NEW CHALLENGES FOR INTERNATIONAL CRIMINAL LAW: HOW TO INCORPORATE CYBERCRIMES COMMITTED DURING ARMED CONFLICTS INTO THE EXISTING LEGAL FRAMEWORK

Hedz Vladyslava, Bondarenko Yevheniia, Zhabchyk Daryna

DOI: https://doi.org/10.61345/1339-7915.2025.3.3

Annotation. The article examines the legal characterization of cybercrimes in the international context, with particular attention to cyber operations committed during armed conflicts. The study explores the distinction between ordinary cybercrimes, typically prosecuted under domestic criminal law and international cooperation frameworks such as the Budapest Convention (2001), and cyberattacks carried out in wartime, which fall under the scope of international humanitarian law and international criminal law. Special focus is placed on the challenges of attributing responsibility, defining cyber operations in the context of warfare, and incorporating such acts into the jurisdiction of international courts.

The urgency of this article is underscored by the ongoing war in Ukraine, which has demonstrated the devastating humanitarian impact of large-scale cyberattacks on civilian infrastructure, such as the Kyivstar incident currently under investigation by the International Criminal Court. This highlights the pressing need to adapt existing international legal frameworks to ensure accountability for cyber-enabled violations of IHL.

The article analyzes how cyber operations can amount to war crimes, crimes against humanity, or even acts of aggression if their effects meet the thresholds established under Rome Statute of the International Criminal Court. It argues that, although the Rome Statute does not explicitly mention cybercrimes, its provisions are sufficiently technology-neutral to encompass cyber conduct when interpreted in light of humanitarian consequences. Reference is made to the Tallinn Manual 2.0, International Committee of the Red Cross positions, and scholarly contributions that emphasize the adaptability of current law to emerging digital threats.

Furthermore, the study highlights ongoing debates among scholars and policymakers regarding whether explicit amendments to the Rome Statute are necessary, or whether consistent interpretation of existing provisions is sufficient. It stresses that while treaty reform may be politically difficult, judicial practice, state cooperation, and interpretive clarification by bodies such as the Council of Advisers on the Application of the Rome Statute to Cyberwarfare can effectively integrate cyber operations into the framework of international criminal accountability.

The study concludes that incorporating cyber operations into international criminal law does not necessarily require new treaties but rather a consistent interpretation and application of existing norms. Ensuring accountability for cyberattacks in armed conflict will depend on judicial practice, state cooperation, and clarification by international institutions. In this way, the article contributes to the broader debate on strengthening the international legal order in response to the realities of modern warfare.

Key words: cybercrime, cyberattacks, international humanitarian law, international criminal law, Rome Statute, war crimes, Ukraine.

1. Introduction.

Since the Russia's full-scale invasion of Ukraine, it has become clear that warfare today extends beyond land, air, and sea to include cyberspace. Cyberattacks have become a systematic component of armed conflict disrupting critical infrastructure, paralyzing government services, and posing direct threats

to civilian safety. These attacks are often accompanied by information and psychological operations aimed at spreading disinformation, inciting panic, and undermining public trust in the state.

According to the Ukrainian government's Computer Emergency Response Team (CERT-UA), more than 200 targeted destructive cyberattacks have been recorded against Ukrainian institutions and companies since early 2022. In 2024 alone, over 4,000 cyber incidents were documented [11]. Among the most high-profile were the December 12, 2023, attack on Kyivstar, Ukraine's largest mobile operator, which left millions without communication or internet access, and the breach of the Parkovy data center in January 2024, which disrupted dozens of public and private services, including government registries, customs systems, Ukrposhta, Naftogaz, and transport infrastructure [12].

In this context, international criminal law (ICL) faces unprecedented challenges. Legal frameworks shaped by past wars are not fully equipped to address the realities of digital warfare. There is currently no universally accepted definition of cyberattacks as war crimes, and questions regarding attribution, the legal status of data as a protected object, and responsibility for complex, multilayered attacks remain contentious. At the same time, international institutions, most notably the International Criminal Court (ICC), have begun investigating such incidents. The case of the Kyivstar attack is under scrutiny as a potential war crime, given its foreseeable consequences for civilian safety [5].

