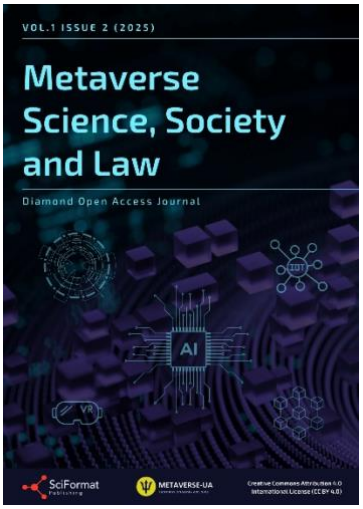

Metaverse Science, Society and Law

Vol. 1, Issue 2 (2025)

SciFormat Publishing

Publisher:
SciFormat Publishing Inc.

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

+15878858911
editorial-office@sciformat.ca

ARTICLE TITLE	IMPLEMENTATION OF INTERNATIONAL HUMANITARIAN LAW IN VIRTUAL ENVIRONMENTS: CHALLENGES AND PROSPECTS FOR REGULATING ARMED CONFLICTS IN THE ERA OF THE METAVERSE AND IMMERSIVE TECHNOLOGIES
DOI	https://doi.org/10.69635/mssl.2025.1.2.29
RECEIVED	28 September 2025
ACCEPTED	03 December 2025
PUBLISHED	15 December 2025
LICENSE	The article is licensed under a **Creative Commons Attribution 4.0 International License.**

IMPLEMENTATION OF INTERNATIONAL HUMANITARIAN LAW IN VIRTUAL ENVIRONMENTS: CHALLENGES AND PROSPECTS FOR REGULATING ARMED CONFLICTS IN THE ERA OF THE METAVERSE AND IMMERSIVE TECHNOLOGIES

Volodymyr Tymoshenko
Doctor of Juridical Sciences, Professor,Professor at the Department of the Educational and Scientific Institute of Military History, Law, and Social Sciences, National Defence University of Ukraine
ORCID ID: 0000-0003-3184-5738

Tetiana Fedchuk
Adjunct at the Department of Military Law and Law Enforcement Activities, Educational and Scientific Institute of Military History, Law, and Social Sciences, National Defence University of Ukraine
ORCID ID: 0000-0002-6821-1969

ABSTRACT

The article examines the implementation of international humanitarian law (IHL) norms in virtual environments during contemporary armed conflicts, with a focus on challenges posed by the metaverse and immersive technologies such as virtual reality (VR) and augmented reality (AR). In the context of the ongoing Russian-Ukrainian war, which began in 2014 and escalated in 2022, the study considers examples of the use of drones, autonomous artificial intelligence (AI) systems, and virtual simulators within the Armed Forces of Ukraine. The author emphasizes the universality of the fundamental principles of IHL – humanity, distinction, proportionality, and precaution – and the need to adapt them to digital realities in which legal gaps arise, including the collective consequences of cyberattacks, the indiscriminate nature of drone-swarm tactics, and double-tap strikes as potential violations.

The literature review covers key sources: the 1949 Geneva Conventions and the 1977 Additional Protocols, the positions of the International Committee of the Red Cross (ICRC) on autonomous weapons systems, NATO hybrid warfare strategies, and reports by Human Rights Watch and Amnesty International on documenting war crimes. The article discusses specific examples, including Russia's massive attacks on Ukraine's energy infrastructure in 2022–2023 using Shahed-136 (Geran-2) drones and cyberattacks (Industroyer2, Sandworm), which caused large-scale blackouts and severely affected the civilian population, as well as the cyberattack on the Viasat KA-SAT satellite network in February 2022, which resulted in collective collateral effects across Europe.

Within the Armed Forces of Ukraine, immersive technologies are being integrated into training through simulators by L7 Simulators (UNITS VR, DRONOBII, Vartovi, Dvobii) and IHL training programs supported by DCAF and the ICRC, which foster a culture of compliance with humanitarian norms. Ukraine is positioning itself as a leader in shaping new IHL standards for hybrid conflicts, advocating for updates to existing norms in UN, CCW, and NATO forums. The study proposes several recommendations: establishing a digital platform for monitoring violations, expanding training programs, strengthening interagency coordination, and deepening international cooperation. Overall, the article underscores the need to clarify and modernize IHL to ensure civilian protection in the era of digital technologies, contributing to broader discussions on the ethical regulation of future warfare.

