-Ukraine Conflict. Lecture Notes in Education Psychology and Public Media, 70(1), 63-69. https://doi.org/10.54254/2753-7048/70/20241010

132. Radu, C.-C. (2023). The Russian-Ukrainian War and Its Impact on Cyber Security in NATO and the EU. Romanian Military Thinking, 2023(4), 38-53. https://doi.org/10.55535/RMT.2023.4.01

133. Reichberg, G. M., & Syse, H. (2021). Applying AI on the Battlefield: The Ethical Debates. En J. von Braun, M. S. Archer, G. M. Reichberg, & M. Sánchez Sorondo (Eds.), *Robotics, AI, and Humanity: Science, Ethics, and Policy* (pp. 147-159). Springer International Publishing. https://doi.org/10.1007/978-3-030-54173-6_12

134. Renic, N., & Christensen, J. G. (2024). *Drones, the Russo-Ukrainian war, and the future of armed conflict*. Djøf Publishing.

135. Renic, N., & Schwarz, E. (2023). Crimes of Dispassion: Autonomous Weapons and the Moral Challenge of Systematic Killing. *Ethics & International Affairs*, *37*(3), 321-343. https://doi.org/10.1017/S0892679423000291

136. Reuters. (2024, 22 febrero). *UK, learning lessons from Ukraine, to spend $5.7 billion on military drones*. Reuters.

137. Rickli, J-M., & Mantellassi, F. (2024). *The war in Ukraine: Reality check for emerging technologies…* Geneva Centre for Security Policy.

138. Rickli, J-M., & Mantellassi, F. (2024). *Ukraine's future vision for AI-enabled autonomous warfare*. CSIS.

139. Roković, V. (2024). The use of new technologies in urban warfare. *Urbana bezbednost i urbani razvoj, Zbornik radova sa treće naučne konferencije*, *Globalizacija, urbani razvij i transformacija gradova*, 271-281. https://doi.org/10.5937/UBUR24271R

140. Romero-Sánchez, A., & Aponte-García, M. S. (2024). The academic spin-off ecosystem: A comparative analysis between Colombia and global trends. Evolutionary Studies in Imaginative Culture, 1538–1563. https://doi.org/10.70082/esiculture.vi.2000

141. Romero-Sánchez, A., Perdomo-Charry, G., & Burbano-Vallejo, E. (2024a). Políticas, transferencia y financiamiento: Factores clave para spin-offs académicas: Revisión sistemática de literatura. Revista Venezolana De Gerencia, 29(Especial 1), 1330–1346. https://doi.org/10.52080/rvgluz.29.e12.27

142. Romero-Sánchez, A., Perdomo-Charry, G., & Burbano-Vallejo, E. L. (2025b). Factores determinantes en la creación de Spin-Off Académicas: Una perspectiva multiteórica. Revista De Ciencias Sociales, 31(1), 162–181. https://doi.org/10.31876/rcs.v31i1.43496

143. Rosenzweig, I., & Pacholska, M. (2025). The use of facial recognition for targeting under international law. *International Review of the Red Cross, 106*(928).

144. Rosert, E., & Sauer, F. (2019). Prohibiting Autonomous Weapons: Put Human Dignity First. Global Policy, 10(3), 370-375. https://doi.org/10.1111/1758-5899.12691

145. Schroeder, D. T., Cha, M., Baronchelli, A., Bostrom, N., Christakis, N. A., Garcia, D., Goldenberg, A., Kyrychenko, Y., Leyton-Brown, K., Lutz, N., Marcus, G., Menczer, F., Pennycook, G., Rand, D. G., Ressa, M., Schweitzer, F., Summerfield, C., Tang, A., Van Bavel, J. J., … Kunst, J. R. (2025). How Malicious AI Swarms Can Threaten Democracy: The Fusion of Agentic AI and LLMs Marks a New Frontier in Information Warfare (Versión 3). arXiv. https://doi.org/10.48550/ARXIV.2506.06299

146. Simmons-Edler, R., Badman, R., Longpre, S., & Rajan, K. (2024). *AI-Powered Autonomous Weapons Risk Geopolitical Instability and Threaten AI Research* (No. arXiv:2405.01859). arXiv. https://doi.org/10.48550/arXiv.2405.01859

147. Slusher, M. (2025). *Lessons from the Ukraine conflict: Modern warfare in the age of autonomy…* CSIS.

148. Smith, B. (2022, 22 junio). *Defending Ukraine: Early lessons from the cyber war*. Microsoft.

149. Soesanto, S. (2022). *The IT Army of Ukraine* (CSS Cyberdefense Report No. 6). ETH Zürich.

150. Sohail, H. (2022). Líneas de falla en la aplicación del derecho internacional humanitario a la ciberguerra tarifa. *Revista de Informática Forense, Digital Seguridad y Derecho*. https://doi.org/10.15394/jdfsl.2022.1761