2. Analysis of scientific publications.

The issue of legal regulation of cyber operations and their qualification under international law (IHL) has been extensively examined by scholars and international institutions. General aspects of cybercrime and mechanisms of international cooperation are reflected in the Council of Europe's Convention on Cybercrime (the Budapest Convention on Cybercrime, 2001) [2] which harmonizes national legislation and provides a framework for prosecuting cross-border cyber offenses.

The applicability of IHL to cyber operations has been addressed in the Tallinn Manual 2.0 [11], which affirms that IHL rules are technology-neutral and extend to cyberspace. The International Committee of the Red Cross (ICRC) has also emphasized that the core principles of distinction, proportionality, and precautions apply equally to cyberattacks conducted during armed conflicts.

Scholars have further explored the incorporation of cyber operations into ICL. Trahan highlights their potential qualification as acts of aggression [13], while Khan stresses that war crimes and crimes against humanity can already encompass cyber conduct without amending the Rome Statute [6]. Ukrainian scholars, such as Vasylkivska and Bondarenko, contribute by situating cyber threats within the broader framework of hybrid warfare, particularly in the context of Russia's aggression against Ukraine [15].

Overall, the literature demonstrates consensus that IHL and ICL applies to cyberspace, though debates persist over definitional clarity and enforcement challenges. These works significantly contribute to understanding the legal dilemmas of cyber warfare and the need for effective mechanisms of accountability.

3. The aim of the work.

This study is driven by the urgent need to reassess how international legal norms protect civilians in modern warfare, which now encompasses both physical and digital domains. The aim of this research is to analyse how ICL can adapt to the emerging challenges posed by cyberattacks in the context of armed conflict. Using the Russian-Ukrainian war as a primary case study, the paper explores relevant precedents, legal gaps, and the implications of recent cyber incidents for the future of international accountability. And to answer the research question: *How can international criminal law adapt to the emerging challenges of cybercrime in the context of armed conflict, particularly in the case of the Russian-Ukrainian war?*

4. Review and discussion.

The legal characterization of cybercrimes in the international context requires careful consideration of both general criminal law frameworks and the specific rules applicable during armed conflicts. In

particular, the application of IHL and ICL to cyber operations has become a pressing issue, as the digital domain increasingly serves not only as a platform for ordinary criminal activity but also as a battlefield where states and non-state actors engage in hostile actions. This dual dimension underscores the need to distinguish between general cybercrimes and cyberattacks conducted in the context of armed conflict, as each category entails different legal qualifications and mechanisms of accountability.

General Cybercrimes vs. Cyberattacks During Armed Conflict. Cybercrimes generally refer to illegal activities directed against or carried out via computer systems and networks. This broad category includes offenses such as unauthorized system intrusions (hacking), theft of data or intellectual property, online fraud and financial theft, identity theft, cyber extortion (e.g. ransomware), and distribution of malicious code. The Budapest Convention on Cybercrime 2001 was the first international treaty to address such crimes, aiming to harmonize national laws and facilitate cross-border cooperation in combating offenses ranging from breaches of network security to computer-related fraud and forgery [2]. Under this framework, cybercrimes are largely treated as transnational criminal offenses prosecuted under domestic law, even when their effects span multiple jurisdictions.

It is crucial to distinguish ordinary cybercrimes from cyber operations that occur in the context of an armed conflict. General cybercrimes (e.g. stealing corporate data, financial cyber fraud, or defacing websites for propaganda) are usually motivated by personal or financial gain, political activism, or espionage, and are perpetrated in peacetime or outside any war context. These acts violate domestic criminal statutes (such as computer misuse and fraud laws) and, when transnational, trigger international cooperation mechanisms like those under the Budapest Convention (2001) [2].

By contrast, cyberattacks during armed conflict, for example, a state or its agents hacking an enemy's critical infrastructure, disabling an air defence system, or disrupting a power grid in the midst of hostilities, are more akin to means and methods of warfare. Such operations are conducted as part of military strategy, intended to advantage one party in a conflict. They can have devastating effects: consider a cyber operation that shuts down a city's electricity and communications during war, potentially causing chaos in civilian services and aiding concurrent kinetic attacks. While the immediate conduct (unauthorized access to systems, causing system malfunctions, etc.) might resemble "cybercrimes" in a technical sense, these wartime cyber operations are governed by an entirely different legal paradigm, namely, international humanitarian law, rather than ordinary criminal law. In short, the same technical act (e.g. penetrating a computer network) might be labelled a crime in peacetime, but if undertaken as part of combat, it is viewed through the lens of jus in bello (law of armed conflict) rather than purely as a domestic criminal offense [10; 13].