KEYWORDS

International Humanitarian Law, Virtual Environments, Metaverse, Immersive Technologies, AI-Enabled Drones, War In Ukraine

CITATION

Volodymyr Tymoshenko, Tetiana Fedchuk. (2025) Implementation of International Humanitarian Law in Virtual Environments: Challenges and Prospects for Regulating Armed Conflicts in The Era of The Metaverse and Immersive Technologies. *Metaverse Science, Society and Law*. Vol. 1, Issue 2. doi: 10.69635/mssl.2025.1.2.29

Introduction

Modern armed conflicts increasingly rely on digital and immersive technologies – from combat simulators to autonomous systems incorporating elements of artificial intelligence. A key example is the war between Ukraine and the Russian Federation, where unmanned aerial vehicles (UAVs), artificial intelligence (AI), virtual reality (VR), augmented reality (AR) training tools, and remotely operated robotic systems are widely employed. Under these conditions, international humanitarian law (IHL) remains the foundation of the rules governing warfare: IHL sets the legal framework for armed conflicts with the aim of limiting violence during war [1, p. 283]. The core of IHL consists of the four Geneva Conventions of 1949 and the 1977 Additional Protocols, ratified by almost all states worldwide [2].

The military realities of 2022–2025 demonstrate the rapid introduction of new methods of warfare (from simulators to AI-enabled drones), which generates numerous humanitarian and legal challenges. On the one hand, IHL was historically designed to restrain traditional means and methods of warfare. On the other hand, the principles of IHL – humanity, distinction, proportionality, and precaution – must, by their very nature, apply "to all kinds of weapons and all forms of warfare, including those of the future" [3]. However, the realities of the digital age raise pressing questions: Do existing norms function clearly when applied to new technologies, and which legal gaps require improvement?

The purpose of the study is to provide a comprehensive analysis of the transformation of international humanitarian law in the context of the current Russian–Ukrainian war and to determine practical mechanisms for its implementation within the activities of the Armed Forces of Ukraine.

Scope of application: military training programs in educational institutions and training centers (integration of IHL into VR/AR-based training); international legal forums and bodies (ICRC, UN, NATO, DCAF) for shaping fundamental approaches to regulating the "digital battlefield"; non-governmental organizations and human rights groups monitoring IHL violations in the digital dimension.

Expected contribution: a foundation for proposals to support international discussions on updating or interpreting IHL in relation to immersive technologies.

Literature Review

The key sources for this study are the 1949 Geneva Conventions and the 1977 Additional Protocols, which define the fundamental scope of protection for persons involved in hostilities. The issue of transforming international humanitarian law (IHL) in the context of contemporary conflicts has been actively explored in both international doctrine and Ukrainian scholarly and analytical sources. Recent academic and policy literature has extensively discussed how IHL should adapt to challenges associated with the increasing use of autonomous weapon systems, artificial intelligence (AI), and immersive technologies (VR/AR).

A central position in this discourse is the International Committee of the Red Cross (ICRC) document expressing concern over the loss of human control over autonomous systems: such systems may "select and engage targets without human intervention," which threatens compliance with humanitarian law principles. The ICRC recommends the creation of new, legally binding rules, including the restriction of certain types of autonomous systems and the assurance of effective human control over systems capable of initiating lethal force [25].

Academic discussions further emphasize the technical risks associated with autonomous weapons. ICRC reports and conference proceedings highlight that compliance with IHL requires the development of "human-centric" approaches – for example, decision-maker training, increased transparency, and the introduction of new methods for weapons testing [27].

NATO materials, particularly the *NATO Hybrid Warfare Strategy* [28], underscore the necessity of adapting legal frameworks to the integration of kinetic, cyber, and informational means of influence.

Analyses by Bellingcat [29] and the *eyeWitness to Atrocities project* [30] demonstrate both the potential and the challenges of documenting war crimes in real time. These approaches are already being applied to document Russian war crimes in Ukraine, as recognized in reports by *Human Rights Watch* (2022) [31] and *Amnesty International* (2022) [32–35].

Key Concepts of the Research Topic

To gain a thorough understanding of the research topic, it is necessary to define and explain the core terms that underpin it. This allows for a clear delineation of the context in which traditional international humanitarian law (IHL) norms intersect with emerging digital realities.

International humanitarian law consists of legal norms established to reduce the human impact of armed conflict. It seeks to safeguard individuals who are not involved, or are no longer involved, in fighting and to set boundaries on the weapons and tactics that may be used during warfare.It encompasses the 1949 Geneva Conventions and their Additional Protocols, as well as customary international law. IHL applies exclusively during armed conflicts (whether international or non-international) and does not govern peacetime, unlike human rights law [36]. In the context of this study, the implementation of IHL refers to the application of these norms in practice, including training, judicial mechanisms, and state policies, with an emphasis on adaptation to new technologies.

Virtual environments are simulated digital spaces created using computer technologies, where users can interact with objects, other users, or artificial intelligence in real time, often with a sense of presence. These include virtual reality (VR), in which users are fully immersed in an artificial world, and augmented reality (AR), where digital elements are superimposed on the real world [37]. In our context, virtual environments are used for training, combat simulations, and even as platforms for cyber operations, raising questions about the application of IHL – for example, regarding the protection of digital objects or simulated civilians.

The metaverse is a unified digital environment in which individuals, acting through avatars, engage with one another and with virtual components in a three-dimensional space that mimics reality, with a focus on social, economic, and entertainment aspects. It combines elements of VR, blockchain, social networks, and digital economies, enabling continuous interaction across different devices [38]. In the era of the metaverse – understood as a period in which such technologies are dominant – regulatory challenges arise, as the metaverse may become a venue for virtual conflicts, propaganda, or even simulated warfare, necessitating the adaptation of IHL to decentralized digital spaces.

