sciendo

STUDIES IN LOGIC, GRAMMAR AND RHETORIC 70 (83) 2025

DOI: 10.2478/slgr-2025-0049

Justyna Magdalena Krzywkowska
Uniwersytet Warmińsko-Mazurski w Olsztynie
Ełk, Poland
e-mail: justyna.krzywkowska@uwm.edu.pl
ORCID: 0000-0002-0667-6453

Svitlana Mazepa
West Ukrainian National University
Ukraine
e-mail: intpolsveta@gmail.com
ORCID: 0000-0003-1282-9089

ORGANISED CYBERCRIME TRENDS IN TIMES OF WAR: THE HIDDEN FRONTLINE OF THE RUSSIA-UKRAINE CONFLICT

Abstract. The article examines current trends in organized cybercrime in the context of the Russian-Ukrainian war, with an emphasis on information operations and their underestimated danger in Europe. The authors prove that Russia's cyberattacks are part of its military strategy, combining traditional and digital means of warfare, including information campaigns, disinformation, attacks on critical infrastructure, economic espionage, and the use of cryptocurrencies to finance illegal activities. Cases of attacks on Ukrainian energy networks, examples of the use of deepfake technologies, and the latest manifestations of online fraud related to the war are considered. The legal regulation of cyber operations is analyzed in the context of international humanitarian law (IHL), the Budapest Convention, and the new UN Convention on Cybercrime. Particular attention is paid to the Tallinn Manual as a tool for the legal qualification of cyberattacks as an act of armed aggression. The authors emphasize the need to develop new legal concepts (cyberwar, cyberpropaganda, information operations) and create effective mechanisms to counter organized cybercrime at the international level. Ukraine's experience in cooperation between the state and civil society in cyberspace is presented as an example of effective counteraction to hybrid threats. The purpose of the article: to show what are the trends in cybercrime during war with a focus on information operations, the danger of which is still underestimated in Europe. To justify the need to regulate organized cybercrime within the framework of cyberwar.

Keywords: cyberwar, Russian-Ukrainian war, information campaigns, cybercrime.

1. Introduction

The information space is the new training ground for modern wars. The Russian war against Ukraine has many dimensions: conventional, economic,

cyber, informational, cultural (https://cip.gov.ua/ua/news/kiberataki-artileriya-propaganda-zagalnii-oglyad-vimiriv-rosiiskoyi-agresiyi). During the world's first large-scale cyberwar, no new "weapons" were discovered in cyberspace. Attacks are carried out using previously known mechanisms, and have long been categorized and have clear recipes for confrontation. Cyberattacks fully comply with the general military strategy of Russia. War is a continuation of the state's policy by other means, including in the information and cyberspace. Cyberattacks are often coordinated with other attacks: conventional ones on the battlefield, as well as with information-psychological and propaganda operations. For example, at the end of 2022, when, after a series of cyberattacks on the energy sector, the Russian Federation launched several waves of missile attacks on energy infrastructure and simultaneously launched a propaganda campaign aimed at shifting responsibility for the consequences (power outages) to Ukrainian state authorities, local governments or big Ukrainian business. Such coordination of attacks in different dimensions of aggression is very common, although coordination is not an absolute rule.

Doctrinally, the Russian Federation often considers the cyber and information dimensions as a single domain of "information confrontation". This confrontation can include either purely information campaigns or something more complex. However, the goal in any case is information manipulation, to which all democratic regimes are naturally vulnerable. Cyberattacks, like conventional attacks by the Russian Federation, do not recognize any rules – infrastructure, humanitarian organizations, private and state-owned companies are under attack. Russian hackers do not accept restrictions and do not recognize borders, attacking different states if they help Ukraine. Therefore, in order to effectively counter authoritarian regimes using the example of the Russian-Ukrainian war, it is necessary to introduce the required legal definitions and adapt military doctrines to modern challenges.

The multidimensionality of Russian aggression manifested itself even before the full-scale invasion. Examples are the so-called "economic wars" and powerful hostile propaganda campaigns. But it was since February 24, 2022 that the correlation between different types of attacks became systemic. This tactic was practiced by Russia in previous armed conflicts (for example, during the aggression against Georgia). That is, if it is not studied and effectively resisted, this tactic will be used in the future against other states. If Russia does not receive a worthy response to all its aggressive actions today, tomorrow it will return with even more audacious attacks that will not be limited to Ukraine (https://cip.gov.ua/ua/news/kiberataki-artileriya-propaganda-zagalnii-oglyad-vimiriv-rosiiskoyi-agresiyi).