Lack of a Universal Definition in Warfare Context. International law currently lacks a universally accepted definition of "cybercrime" or "cyberattack" in the context of warfare. The term cybercrime itself is generally not used in treaties or official documents to describe cyber operations by belligerents; instead, terms like "cyber warfare," "cyber operations," or "cyber attacks" are used in scholarship and policy to denote hostile cyber activities between states. Notably, no global treaty to date defines cyber warfare or enumerates cyber operations as distinct war crimes. The Tallinn Manual 2.0 (2017) – a non-binding but influential restatement by experts – attempts to articulate how existing international law applies to cyberspace, distinguishing between cyber operations below the threshold of armed conflict and those amounting to uses of force or occurring during conflict [10]. However, even the Tallinn Manual does not provide a singular definition of "cyber warfare," instead applying established legal definitions (e.g. "attack," "use of force") to cyber contexts [10].

Similarly, the term "cyber terrorism" or "cyber warfare" has no agreed legal meaning in United Nations instruments. As Trahan observes, we are still operating with analogy and interpretation: cyber means are viewed through pre-existing legal categories (such as the United Nations Charter's prohibition on the use of force, or the war crimes listed in the Rome Statute), rather than through any cyber-specific legal definition [13].

The result is a gap in terminology – states and experts recognize the reality of cyber operations in conflict, but international law has yet to formally codify what constitutes a "cyber attack" or "cybercrime" in war. In practice, this means that whether a particular malicious cyber act in wartime is deemed lawful or unlawful is determined by applying general principles of international law (e.g. sovereignty, non-intervention, or IHL rules) to the facts, rather than by referencing a bespoke "cyber law" treaty definition. Efforts like the Budapest Convention address cybercrime generally, and the Tallinn Manual 2.0 and ongoing UN discussions provide guidance for state behavior, but a universally-endorsed definition of

cyber warfare or cybercrime in armed conflict remains absent [10; 13]. This lack of definitional consensus underscores the importance of context: the same conduct might be labeled differently – as an ordinary crime, or as an act of war, depending on whether it occurs in peacetime or during an armed conflict.

Application of International Humanitarian and Criminal Law to Cybercrimes During Armed Conflict. Once an armed conflict exists (whether an international armed conflict between states or a non-international conflict), IHL applies to all military operations undertaken by the belligerents. This includes cyber operations just as much as traditional kinetic operations. Although treaties like the Geneva Conventions were drafted long before cyber warfare, their rules are technology-neutral and have been interpreted to govern new means of warfare. The consensus among experts and institutions (reflected in the Tallinn Manual 2.0 and the position of the ICRC) is that cyber-attacks during armed conflict must abide by the same fundamental IHL principles as any other attack [10; 5].

Thus, a hacking operation that disables an adversary's military air defence network would be considered a lawful act of war in principle, whereas a similar operation targeting civilian infrastructure for the sake of terrorizing the population would be unlawful. In practice, states and the ICRC have increasingly affirmed that IHL limits apply to cyber operations in war, ensuring humanitarian protections are not bypassed using new cyber means [5].

Cyber operations during armed conflict must comply with three fundamental IHL principles: distinction, proportionality, and precautions. Distinction prohibits targeting civilians or civilian infrastructure; cyberattacks on hospitals or water systems violate this rule just as physical attacks would [5]. Proportionality forbids operations where expected civilian harm is excessive relative to the anticipated military advantage, especially relevant in cyber contexts where cascading effects (e.g., power grid failures) can impact civilians far beyond the intended target [10]. Precautions require attackers to minimize civilian harm, such as by designing malware with safeguards or verifying targets are not dual-use (AP I, art. 57) [10]. Breaching these principles renders a cyber operation unlawful under IHL [5].

It should be emphasized that these IHL principles apply irrespective of the weapon or method used. Cyber weaponry does not enjoy a legal grey zone or impunity. If a cyber operation inflicts consequences prohibited under IHL, it is no different than using a conventional bomb or weapon to do so. For instance, deliberately causing a city-wide blackout in winter purely to spread terror among the civilian population would breach the prohibition on attacking civilians. Conversely, operations that solely affect military systems (e.g. hacking into an enemy's military radar to misdirect aircraft, or disabling a hackable military drone) are permissible under IHL, so long as the resulting effects do not escape into the civilian realm. Under IHL, a cyber operation is judged by its effects and context, not by its novelty.