Immersive technologies are tools that create a sense of full engagement in a simulated reality by integrating the physical and digital worlds through visual, auditory, and tactile stimuli [39]. These technologies encompass virtual reality (VR), augmented reality (AR), mixed reality (MR), and various other systems that use head-mounted displays, sensing devices, and artificial intelligence to reproduce or simulate environments. In this context, they are applied in training to simulate IHL compliance scenarios, but they also raise ethical concerns, such as potential psychological effects on users or the risk of misuse for disinformation.

The implementation of IHL in virtual environments involves adapting traditional norms – such as the principles of distinction, proportionality, and the prohibition of unnecessary suffering – to digital platforms where conflicts may be hybrid, ranging from cyberattacks to virtual war simulations. Challenges include jurisdictional issues, protection of human rights in immersive spaces, and gaps in existing treaties that did not foresee digital technologies. Prospects for regulation involve developing new international norms or expanding interpretations of existing ones – for instance, through ICRC recommendations on the use of VR – and establishing standards for the metaverse to prevent abuses during conflicts.

Immersive Technologies in Training and Education of the Armed Forces of Ukraine

Modern virtual reality (VR) and augmented reality (AR) technologies are actively used in military training, including within the Armed Forces of Ukraine. The AFU have announced competitions and projects for the development of VR/AR simulators that enable service members to practice tactical skills in "close-to-real" conditions. For example, the company **L7 Simulators** has developed [4]:

– **UNITS VR System** for comprehensive training of MANPADS and anti-aircraft crews. It provides highly realistic conditions for operating modern MANPADS and anti-aircraft machine guns, enabling detection, tracking, and engagement of aerial targets in a safe environment.

– **UNITS LT Laser Simulator**, an innovative system that allows service members to practice shooting skills without using ammunition. Through realistic combat scenario simulations and precise result tracking, personnel can train effectively in a safe setting and improve readiness for real missions.

– **DRONOBII Training Complex** is an interactive virtual range developed to teach military personnel how to use a pump-action shotgun to counter FPV drones. The platform reproduces realistic battlefield conditions, allowing trainees to practice engagement methods and strengthen their ability to defeat aerial threats. It supports individual instruction and contributes to overall force readiness.

– **CITADELE Multimedia Classroom** is designed for teaching the *"Defense of Ukraine: Integrated Course"* in secondary general schools. This system provides modern, safe, and high-quality marksmanship training that aligns with current educational requirements.

– **Vartovi Simulator** serves as a training tool for UAV interceptor teams. It immerses users in a virtual environment where they can practice detecting, tracking, acquiring, and disabling hostile unmanned aircraft.

– **Duel FPV Simulator**, used together with the DRONOBII system, creates an integrated training solution for countering FPV drones and disrupting enemy operators controlling them.

In this scenario, the FPV operator appears in the virtual training zone wearing FPV goggles and attempts to strike the trainee by navigating the drone. The live video feed from the goggles is transmitted to a laptop. The trainee, using a VR headset and a mock pump-action shotgun or AK-74, follows the drone's movement and conducts simulated engagements.

Thus, immersive simulators enhance personnel readiness without exposing them to actual battlefield risks. Consequently, service members of the Armed Forces of Ukraine also incorporate IHL principles into such training. At the initiative of the General Staff of the AFU and with the support of the Geneva Centre for Security Sector Governance (DCAF), a series of integrated IHL courses were conducted for sergeants and officers [5]. Special attention is given to ***media literacy***, training personnel to verify and counter information threats, which also falls within the scope of civilian protection. In this way, even at the stage of soldier and sergeant training, VR/AR simulators and IHL courses help cultivate an understanding of relevant legal norms, including the principles of distinction and proportionality. DCAF has even issued methodological recommendations for integrating IHL into military training, emphasizing that the "implementation of fundamental IHL values in military practice" and updating curricula constitute best international practices [6].

The extensive use of unmanned and autonomous systems is a defining feature of the Russian–Ukrainian war. Both sides employ drones for various purposes, ranging from reconnaissance to strike and kamikaze operations. The Ukrainian military has developed frontline "drone laboratories," allowing rapid implementation of innovations. For instance, combat FPV drones remotely operated by an operator are used along the contact line for precision strikes and fire adjustment, while "Vampire" bomber drones, developed by the Ukrainian company SkyFall, significantly increase strike effectiveness. In addition, Ukraine has successfully conducted long-range attacks using maritime drones, some even modified for anti-aircraft tasks, marking the first recorded cases of striking Russian Aerospace Forces helicopters during the Battle of the Black Sea [7].