2. Analysis of the current situation

In the period leading up to Russia's full-scale invasion of Ukraine on February 24, 2022, the actions of Russian state actors, in particular the Sandworm group, which is suspected of carrying out a number of aggressive cyberattacks against Ukrainian state institutions, military structures, and civilian infrastructure, played an important role. Among such attacks was the NotPetya malware, which had the characteristics of "ransomware" software, which was spread in 2017. It initially targeted Ukrainian government and commercial networks, but later spread beyond Ukraine, causing damage in various countries worth about $10 billion. The conflict between Russia and Ukraine has also been accompanied by large-scale cyber sabotage, in particular against critical infrastructure. In December 2015 and December 2016, the BlackEnergy and Industroyer malware caused a shutdown of part of the Ukrainian power grid, leaving hundreds of thousands of citizens without electricity.

Following the start of full-scale Russian aggression in 2022, Russia-related cyber operations continued. They included DDoS attacks, the use of malware, including so-called "vipers", and the hacking of the ka-Sat satellite network, one of the most notable incidents in this area. In response, since February 24, 2022, there has been an increase in the activity of non-state actors acting in support of Ukraine in cyberspace. These include, in particular, the "Cyber guerrillas of Belarus", the "IT Army of Ukraine", as well as individual proactive (Biggio 2024). Analysis of Russia's further cyber activities have shown that Russia is still using DDoS attacks and malware codes to disrupts operation of Ukrainian government, banks and some prominent private companies without major impact (Štrucl 2022).

Head of the Cyber Police Department of the National Police of Ukraine Yuriy Vykhodets reported that in 2024, law enforcement officers exposed and documented nine criminal organizations. "Also, 2.5 thousand cyber crimes were registered based on the materials of the Department's employees. Thus, almost 2 thousand suspects were informed of their suspicions, who are accused of committing 3.5 thousand criminal offenses. At the same time, the victims were provided with compensation of more than 168.6 million hryvnias". Thus, in 2024, 57 organized groups (9 of them are criminal organizations) were neutralized in the direction of countering organized cyber crime, which included 254 participants who committed more than 1 thousand crimes (https://cyberpolice.gov.ua/news/zvitpro-diyalnist-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u--roczi-7074/).

In today's world, the line between state and criminal actors is blurring. The SOCTA report notes that cybercriminal groups often operate under the cover of or in collaboration with states, carrying out politically motivated missions in exchange for immunity or benefits. In the case of Ukraine, we observe a symbiosis between information warfare, cyber espionage, sabotage, and economic damage, which fits into the concept of organized state cybercrime, which SOCTA warns about. EU Serious and Organised Crime Threat Assessment 2025 shows that there is an increase in politically motivated cyber-attacks against critical infrastructure and public institutions, originating from Russia and countries in its sphere of influence. Politically motivated cyber-attacks demonstrate precisely how the three elements of the DNA of crime work in tandem, completely changing the criminal landscape. Cyber-attacks are increasingly directed by networks and agents based outside EU external borders. Digital platforms and tools provide the perfect breeding ground for illicit activities. Cutting-edge technologies are making attacks faster, smarter, and more devastating than ever (https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime).

In January 2024, Ukrainian law enforcement, with the support of Europol, arrested an individual believed to be the mastermind behind a sophisticated cryptojacking scheme that used compromised computers to mine cryptocurrency (Europol Press Release, 12 January 2024). Ukrainian investigators are also looking into the suspect's potential involvement in pro-Russian hacker groups IOCTA (https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024).

3. Cybercrime trends in the framework of the Russian-Ukrainian war

One of the most common and relevant tools for carrying out cybercriminal activities, taking into account the specifics of the war in Ukraine, are attacks on critical infrastructure. In order to influence the course of the war and the mood of society, cybercriminals can carry out **attacks** on energy, transport, financial and telecommunications systems and other critically important infrastructure facilities, which ultimately can have catastrophic consequences for the stable functioning of the state. Thus, according to the State Service for Special Communications and Information Protection of Ukraine, since the beginning of the Russian invasion of Ukraine, the number of cyberattacks on critical infrastructure has increased by 400% compared to the pre-war years. In 2022 alone, cybercriminals associated