War Crimes via Cyberattacks. International criminal law comes into play when serious violations of IHL or other core international prohibitions occur, attaching individual liability to commanders, hackers, or political leaders who orchestrate those acts. War crimes, as defined in Article 8bis of the Rome Statute (1998) [9], encompass grave breaches of the Geneva Conventions and other serious violations of the laws and customs of war. The key point is that IHL violations committed through cyber means can constitute war crimes, just as if they were committed with kinetic weapons. There is no requirement that a crime be carried out with traditional weaponry, it is the outcome and intent that matter. For example, if during an armed conflict a military officer deliberately launches a cyber operation knowing it will shut down the power to a hospital and kill patients, that act could be charged as the war crime of intentionally directing attacks against a civilian object or treacherously killing civilians (Art. 8(2)(b)(ii) and (b)(i)) [9].

Likewise, causing destructive effects by cyber means that are clearly disproportionate to the military advantage (e.g. unleashing a virus that spreads uncontrollably beyond an intended military target, causing widespread civilian damage) could amount to the war crime of launching an indiscriminate attack or an attack causing excessive civilian harm (Art. 8(2)(b)(iv)) [9]. The Tallinn Manual 2.0 explicitly notes that individuals can be held criminally responsible for war crimes committed via cyber operations (Rule 84) [10]. The ICC, in theory, could prosecute cyber-related war crimes if they fit the existing definitions and occur in a situation under its jurisdiction. One challenge in prosecuting cyber war crimes is evidentiary, but legally, instruments like the Rome Statute are capable of covering cyber conduct. Indeed, scholars have affirmed that no amendment of the Rome Statute is required to accommodate cyber warfare – "cyber" is simply a means by which the already criminalized acts (willful killing, attacking protected objects, etc.) may be carried out [10]. In sum, cyberattacks can qualify as war crimes when they meet the definition of any war crime provision (e.g., targeting civilians, perfidy, destruction beyond military necessity) during armed conflict.

Crimes Against Humanity and Cyber Operations. Apart from war crimes (which require an armed conflict context), Crimes Against Humanity (CAH) under Article 7 of the Rome Statute can occur in peacetime or war and consist of specified inhumane acts (murder, persecution, etc.) committed as part of a widespread or systematic attack against a civilian population, with knowledge of the attack [9]. The question arises whether cyberattacks could form part of such an "attack against a civilian population" to constitute crimes against humanity. The term "attack" in CAH is defined in the ICC Elements of Crimes as a course of conduct involving the multiple commission of acts against civilians pursuant to a policy (Art. 7(2)(a)) [9]. Unlike IHL, this concept of "attack" is not necessarily limited to kinetic violence, it broadly covers any mistreatment of a civilian population. Therefore, a series of malicious cyber operations directed against civilians could amount to crimes against humanity if they reach the required scale and organization. For instance, imagine a regime intentionally and repeatedly using cyber means to shut off power and water to cities inhabited by a particular ethnic group, as part of a systematic persecution.

There is ongoing debate over whether non-physical harm from cyber operations can constitute crimes against humanity. While many CAH, such as extermination or enslavement, involve physical violence, some experts argue that cyber-induced suffering, like deprivation of essential services, may qualify under acts such as persecution or "other inhumane acts" [1]. The Council acknowledges that cyber operations without direct physical harm may not meet the threshold for certain crimes (e.g., murder), but concludes that cyber means can fulfill the contextual elements of CAH if they are part of a widespread or systematic attack against civilians [1]. Large-scale cyber campaigns causing severe harm, especially when tied to state policy, could thus fall within Article 7 of the Rome Statute. The lack of case law does not preclude their legal qualification.

Cyberattacks and the Crime of Aggression. The crime of aggression under Article 8bis of the Rome Statute criminalizes leadership responsibility for launching illegal uses of force that constitute a manifest violation of the UN Charter [9]. While traditionally linked to invasions or bombardments, legal scholars increasingly recognize that cyber operations can also meet this threshold if their effects are equivalent to conventional armed attacks [1; 10]. According to the Tallinn Manual 2.0, a cyber operation may amount to a "use of force" or even an "armed attack" under the UN Charter if it causes severe physical destruction, loss of life, or large-scale disruption (Rules 69, 71) [10].