Ukraine is also developing software solutions to counter enemy drones. For example, the Sky Hunter project (2025) automates the interception of conventional enemy UAVs using anti-drone FPV drones: the system analyzes target coordinates from radars, calculates the trajectory of the FPV "hunter," and directs it to neutralize Shahed, Molniya, ZALA, and Supercam drones [8]. This automation significantly reduces the workload on air defense systems and accelerates response times.

Simultaneously, the AFU's air defense (AD) is being modernized with integrated human-AI interaction. In November 2025, the French Alta Ares system with a built-in AI module was introduced in the AFU, designed to intercept kamikaze drones [9]. Such technologies enable the detection and neutralization of enemy UAVs before they reach lethal zones around targets.

Consequently, NATO and its allies recognize Ukraine's unique expertise in unmanned systems. At recent summits, Western leaders emphasized that "Ukraine is currently the continent's sole expert in countering drones" [7]. The European Political Community Summit labeled the AFU a "drone superpower," with Denmark and the Netherlands seeking to adopt Ukrainian air defense training practices. As NATO Secretary General M. Rutte noted, "Ukraine is a formidable force in military innovation and drone countermeasures," and its experience is critical for revising NATO tactics [7]. The conclusion is clear: the use of virtual and autonomous systems necessitates not only previously unavailable training models but also a new vision for protective norms in international law.

Humanitarian-Legal Principles and Their Challenges in Digital Space

Among the core principles of international humanitarian law (IHL) are humanity, military necessity, distinction, and proportionality, which define the legal boundaries of hostilities. In particular, the principle of distinction – a cardinal rule of IHL enshrined in Article 48 of Additional Protocol I to the Geneva Conventions [10] – requires parties to a conflict to "distinguish between civilians and combatants" and "between military objectives and objects protected against attack." This provision is codified in Article 48 of Additional Protocol I (1977) [11]. However, new technologies complicate its implementation. For instance, fully autonomous combat systems "select and engage targets independently," making technical and software safeguards critically important. As IHL theorist S. Bondarenko notes, "the autonomous functioning of such systems requires strict mechanisms to ensure the differentiation between legitimate military objectives and protected objects" [11]. Without such safeguards, the risk of attacks on civilian objects increases.

Similarly, the principle of proportionality (Art. 51(5)(b), Additional Protocol I [10]) prohibits attacks that may cause "incidental harm" to civilians that would be "excessive in relation to the anticipated concrete and direct military advantage" [11].

In the context of cyber and drone attacks, assessing potential collateral effects becomes more challenging due to the unpredictability of new technologies. The ICRC explicitly emphasizes that despite the novelty of modern warfare methods, "existing law applies to all military operations, cyber and kinetic alike, and must be respected" [3]. According to the ICRC, IHL norms are "designed to apply to all types of warfare and all weapons, including those that may exist in the future" [3]. Therefore, prohibitions on attacks against civilians or indiscriminate attacks also extend to digital means: if an enemy cyber operation causes a hospital or power grid to go offline, it may be equated to an attack on a civilian object.

The ICRC provides an illustrative example: even if, prior to an armed conflict, computerized hospital systems were not considered critical military objectives, a physical missile strike on the hospital is absolutely prohibited; similarly, a successful cyberattack on the hospital's computer infrastructure does not remove its protected status [3]. In other words, a cyberattack causing failure or malfunction of hospital equipment falls under the protection regime for civilian infrastructure.

At the same time, the use of virtual reality technologies creates new contexts. For example, during VR-based training, it is necessary to clearly model the "red lines" of IHL: from simulating humanitarian scenarios to identifying virtual civilians. Although these are not actual hostilities, practicing IHL compliance in virtual simulations helps cultivate the appropriate behavioral culture among soldiers.

On the other hand, challenging questions arise: for instance, are software programs supporting civilian objects protected, and can the destruction of software be considered a cyber weapon? Currently, IHL does not provide detailed guidance on some of these issues, indicating the need for practical guidance and potentially updated international rules.

Examples of Legal Gaps and Adaptation of Existing Norms

The war in Ukraine, ongoing since 2014, reached a critical phase in 2022. Hostilities between 2022 and 2025 demonstrate numerous instances in which IHL must be interpreted in light of new circumstances. For example, in 2022–2023, Russia carried out large-scale attacks on Ukraine's energy and civilian infrastructure using Shahed-136 "Geran-2" drones, causing extensive blackouts [12]. In addition, Russia conducted cyberattacks on Ukraine's energy systems in 2022, for instance using the Industroyer2 malware aimed at energy providers to disrupt network operations [13]. At the end of 2022, Russian cyber espionage compromised parts of the energy grid – a rare example of cyberwarfare [14]. These cyberattacks were sometimes coordinated with physical strikes (missiles, drones) to maximize damage. While a direct missile strike on a populated area is prohibited, a key debate remains: can a cyberattack on energy networks – sometimes combined with kinetic strikes – be classified as a violation of IHL, given its substantial impact on civilian life? Such cases highlight the need to clarify the status of digital objects.