with Russian hacker groups carried out a number of attacks on Ukrainian energy infrastructure, among which attacks on energy network operators accounted for a significant share. An equally important and widespread component of cybercriminal activity in wartime is **information campaigns** aimed at spreading false information, manipulating social networks, creating fake news, and undermining trust in official sources of information. This activity is becoming an integral part of modern psychological operations aimed at destabilizing society. According to the State Service for Special Communications and Information Protection of Ukraine, in 2022 alone, the number of cyber incidents in Ukraine increased by 2.8 times, and the number of disinformation campaigns exceeded 200. In the context of the active development of digital currencies, cryptocurrencies are beginning to play a significant role in financing illegal operations. According to a FATF study, in 2022, the share of cryptocurrency transactions related to illegal activities increased to 2.1%. The rapid growth of the role of cryptocurrencies in criminal activity in the digital space is due to the complexity of tracking transactions and constant changes in their implementation schemes. This significantly complicates the work of law enforcement agencies in the fight against financial crimes and raises the issue of developing new tools and approaches to regulating these processes. The results of a study conducted by the European Banking Authority show that one of the main problems in controlling the use of cryptocurrency is the lack of a harmonized legal framework. The rapid development of blockchain technologies leads to the fact that regulators do not have time to adapt their legislative initiatives to the realities of the functioning of the financial system, thereby creating favorable opportunities for criminals to use cryptocurrency for illegal financial transactions. Innovative technologies have a significant impact on the effectiveness of timely identification of criminal transactions in cyberspace. Cybercriminals' active use of artificial intelligence, machine learning and automated attacks allows them to increase the effectiveness of their actions and avoid punishment (Pelih 2024).

4. Cyberattacks on critical infrastructure

The rapid adoption of GenAI harkens back to another global phenomenon with a similar path of destruction: unregulated social media. To that end, we see significant urgency from governments around the world, eager to not repeat the same mistakes with GenAI. In March 2023, the European Union passed the Artificial Intelligence Act and eight months later, the United States issued an executive order 14110 or EO for Safe,

Secure, and Trustworthy Development and Use o Artificial Intelligence. The message is clear: The responsibility for the safe usage of AI-powered tools lies squarely on the provider and users – with hefty penalties for misuse. The providers are responding in kind. OpenAI is delaying the release of Sora AI to ensure content provenance and to enable users to identify real vs. increasingly real-looking but fake videos. Deepfakes put us all at increasing risk of widespread mis- and disinformation, phishing and vishing attacks, breaches, data loss, regulatory fines, and reputational damage at scales previously unknown to us (Threat Landscape Report 2024).

During wartime, the most common targets of cyberattacks are government agencies, military facilities, and law enforcement agencies. As a rule, the purpose of these attacks is to collect intelligence information, disrupt communication and order. Stealing confidential data from government structures or military plans allows the adversary to obtain critically important information for predicting military actions and undermining the country's defense capabilities. The attacks focused on the psychological effect, rather than completely disabling critical systems (Bányász et al. 2024).

It should also be noted that due to the unscrupulous behavior of some c'tizens, the enemy can find certain information simply in social networks, open sources and messengers. There is no need to do complex cyber operations, sometimes the enemy can simply Google a lot of important information. In addition to scammers, the danger is also posed by hacker attacks (https://cyberpolice.gov.ua/article/xakerski-ataky-ta-yak-vid-nyx-zaxystytysya-rekomendacziyi-kiberpolicziyi-7865/) by Russia. They target government institutions, critical infrastructure, financial systems and even individual citizens. «Cyber attacks are part of the war where attackers try to attack critical infrastructure, steal important information, destroy data or disrupt the functioning of online resources important to Ukrainians» (https://mvs.gov.ua/news/internet-saxraistvo-v-mvs-rozpovili-pro-metodi-protidiyi).

5. Information companies

Another serious problem is information attacks and the spread of disinformation, which undermine trust in official sources of information and contribute to the demoralization of society. We argue that information manipulation and relevant operations should be considered a cybersecurity threat, since such operations directly affect at least one of the three components of the information security model and in particular that of integrity of information, as well as other cybersecurity principles (such as authentic-

ity and accountability) and leverage on other types of cybersecurity tactics, techniques and procedures (ENISA's Threat Landscape 2023).

It has already been scientifically proven how the Russian Federation teaches GPT chat with its propaganda, distorted history and fakes (https://www.newsguardrealitycheck.com/p/a-well-funded-moscow-based-global). Little academic attention has been paid to Russia's use of artificial intelligence to influence the Ukrainian military through information and psychological operations.