For example, a state-led cyber campaign disabling a country's power grid, defence systems, and financial infrastructure, resulting in widespread civilian harm, could qualify as an act of aggression, particularly if planned and executed by state leaders without justification [1]. As Trahan emphasizes, international law is effects-based: cyber operations that mimic the impact of kinetic force should be treated equivalently [13]. No amendments to the Rome Statute are required, the current wording of Article 8bis is broad enough to include cyber-enabled aggression.

The Kyivstar Cyberattack as a Potential War Crime. The December 2023 cyberattack on Kyivstar, Ukraine's largest mobile network operator, serves as a landmark example in the evolving debate over the legal qualification of cyber operations during armed conflict. The attack, allegedly carried out by the Russian hacking group Sandworm, which has documented ties to Russian military intelligence, disrupted communications for over 24 million users, including emergency services, air raid warning systems, banking operations, and civilian internet access. This incident marked one of the most damaging cyberattacks on a civilian infrastructure target in Ukraine since the start of Russia's full-scale invasion [8].

This event is particularly significant because it is currently under investigation by the ICC as a potential war crime. According to sources close to the ICC's ongoing investigation, the attack is one of at least four major cyber incidents targeting critical Ukrainian infrastructure that are being examined for their legality under IHL [8]. The inclusion of the Kyivstar attack in this inquiry suggests that international legal bodies are beginning to treat cyber operations with physical-world consequences as serious violations of the laws of armed conflict.

The foreseeable consequences of the attack raise acute legal and moral concerns. Professor Michael Schmitt has argued that such cyber operations may meet the threshold of war crimes if they directly harm civilians or civilian infrastructure, or disrupt essential services with predictable humanitarian consequences [10]. In this case, the disabling of Kyivstar not only interrupted ordinary telecommunications but jeopardized human lives by cutting access to mobile apps used for air raid alerts, a violation that could potentially satisfy the legal requirements for "intentionally directing attacks against civilian objects" under Article 8(2)(b)(ii) of the Rome Statute [9].

In terms of international legal frameworks, the attack on Kyivstar exemplifies the kinds of operations that blur the boundary between civilian and military targets. While Kyivstar is a commercial telecom provider, its services are used for emergency alerts and public warning systems, placing it within the realm of dual-use infrastructure. Under IHL's principle of distinction, attacking infrastructure used predominantly for civilian purposes constitutes an unlawful act if not justified by concrete and direct military advantage. Moreover, the principle of proportionality prohibits attacks where expected civilian harm outweighs the anticipated military gain. Given the scope of disruption and the fact that no military systems were directly affected, the proportionality of the attack is highly questionable.

The Human Rights Center at UC Berkeley has submitted confidential reports to the ICC identifying Sandworm as responsible for at least five cyber operations potentially qualifying as war crimes [3]. Among these, the Kyivstar attack is a focal point due to its scale, public impact, and the clarity of its civilian target. If the ICC ultimately issues indictments or arrest warrants related to this case, it would establish a historic precedent, not only affirming that cyber operations fall under the jurisdiction of ICL but also clarifying the threshold at which digital attacks on civilian infrastructure amount to prosecutable crimes under IHL.

Importantly, this case also underscores the evidentiary challenges in prosecuting cyber-related war crimes: attribution must be precise, and the causal links between the cyber operation and civilian harm must be demonstrable. However, with increasing reliance on digital infrastructure during warfare, such legal inquiries will become more frequent and necessary.

In sum, the Kyivstar case is not merely an isolated incident of digital sabotage; it is a critical test case for the application of war crimes jurisprudence to cyberspace. Its legal assessment may shape the contours of international criminal accountability for cyber operations in the years to come, clarifying that in the eyes of the law, cyber weapons do not operate in a normative vacuum. When aimed at civilian infrastructure with foreseeable human costs, they may trigger the gravest legal consequences.

Possible Ways for the Legal Incorporation of Cybercrimes into International Criminal Law. The war in Ukraine has exposed how cyberattacks (targeting energy, communications, or medical infrastructure) can cause humanitarian harm comparable to kinetic warfare [5; 8]. Despite the absence of explicit reference to "cybercrimes" in the Rome Statute, growing expert consensus suggests that existing crimes under ICL can apply to certain cyber operations, provided their effects meet the legal thresholds [1; 13].