Another notable example is the widespread use of swarm tactics or saturation attacks with drones, where hundreds or thousands of inexpensive FPV or kamikaze drones are launched simultaneously to overwhelm air defenses and create so-called "kill zones"– areas where survival or passage for personnel and equipment is virtually impossible [15].

Under IHL, the use of indiscriminate weapons that cannot distinguish between military and civilian objects (principle of distinction) is strictly prohibited. The principle of proportionality is also violated if the expected civilian harm is disproportionate to the military advantage. In the war in Ukraine, the adversary actively employs such tactics. Russia creates "kill zones" up to 20 km deep using dense lines of FPV interceptors and mass launches of Shahed/Geran-2 drones, making certain sections of the front nearly impassable for logistics and infantry [16].

The issue of proportionality becomes particularly acute when military targets (e.g., equipment or troop positions) are located in residential areas or near civilian objects. While the presence of military equipment makes the object a legitimate target, and a mass drone swarm a permissible means of attack [17], complications arise when, after an initial kamikaze drone strike, wounded personnel and rescuers remain on site. If a second or third wave of drones automatically strikes everyone present, this constitutes a classic "double-tap strike," considered a war crime as it deliberately targets those providing aid to the wounded [18; 19].

Due to the lack of individual control over each drone in a large swarm – or due to operator delays when hundreds are launched simultaneously – it becomes impossible to accurately calculate the ratio of military advantage to civilian harm. This creates a new cumulative effect from multiple drones, which is difficult to

predict and was not anticipated by traditional proportionality norms at the time the Geneva Conventions were drafted. Experts now emphasize that IHL urgently requires clarification for such "distributed" attacks [20].

Cyber operations expose some of the sharpest legal gaps in IHL. Traditional IHL rules strictly prohibit collective punishment (Article 33, Fourth Geneva Convention 1949 [21]; Article 75(2)(d), Additional Protocol I 1977 [10]) and any attacks targeting civilians as such (Article 51(2), AP I). The prohibition of collective punishment is based on the principle of individual responsibility: punishment cannot be applied to an entire group for the actions of specific individuals.

However, by their nature, cyber operations often produce collective (dispersed) effects even when formally aimed at military objectives. A classic example is the shutdown of electricity, water, or dam/wastewater management systems for an entire region or city, leaving hundreds of thousands of civilians without essential services. Such actions may constitute collective punishment if their actual or incidental purpose is to exert pressure on the civilian population to demoralize or coerce them into surrender [22].

Similarly, the cyberattack on the Viasat KA-SAT satellite network in February 2022 (one hour before the full-scale invasion) disabled thousands of modems across Europe and disrupted military command, while also affecting civilian communications, energy companies, and wind farms in Germany – a classic case of a "collective incidental effect" [23].

Integration of IHL Norms into Ukrainian Armed Forces Training Measures

The experience of the Ukrainian Defense Forces demonstrates that effective implementation of IHL on the battlefield begins with personnel training. Alongside VR simulators for combat coordination, games and scenario-based exercises are intensively used, where commanders practice decision-making in accordance with IHL requirements. The Armed Forces of Ukraine actively cooperate with the ICRC and international partners, adapting training programs to reflect their own combat experience. For instance, in addition to the previously mentioned DCAF-led courses, military legal officers prepare handouts covering real-life situations – such as "collateral casualties during enemy pursuit" or "rules of conduct regarding prisoners of war" – requiring time-sensitive decision-making. Attention is also given to operating in multicultural environments, such as providing medical aid to civilians of different nationalities. Furthermore, civil-military cooperation officers attended IHL courses in The Hague in 2025, while NCO instructors were sent for IHL training in France.

Notably, the National Defense University (NDU) has introduced VR headsets (e.g., Meta Quest 3) into the educational process [24]. This enables the creation of realistic 3D scenarios closely approximating combat conditions, while simultaneously training psychological resilience, decision-making speed, and stress response. VR is also applied in specialized psychological training sessions, as well as in coordination and recovery exercises for personnel; for example, engaging in VR scenarios allows soldiers to "rehearse" complex situations and process emotional or traumatic experiences.

The use of VR and AR technologies in the training of commanders – for example, within combat training and junior officer/NCO leadership training – allows the modeling of complex combat scenarios in densely populated urban areas, where compliance with IHL norms is critically important. Modern simulators replicate situations involving first aid and tactical medical care, evacuation of civilians, passing through checkpoints, and dilemmas where a commander must choose between opening fire or maneuvering, taking into account the principles of distinction, proportionality, and precautionary measures (Geneva Conventions, 1949; Additional Protocol I, Articles 48–57). AR systems (e.g., IVAS helmets or NATO-equivalent devices) provide enhanced situational awareness through overlaying data on terrain, unit locations, identification of "friend/foe," and threat indicators; however, the final decision to use force always remains with the service member, in accordance with IHL requirements.

The integrated use of VR simulations combined with physical exercises has proven effective in preparing commanders. According to NATO and ICRC assessments, such methods enhance the ability of officers and NCOs to apply IHL norms accurately and rapidly under the stress of modern urban combat operations.