In March 2022, a fabricated video surfaced online purporting to show Ukrainian President Volodymyr Zelensky urging Ukrainian soldiers to lay down their arms and surrender to Russian forces. The video was posted on the website of the Ukraine 24 television channel, which was hacked. In the video, Zelensky looked unnatural: his head was disproportionately large and his voice sounded unnaturally deep (https://www.bbc.com/news/technology-60780142?utm_source=chatgpt.com). Ukrainian authorities quickly denied the video. President Zelensky published an address in which he called the deepfake a «childish provocation» and assured that Ukraine would not capitulate. Many news companies were accompanied by coordinated bot attacks to spread disinformation (https://www.businessinsider.com/volodymyr-zelenskyy-deepfake-video-surrendering-ukraine-russia-forces-20223?utm_source=chatgpt.com).

In 2024, NewsGuard research uncovered a Russian network called "Pravda" that used AI chatbots to spread disinformation. The network consisted of over 150 news sites that published false narratives, including the alleged existence of US bio-labs in Ukraine and President Zelensky's misuse of military aid. These fake messages were aimed at influencing Western AI models, which sometimes repeated these disinformation claims. Ukraine's armed forces need significant support from the West to have the resources and technological capabilities to adequately defend against Russia's use of AI in influence operations. Ukraine can effectively defend itself against Russia's continued attacks using AI in the information space only by working closely with partners.

6. Online Financial Crimes. Cryptocurrency, Laundering, Fraud, Drops

Economic instability and the active use of cryptocurrencies are factors that contribute to financial crimes. Since the beginning of the war, the number of crimes related to "money mule" or drop schemes has increased sig-

nificantly. The drop mechanism works according to a simple but effective model. Fraudsters recruit people through social networks or advertisements for "easy work", after which they ask to open a bank account or transfer data to an existing one. Funds obtained illegally pass through these accounts. According to cyber police, the number of such crimes has increased by 40% since the beginning of the war compared to the pre-war period. Money mules were used in schemes of fake charity collections "at the Armed Forces of Ukraine", in fake online stores, crypto fraud and transfers through international money laundering services.

Many citizens still do not understand that they can easily become accomplices in crimes. The number of fraudulent schemes is growing, and criminals are constantly improving their methods. At the same time, effective protection is possible if users follow the basic rules of cybersecurity: verify information, do not transfer confidential data to third parties, and use reliable account protection tools.

In this study, we will only look in more detail at new types of cybercrimes related to the Russian-Ukrainian war. Today, Ukrainians are being robbed of their WhatsApp accounts. Attackers send messages on WhatsApp, urging people to vote for an electronic petition to posthumously award the title of "Hero of Ukraine" to servicemen of the Armed Forces of Ukraine. The messages contain a link to a fake website that imitates the official website of "Electronic Petitions". As a result, the victim follows the link in the fake message and ends up on a website where they need to enter their phone number and receive a code. The victim enters the code in WhatsApp to "add a trusted device". Attackers gain access to the victim's WhatsApp account. Attackers can read your messages, see your photos and videos and send messages in your name. Russian special services continue to attempt to destabilize the situation in the country by recruiting Ukrainian citizens to commit illegal actions in favor of the aggressor country.

7. Conventional dimension of cyberwarfare

The Geneva Conventions of 1949 and the Additional Protocols of 1977 are key legal instruments and concern the protection of civilians in armed conflict. If cyber operations result in physical harm to civilians or civilian objects, they may fall under IHL regulation. There is considerable debate as to whether cyber attacks can be equated with attacks under IHL if they cause damage to critical infrastructure.

The main aim of IHL is to regulate warfare as to avoid any harm to civilians and non-combatants. But IHL needs support from the global com-

munity in achieving this in the sphere of cyberspace. Cyber-attacks have proved their deadly capacity to be employed as effective weapons and cyber-attacks are here to stay (Bokil 2023).

The Budapest Convention on Cybercrime (officially the Council of Europe Convention on Cybercrime, 2001) sets out a clear list of offences that member states must criminalise in their national legislation. It covers four main categories of cybercrime:

I. Offences against the confidentiality, integrity and availability of computer data andsystems: unauthorised access to computer systems (art. 2) – hacking; unauthorised interception of data (art. 3) – for example, interception of e-mail or internet traffic; unauthorised interference with computer data (art. 4) – deletion, corruption, alteration of data; unauthorised interference with a system (art. 5) – attacks affecting the functioning of computers or networks. Misuse of devices (Article 6) – creation, sale or distribution of means for committing the above-mentioned crimes (for example, hacking programs).