151. Solovyeva, A., & Hynek, N. (2023). When stigmatization does not work: Over-securitization in efforts of the Campaign to Stop Killer Robots. *AI & SOCIETY*, *38*(6), 2547-2569. https://doi.org/10.1007/s00146-022-01613-w

152. Sotoudehfar, S., & Sarkin, J. J. (2023). Drones on the Frontline: Charting the Use of Drones in the Russo-Ukrainian Conflict and How Their Use May Be Violating International Humanitarian Law. International and Comparative Law Review, 23(2), 129-169. https://doi.org/10.2478/iclr-2023-0018

153. Spansvoll, R. (2024). The Weaponisation of Social Media, Crowdfunding and Drones: Una guerra popular en la era digital. *The RUSI Journal*, *169*(1-2), 46-60. https://doi.org/10.1080/03071847.2024.2350478

154. Suarez Ortiz, S., Henríquez Torres, I., & Angulo Medina, R. (2023). The Russia-Ukraine conflict: Analysis of the international responsibility of the States, the principles of non-intervention, and prohibited use of force under the International Court of Justice jurisprudence. Revista Ruptura. https://doi.org/10.26807/rr.v4i4.111

155. Tsagourias, N., & Farrell, M. (2020). Cyber Attribution: Technical and Legal Approaches and Challenges. European Journal of International Law, 31(3), 941-967. https://doi.org/10.1093/ejil/chaa057

156. Tsybulenko, E., & Kajander, A. (2022). Customary International Humanitarian Law and Article 36 of Additional Protocol I to the Geneva Conventions: A Stopgap Regulator of Autonomous Weapons Systems? *TalTech Journal of European Studies*, *12*(2), 87-112. https://doi.org/10.2478/bjes-2022-0013

157. U.S. Department of Justice. (2020). *Six Russian GRU officers charged in connection with worldwide deployment of destructive malware*. https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

158. UNESCO & UNOSAT. (2023). *UNESCO and UNOSAT join forces to safeguard Ukraine's cultural heritage*.

159. UNESCO. (2024, 30 octubre). *UNESCO assesses damage to cultural heritage after attack in Lviv*. https://www.unesco.org/en/articles/unesco-assesses-damage-cultural-heritage-after-attack-ukrainian-city-lviv

160. UNESCO. (2025, 27 octubre). *Deepfakes and the crisis of knowing*. https://www.unesco.org/en/articles/deepfakes-and-crisis-knowing

161. Verdiesen, I., Santoni de Sio, F., & Dignum, V. (2021). Accountability and Control Over Autonomous Weapon Systems: A Framework for Comprehensive Human Oversight. *Minds and Machines*, *31*(1), 137-163. https://doi.org/10.1007/s11023-020-09532-9

162. Victoria Ochoa, D., Aponte García, C., García Valdés, M., Aponte García, M., Romero Sánchez, A. (2023). Normative Statements and Correction Claim in the Logical Comprehension Domain. Migration Letters. 20, S9 (Nov. 2023), 653–666. DOI: https://doi.org/10.59670/ml.v20iS9.4835

163. Winter, E. (2021). The Accountability of Software Developers for War Crimes Involving Autonomous Weapons: The Role of the Joint Criminal Enterprise Doctrine. *University of Pittsburgh Law Review*, *83*(1). https://doi.org/10.5195/lawreview.2021.822

164. Winter, E. (2022). The Compatibility of Autonomous Weapons with the Principles of International Humanitarian Law. *Journal of Conflict and Security Law*, *27*(1), 1-20. https://doi.org/10.1093/jcsl/krac001

165. Wood, N. (2022). Autonomous Weapons Systems and Force Short of War. *Journal of Ethics and Emerging Technologies*, *32*(2), 1-16. https://doi.org/10.55613/jeet.v32i2.115

166. Zhabchyk, D., Hedz, V., & Bondarenko, Y. (2025). New challenges for international criminal law: How to incorporate cybercrimes committed during armed conflicts into the existing legal framework. Visegrad Journal on Human Rights, 3, 17-24. https://doi.org/10.61345/1339-7915.2025.3.3

167. Абрашин, Р. П. (2024). On Thin Ice: Qualification of Cyber-Attacks on Personal Data under International Humanitarian Law. *Журнал ВШЭ По Международному Праву (HSE University Journal of International Law)*, *2*(4), 36-52. https://doi.org/10.17323/jil.2024.24743