Ukraine's Role in Shaping a New Model of Humanitarian Law

One of the fundamental aspects of IHL is establishing accountability for violations of the rules of war and ensuring the protection of innocents. In the digital age, ideal mechanisms of human control over weaponry are increasingly challenged. The ICRC emphasizes that autonomous systems "replace human decisions over life and death with processes driven by sensors, software, and machines" [25].

This raises complex questions: if AI mistakenly selects a civilian target, who bears responsibility – the developers, the commander who deployed the system, or the producing state? The ICRC draws a clear conclusion: under such circumstances, "new legally binding rules" are required, including explicit prohibitions on projects involving AWS (Autonomous Weapon Systems) without sufficient predictability.

Moreover, in cases of war crimes committed using digital technologies (e.g., cyberattacks causing civilian casualties), the principle of individual accountability remains imperative for actors on both sides of the conflict. Ukrainian law and practice already include mechanisms for investigating such crimes.

Having become a testing ground for high-tech warfare, Ukraine naturally assumes an active role in international discussions on updating humanitarian law. Globally, it is recognized that Ukrainian experience will shape future safety standards. As Deputy Minister of Defense H. Hvozdiyar noted, Ukraine "is not only defending itself but also establishing new security standards for the wars of the future" [26]. This underscores the country's readiness to lead in adapting legal norms to high-tech conflicts.

At the international level, the Ukrainian government and military representatives advocate for consideration of digital combat realities in the work of the UN, the Convention on Certain Conventional Weapons (CCW), and other forums. In UN General Assembly and Security Council resolutions, Ukraine insists on continued control over modern weaponry and full investigations of war crimes involving their use. Simultaneously, the Ministry of Defense integrates legal education into officer training and embeds IHL principles in policy documents, including defense reform plans.

In accordance with its defense development strategy, the Armed Forces of Ukraine implement procedures for operational legal oversight of each new technology. For example, joint working groups of military lawyers and IT specialists provide assessments. Through this approach, Ukraine offers the international community not only criticism of the Russian invasion but also a constructive framework for advancing the law. Considering friendly and partnership ties with NATO countries, the Ukrainian approach to cyberweapons and adaptive defense is already being discussed at the alliance level.

Based on this research and analysis of the contemporary challenges Ukraine faces in ensuring compliance with IHL during ongoing hostilities, a series of recommendations has been formulated aimed at enhancing the effectiveness of legal mechanisms governing the actions of Armed Forces personnel in the course of the Russo-Ukrainian War.

Recommendations

1. **Development of a Unified Interagency Digital Platform for Monitoring IHL Violations.** Ukraine currently lacks a centralized system for collecting, consolidating, and analyzing information on potential IHL violations. It is recommended to establish a digital platform to facilitate data exchange between the Ministry of Defense, Ministry of Internal Affairs, Security Service of Ukraine, Prosecutor General's Office, and other agencies responsible for documenting war crimes. Such a solution would improve the accuracy of recording violations, enable timely responses, and ensure an adequate evidentiary standard for international institutions.
2. **Integration of IHL Specialists' Functions into Existing Units of the Armed Forces.** Creating new positions within the Armed Forces structure is unlikely; therefore, it is advisable to review and partially expand the functional responsibilities of personnel in legal services, civil-military cooperation units (CIMIC), communication departments, and operational support services. This approach would provide expert guidance to personnel without altering the organizational structure.
3. **Expansion of Content and Frequency of Existing IHL Training Programs.** IHL trainings already exist within the Armed Forces and other security agencies, including support from the ICRC and NATO partners. It is recommended to strengthen the practical component of these trainings, including simulations of real combat scenarios, case studies from open sources, and analysis of IHL violations committed by the aggressor state. This approach fosters resilient decision-making skills in complex operational environments.
4. **Standardization and Improvement of Information Space Monitoring Procedures.** The Main Communication Directorate of the Armed Forces already monitors official military unit resources for IHL compliance. It is advisable to formalize and unify these procedures through checklists, methodological guidelines, response algorithms, and internal instructions at all levels of military command. This ensures a consistent approach and reduces the risk of violations due to inattention or lack of awareness.
5. **Strengthening Interagency Coordination for Documenting War Crimes.** Given the number of agencies authorized to record and investigate IHL violations, it is necessary to clearly define competencies, eliminate duplication, and harmonize actions. Such coordination is feasible and aligns with international standards, including NATO practices for interagency working groups.

6. **Development of Digital Technologies for Information Processing.** The use of secure platforms, algorithms for preliminary automatic verification of materials, geolocation tools, and metadata recording represents a promising direction for Ukraine and aligns with global trends. Implementing these solutions does not require changes to the Armed Forces' regulatory structure but does require interagency support and funding.

7. **Deepening International Cooperation.** Ukraine can continue to expand collaboration with the ICRC, NATO DEEP, EU Advisory Mission, and other partners providing advisory and training support. Such cooperation facilitates the harmonization of national practices with international standards and ensures continuous exchange of expertise.