Amending the Rome Statute to include cyber operations is one option, but it is politically difficult. Most scholars argue that no new categories are needed, rather, existing crimes like war crimes and crimes against humanity can encompass cyber conduct if the act causes prohibited harm [6]. The Council of Advisers support this view, noting that cyber means can serve as the method of committing existing offenses [1].

For example, under Article 8(2)(b)(ii) of the Rome Statute, intentional attacks on civilian infrastructure may qualify as war crimes [9]. A cyber operation disabling a hospital or power grid during conflict could be prosecuted if the necessary intent and consequences are proven [9; 11]. While many IHL rules are technology-neutral, further interpretive clarification, such as from the Assembly of States Parties, would help ensure legal certainty without overstepping the principle of legality (Art. 22 of the Rome Statute) [9].

Incorporating cyber operations into the crime of aggression under Article 8bis is more complex. The threshold "use of armed force" manifestly violating the UN Charter, could be met if a cyberattack causes severe disruption equivalent to conventional force [13]. The Tallinn Manual and the Council of Advisers note that destructive cyberattacks on defence or critical infrastructure may meet this standard. However, jurisdictional limits, such as Russia's non-membership in the ICC, hinder current prosecutions, prompting calls for a special tribunal on aggression related to Ukraine, potentially covering cyber elements [7].

Where ICC jurisdiction or doctrine falls short, other legal options exist:

Hybrid or special tribunals could be established to try cyber offenses in the context of armed conflict, especially where the ICC cannot act.

Domestic prosecutions are already occurring. For example, Ukraine has opened cases against cyberattacks on its mobile network and civilian infrastructure [4]. States can also rely on universal jurisdiction for grave breaches of IHL.

Cybercrime treaties, like the Budapest Convention (2001), create obligations for states to criminalize and cooperate on cyber offenses. While primarily applicable in peacetime, they complement ICL by denying haven to cybercriminals and supporting evidence sharing.

Incorporating cybercrimes into ICL does not necessarily require new treaties. Through consistent interpretation of existing norms, supported by clarification, practice, and multilateral cooperation, international law can evolve to address cyber harm. As Trahan notes, the key lies in ensuring that cyberspace is not a legal void, but a domain governed by the same accountability principles as traditional warfare [13].

5. Conclusions.

The analysis demonstrates that cyberspace has become an indispensable dimension of modern armed conflicts, producing humanitarian consequences comparable to those of conventional warfare. While general cybercrimes are effectively addressed within existing frameworks such as the Budapest Convention, cyber operations conducted in wartime raise complex questions of legal qualification and accountability under international humanitarian law and international criminal law.

First, the absence of a universally accepted legal definition of "cyber warfare" or "cybercrime" in armed conflict creates interpretative gaps. Nevertheless, the principles of distinction, proportionality, and precautions under international humanitarian law are sufficiently technology-neutral to apply to cyber operations. The same act that constitutes a crime in peacetime may amount to a war crime if carried out as part of hostilities and with foreseeable civilian consequences.

Second, international criminal law already provides mechanisms to prosecute cyber-enabled violations. Cyber operations can qualify as war crimes, crimes against humanity, or even acts of aggression if they meet the substantive thresholds established in the Rome Statute. The ICC's current consideration of cases such as the Kyivstar attack underscores the growing recognition that cyber means do not exist in a legal vacuum.

Third, while amending the Rome Statute to explicitly include cyber operations remains politically challenging, the prevailing scholarly and institutional consensus affirms that existing provisions are adequate if interpreted consistently. Therefore, the priority lies not in creating new categories of crimes but in ensuring robust application of current norms, supported by state practice, judicial clarification, and multilateral cooperation.

In conclusion, the effective incorporation of cyber operations into international criminal law is essential to maintaining accountability in contemporary warfare. As the war in Ukraine illustrates, digital weapons can inflict humanitarian harm of unprecedented scale. International law must therefore continue to evolve through interpretation, case law, and coordinated state action to guarantee that cyberspace does not become a zone of impunity.