II. Computer-related crimes (Articles 7–8): Computer data forgery (Article 7) – creation or use of false data for the purpose of deception. Computer fraud (Article 8) – use of a computer to obtain material benefit by deception.

III. Content-related crimes (Article 9): Child pornography – creation, distribution, storage of child pornography.

IV. Copyright infringement crimes (Article 10): Violation of copyright and related rights using computer systems. (Buçaj, Idrizaj 2024).

There are different views on the Russian-Ukrainian war from the perspective of cyber activity as cyberwar, since legal regulation depends on certain criteria, such as the nature of the conflict (internal, international, NIAC); the type of cyber operations (attack, information campaign, espionage); the status of the perpetrators (state/non-state actors) (Stinissen 2015). Non-state actors play a critical role in cyber conflicts. The mixed nature of the conflict (cyberwar + conventional war + hacktivism) requires new approaches to cybersecurity. Although the Budapest Convention is not specifically designed to regulate cyber operations in armed conflict, it can be partially applied to analyze cyber attacks that have the characteristics of a criminal offense, even in the context of war. Information campaigns can be covered by this convention if they include, for example, unauthorized access.

Russia is not a party to the convention, so it is not obliged to cooperate, investigate or extradite suspects. The convention does not regulate the actions of states in armed conflicts (e.g., cyberattacks as a means of aggression).

8. UN Convention

The new UN Convention against the Use of Information and Communications Technologies for Criminal Purposes, which was adopted by the UN General Assembly in January 2024 (also known as the UN Convention on Cybercrime), has been the subject of serious debate in the international legal community, as it differs significantly from the Budapest Convention in both approach and objectives.

The main differences and innovations of the new UN Convention are, first of all, in the broader list of criminalized acts. These include: fraud, money laundering, terrorist activities using ICTs, dissemination of information that may be regarded as extremist or subversive, illegal content, including fakes or "unwanted information" (which raises concerns about freedom of expression), and attacks on "public order" through ICTs (a vague formulation that may allow states to prosecute opposition online content). The Convention gives state parties the right to independently determine what constitutes a crime related to the use of ICTs; to restrict the transfer of data and information to other states, which may create barriers to international cooperation; to restrict access to content for reasons of national security or morality. Although the UN Convention on Cybercrime does not require intentional participation in the offences established under the Convention, Article 19 already requires intent. This creates a risk that in some Member States online intermediaries could be held liable for information disseminated by their users, even without actual knowledge or awareness of the illegal nature of the content – in contrast to the approach adopted in the EU for digital services. Such a risk could encourage overly broad content moderation measures by platforms, which would harm freedom of expression and could disproportionately affect marginalised communities. Furthermore, Article 18 of the UN Convention is much broader (referring to "participation") than the corresponding article in the Council of Europe Budapest Convention on Cybercrime (which provides that the offence must be "committed in the interests of cooperation") and lacks the clarification provided for in paragraph 125 of the Explanatory Report to the Budapest Convention (https://www.hrw.org/news/2024/10/21/eu-member-states-should-vote-no-un-cybercrime-treaty).

If we talk about the role of the Convention in the context of cyberwarfare and information campaigns, then Ukraine will be able to use the Convention's mechanisms for the international search for participants in Russian cyberattacks, if they operate from participating countries. But if clear human rights guarantees are not spelled out, then Russia will be able

to use the Convention to legitimize the persecution of activists or the «cyber army» of Ukraine. The UN Convention against Cybercrime was adopted by the UN General Assembly on December 24, 2024, but has not yet entered into force.

9. Regulating Organized Cybercrime in the Context of Cyberwar

One of the most significant contributions to the attempt to regulate organized cybercrime in the context of cyberwar was the publication of the Tallinn Manual (Tallinn Manual on the International Law Applicable to Cyber Warfare 2013; Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 2017). In the 2013 and 2017 editions, it is mentioned as the main international legal document that helps interpret the application of international law to cyber operations (Jensen 2016). The Tallinn Manual helps to analyze these attacks as "use of force": some large-scale cyberattacks can be qualified as use of force if they have consequences similar to an armed attack (for example, disabling energy systems, causing casualties). The issue of distinguishing civilian and military objects and how to legally prove that the attack was carried out by the state (Russia), and not by hacktivists or private groups, is still difficult. The complexity of the analysis and qualification also lies in the combination of cyberattacks with information campaigns, fakes, and manipulation of public opinion.