Conclusions

The experience of the 2022–2025 war demonstrates that the digitalization of military technologies necessitates careful reconsideration of IHL. Existing norms –such as the principles of distinction, prohibition of indiscriminate methods, and protection of the wounded and medical personnel—remain relevant but require detailed guidance and practical instructions for application to VR/AR and cyber means.

Ukraine has already begun taking steps in this direction: modernizing Armed Forces training according to international recommendations, disseminating best practices, and developing its own operational rules for working with new technologies.

At the same time, the international community must clarify how to protect civilians in the era of drones and virtual training: whether additional conventions on cyberwarfare are needed, how to classify "virtual" crimes, and what role private technology companies should play. The key conclusion is clear: despite all innovations in the means of warfare, humanity and the law must remain an intangible shield in any environment – real or virtual.

The authors declare no conflicts of interest.

All data supporting the findings of this study are openly available in the article. No additional datasets were generated or used during the research.

This research received no external funding.

REFERENCES

1. Crawford, E., Pert, A. (2024). *International humanitarian law*. Cambridge University Press.
2. Bothe, M., Partsch, K. J., & Solf, W. A. (2024). *New Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Convention of 1949* (Vol. 1). Martinus Nijhoff Publishers.
3. International Committee of the Red Cross (2021) *Cyber warfare: Does international humanitarian law apply?* https://www.icrc.org/en/document/cyber-warfare-and-international-humanitarian-law
4. Preparing fighters to real and virtual experiences. https://www.l7simulators.com/en#about-us
5. Armed Forces of Ukraine. (2024). *The leadership of the Armed Forces of Ukraine pays special attention to the unconditional and universal compliance by servicemen with the norms of international humanitarian law*. https://www.zsu.gov.ua/news/kerivnycztvo-zbrojnyh-syl-ukrayiny-zvertaye-osoblyvu-uvagu-na-bezzasterezhne-i-povsyudne-dotrymannya-vijskovosluzhbovczyamy-norm-mizhnarodnogo-gumanitarnogo-prava .
6. Jasutis, G., Mikova, R. (2023). *Parameters of effective military training in international humanitarian law*. DCAF – Geneva Centre for Security Sector Governance.
7. Kirichenko, D. (2025). *Drone superpower Ukraine is teaching NATO how to defend against Russia.* Atlantic Council. https://www.atlanticcouncil.org/blogs/ukrainealert/drone-superpower-ukraine-is-teaching-nato-how-to-defend-against-russia/
8. Високий Замок. (2025). *Українські розробники створюють застосунок для автоматичного збиття ворожих дронів*. https://wz.lviv.ua/news/528548-ukrainski-rozrobnyky-stvoriuiut-zastosunok-dlia-avtomatychnoho-zbyttia-vorozhykh-droniv
9. ZN.ua. (2023). *Україна збиває дрони французькими системами із вбудованим ШІ.* https://zn.ua/ukr/war/ukrajina-zbivaje-droni-frantsuzkimi-sistemami-iz-vbudovanim-shi.html
10. United Nations. (1977). Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I). Verkhovna Rada of Ukraine. https://zakon.rada.gov.ua/go/995_199
11. Бондаренко, С. Ю., Жук, Д. Ю. (2025). Перетин міжнародного гуманітарного права і нових технологій у війні: захист безпеки при дотриманні гуманітарних принципів. *Міжнародне гуманітарне право та основи безпеки у період збройних конфліктів*, 130.