References:

1. Council of Advisers. Report on the Application of the Rome Statute of the International Criminal Court to Cyberwarfare. Permanent Mission of Liechtenstein to the United Nations, 2021. URL: https://crimeofaggression.info/wp-content/uploads/GIPA_The-Council-of-Advisers-Report-on-the-Application-of-the-Rome-Statute-of-the-International-Criminal-Court-to-Cyberwarfare.pdf.

2. Council of Europe. Convention on Cybercrime (Budapest Convention). European Treaty Series No. 185, 2001. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

3. Human Rights Center, UC Berkeley School of Law. Accountability for Cyber-Enabled International Crimes [Electronic resource]: Article 15 communications submitted to the International Criminal Court (2022–2023) regarding Sandworm cyber operations. Berkeley, 2024. URL: https://humanrights.berkeley.edu/projects/accountability-for-cyber-enabled-international-crimes.

4. IBANet. Ukraine Investigates Wartime Cyberattacks as Part of War Crimes Cases. 2024. URL: https://www.ibanet.org/article/cyberattacks-ukraine-investigation.

5. International Committee of the Red Cross. International Humanitarian Law and Cyber Operations During Armed Conflicts: ICRC Statement to the UN Open-Ended Working Group. 2022. URL: https://www.icrc.org/en/document/icrc-statement-cyber-operations-during-armed-conflicts.

6. Khan K. ICC Prosecutor's Statement on Emerging Cyber Threats. Office of the Prosecutor, International Criminal Court, 2023. URL: https://www.icc-cpi.int/news/statement-icc-prosecutor-karim-aa-khan-kc-conference-addressing-cyber-enabled-crimes-through.

7. Lieber Institute. The Legal Challenges of Prosecuting Cyber Aggression. 2024. URL: https://lieber.westpoint.edu/legal-prosecution-cyber-aggression.

8. Reuters. ICC Examines Russian Cyberattacks in Ukraine as Possible War Crimes. 2024. URL: https://www.reuters.com/world/europe/icc-probes-cyberattacks-ukraine-possible-war-crimes-sources-2024-06-14.

9. Rome Statute of the International Criminal Court. United Nations Treaty Series, Vol. 2187, p. 90, 1998. URL: https://www.icc-cpi.int/sites/default/files/RS-Eng.pdf.

10. Schmitt M.N. (Ed.). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press, 2017. URL: https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/2017-Tallinn-Manual-2.0.pdf.

11. State Service of Special Communications and Information Protection of Ukraine. CERT-UA Processed 4,315 Cyber Incidents Last Year. 2025. URL: https://cip.gov.ua/en/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv.

12. State Service of Special Communications and Information Protection of Ukraine. Intensity Does Not Decrease: State Service of Special Communications and Information Protection Records an Increase in Cyber Incidents Almost Twice Since the Beginning of 2022. Forbes Ukraine, 31 January 2024. URL: https://forbes.ua/news/intensivnist-ne-zmenshuetsya-derzhspetszvyazku-fiksue-zbilshennya-kiberintsidentiv-mayzhe-vdvichi-z-pochatku-2022-go-31012024-18892.

13. Trahan J. Cyber Operations and the Crime of Aggression. Case Western Reserve Journal of International Law, 2025, Vol. 57, No. 1, pp. 77–108. URL: https://scholarlycommons.law.case.edu/jil/vol57/iss1/6.

14. United Nations General Assembly. Definition of Aggression: Resolution 3314 (XXIX), 1974. URL: https://www.un.org/ruleoflaw/files/GARes3314.pdf.

15. Vasilkyvska I., Bondarenko Y. Information and Cyber Security in the Light of Hybrid Threats. Visegrad Journal on Human Rights, 2022, № 3, pp. 38–43. URL: https://journal-vjhr.sk/wp-content/uploads/2023/01/Visegrad_3_2022.pdf.

Vladyslava Hedz,
Master of Law, Kyiv National Economic University named after Vadym Hetman,
Master of Public Policy and Governance, Kyiv School of Economics,
E-mail: vladyslavahedz@gmail.com

Daryna Zhabchyk,
Master of Public Policy and Governance, Kyiv School of Economics
E-mail: dzhabchyk@kse.org.ua

Yevheniia Bondarenko,
PhD, associate professor of the Department of Public and International Law
Kyiv National Economic University named after Vadym Hetman, Ukraine
E-mail: bondarenko.yevheniia@kneu.edu.ua
ORCID: 0000-0003-0468-7949