12. Mackintosh, E., & Kesaieva, Y. (2023). Inside Russia's plot to plunge Ukraine into darkness, and how Ukrainians have survived. CNN. https://edition.cnn.com/interactive/2023/02/europe/putin-ukraine-energy-infrastructure-attack/index.html
13. Pearson, J. (2023). Russian spies behind cyber attack on Ukraine power grid in 2022 - researchers. Reuters. https://www.reuters.com/technology/cybersecurity/russian-spies-behind-cyberattack-ukrainian-power-grid-2022-researchers-2023-11-09/
14. Abraham, D., Houmb, S. H., Erdodi, L. (2025). Cyber-attacks on energy infrastructure – A literature overview and perspectives on the current situation. Applied Sciences, 15(17), Article 9233. https://doi.org/10.3390/app15179233
15. Militarnyi. (2025). The kill zone of modern warfare: Size and structure, control and means of destruction, survival and shifting the lines. https://militarnyi.com/en/articles/the-kill-zone-of-modern-warfare-size-and-structure-control-and-means-of-destruction-survival-and-shifting-the-lines/
16. ZeroLineIntel. (2025). Rubicon is real: Russia's elite drone vanguard enters the fight. https://zerolineintel.com/rubicon-is-real-russias-elite-drone-vanguard-enters-the-fight/
17. Just Security. (2024). Death toll climbs in Ukraine with Russia's 'double-tap' strikes. https://www.justsecurity.org/97455/ukraine-russia-double-tap-strikes/
18. Radio Free Europe/Radio Liberty. (2025). Ukraine says Russia hits firefighters with 'double-tap' strike. https://www.rferl.org/a/russia-ukraine-drones-attacks-nato-response-chernihiv/33536204.html
19. Truth Hounds. (2024). Examining the pattern of Russian double-tap strikes in Ukraine. https://truth-hounds.org/en/cases/cruelty-cascade /
20. Boulanin, V. (2025). Autonomous weapon systems in the Russia-Ukraine war: Issues and recommendations. SIPRI Insights on Peace and Security.
21. United Nations. (1949). Женевська конвенція про захист цивільного населення під час війни [Geneva Convention relative to the Protection of Civilian Persons in Time of War]. Verkhovna Rada of Ukraine. https://zakon.rada.gov.ua/laws/show/995_154#Text
22. International Federation for Human Rights. (2022). Ukraine: Russia's attacks against energy infrastructure violate international humanitarian law. https://www.fidh.org/en/region/europe-central-asia/ukraine/russia-attacks-against-energy-infrastructure-ukraine
23. Schmitt, M. N., Keitner, C. I. (2023). Ukraine, cyberattacks, and the lessons for international law. American Journal of International Law, 117(3), 355–400. https://doi.org/10.1017/ajil.2023.34
24. National University of Defense of Ukraine. (n.d.). *VR in education* [Web page]. Retrieved November 21, 2025, from https://nuou.org.ua/en/u/news/vr-in-edu.html
25. ICRC. (2021). *ICRC position on autonomous weapon systems*. International Committee of the Red Cross. https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems
26. Uryadovyi Kurier. (2025). Нові стандарти безпеки у війнах майбутнього. Урядовий Кур'єр. https://ukurier.gov.ua/uk/news/novi-standarti-bezpeki-u-vijnah-majbutnogo/
27. Conroy, S. K. (2024). *Spotlight session on autonomous weapons systems at ICRC 34th International Conference*. arXiv. https://doi.org/10.48550/arXiv.2411.08890
28. NATO. (2020). NATO's approach to hybrid warfare.
29. Bellingcat. (2022). *Bellingcat annual report 2022*. https://www.bellingcat.com/app/uploads/2023/06/Bellingcat-Annual-Report-2022_com.pdf
30. International Bar Association. (2025). *Innovative eyeWitness to Atrocities app is focus of IBA and JustTalk Ukraine technology event*. IBA. https://www.ibanet.org/Innovative-eyeWitness-to-Atrocities-app-is-focus-of-IBA-and-JustTalk-Ukraine-technology-event
31. Human Rights Watch. (2022). "Відповідальність має вирішальне значення". Коментар HRW про права людини в Україні у 2022 році. Радіо Свобода.: https://www.radiosvoboda.org/a/news-hrw-zvit-2022-ukrajina/32219920.html
32. Amnesty International. (2022). *Ukraine: Russia's unlawful transfer of civilians a war crime and likely a crime against humanity* – репортаж про насильницьке переміщення цивільних, фільтрацію й порушення МГП. https://www.amnesty.org/en/latest/news/2022/11/ukraine-russias-unlawful-transfer-of-civilians-a-war-crime-and-likely-a-crime-against-humanity-new-report/
33. Amnesty International. (2022). *"ANYONE CAN DIE AT ANY TIME": Indiscriminate attacks by Russian forces in Kharkiv, Ukraine* – звіт з аналізом безрозбірних обстрілів у Харкові. https://www.amnesty.de/sites/default/files/2022-06/Amnesty-Bericht-Ukraine-Russland-Streumunition-Charkiw-Juni-2022.pdf
34. Amnesty International. (2022). *Ukraine: Forcible Transfer and Poor Treatment of Civilians from Occupied Ukraine*. Executive Summary (pdf). https://www.amnesty.org/en/wp-content/uploads/2022/11/Amnesty-Bericht-Ukraine-Russland-Verschleppung-Zivilpersonen-November-2022.pdf
35. Amnesty International. (2022). *Report on Violations of International Humanitarian and Human Rights Law in Ukraine*. https://www.amnesty.org/en/wp-content/uploads/2022/09/EUR4659882022ENGLISH.pdf

36. International Committee of the Red Cross. What is international humanitarian law? https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/what_is_ihl.pdf
37. International Committee of the Red Cross. Virtual reality. ICRC. https://www.icrc.org/en/article/virtual-reality
38. Cambridge University Press. Metaverse. In Cambridge Dictionary. https://dictionary.cambridge.org/us/dictionary/english/metaverse
39. Ada Lovelace Institute. (2024). Immersive technologies: Explainer. Ada Lovelace Institute. https://www.adalovelaceinstitute.org/resource/immersive-technologies-explainer/
40. Kostenko, O., Prokopovych-Tkachenko, D. I., Sarychev, V. (2023). Metaverse: The need to develop a national security foresight for virtual environments. IX International Scientific and Practical Conference “Modern science: actual problems”, November 28–29, 2023, Manchester, UK. https://doi.org/10.5281/zenodo.10257264