Issues related to the qualification of non-state cyber actors involved in international armed conflict. The problems arise mainly because the norms of international humanitarian law are largely shaped by the historical context in which they were created. This leads to difficulties in applying these norms to new scenarios of warfare that have emerged in recent years and threaten international peace and security, in particular through new means of warfare such as cyber operations.

This is confirmed, in particular, by analyzing the applicability of Article 4 (A) of the Third Geneva Convention: this article seems not entirely suitable for the modern military context due to the strict requirements it imposes, which make it impossible to qualify the Anonymous collective as combatants. Having rejected this possibility and, accordingly, having established that the Anonymous group belongs to the category of "civilians", we asked ourselves the question: can the concept of "direct participation in hostilities be used to describe their actions?".

The Tallinn Manual is a fundamental interpretative tool that facilitates the legal qualification of hackers involved in armed conflicts by offering a less strict interpretation of the requirements set out in these recommendations. This should not be surprising, given that the Tallinn Manual – unlike other legal instruments – was specifically designed for cyberspace and its specificities. In conclusion, regulating new warfare scenarios, including cyberspace, requires the development of new rules that take into account the latest weapons and the consequences they may cause, in order to ensure international security (Galloro, Guida 2024).

In this article, the Tallinn Manual's analytical framework will be used to determine whether the cyberattacks in the Russia-Ukraine conflict constitute force usage under international law. The key problems in this analysis are the assessment of the severity of the attack and the involvement of the state. Specifically, we will examine these two elements to argue whether the cyberattack launched by Russia just before invading Ukraine, constitute the use of force. It should be noted that although the Tallinn Manual has been the subject of much controversy and is only a research work that does not represent the views of any country or organization, its influence cannot be ignored. Some countries have recognized the legal status of the Tallinn Manual and used it as an important reference standard for policy making (Leng 2023).

The Tallinn Manual and Tallin Manual 2.0 both analyze extensively the legal implications of cyber-operations in the context of international law and nation states. The popular vision of cyber-war is one in which critical infrastructure, telecommunications, the internet and all connected systems are completely shut down, effectively crippling society (MacDonald 2022).

10. Conclusion

The topic of the study is deep and complex. Cyberattacks are a weapon in war, and the types and mechanisms of their implementation have long been known, DDOS attacks, ransomware, data collection or damage. But we should not underestimate information campaigns as a type of cybercrime. Such campaigns significantly affect not only the polarization of society and the imbalance of the state as a whole, but also the results of elections and the stability of states as a whole.

Ukraine's experience is important in regulating organized cybercrime within the framework of cyberwar. The example of interaction between law enforcement agencies and civilians is an unprecedented example of effective

counteraction to Russian disinformation campaigns and cyber propaganda (Mazepa 2024). The Tallinn Manual, together with the Budapest and new UN Conventions on Cybercrime, create a legal basis for qualifying many cyberattacks as use of force and criminal acts, which requires further harmonization of international humanitarian law. Key challenges remain the issues of attribution of attacks, distinction between military and civilian targets, ensuring a proportionate response, and jurisdiction over cybercriminals.

In the future, it is necessary to:

- Clearly define and enshrine in national and international law the concepts of information operations, cyberwarfare, and cyberpropaganda;
- Develop a mechanism for regulating organized cybercrime in armed conflicts;
- Deepen international cooperation to exchange data, conduct joint investigations, and implement common standards to counter digital threats.

Only by combining a clear legal framework with technological and organizational measures can the international community effectively counter the evolution of cybercrime and protect democratic institutions from new hybrid threats.

REFERENCES

Literature

Bányász, Péter and Adrienn Kiss, Sándor Magyar, Dávid Kiss (2024): "Empirical analysis of the cyberattacks of the Russian-Ukrainian war". In: Információs Társadalom 24 pp. 9–32. DOI: 10.22503/inftars.XXIV.2024.2.1.

Biggio, Giacomo (2024): "The Legal Status and Targeting of Hacker Groups in the Russia-Ukraine Cyber Conflict". In: Journal of International Humanitarian Legal Studies 15, pp. 142–182.

Bokil, Rohit (2023): "Cyber Warfare: Taking War to Cyberspace and its Implications for International Humanitarian Law". In: International Journal for Multidisciplinary Research vol. 5, n. 1, pp. 1–12.

Buçaj, Enver and Idrizaj, Kenan (2024): "The need for cybercrime regulation on a global scale by the international law and cyber convention". In: Multidisciplinary Reviews, 8(1), 2025024. DOI: https://doi.org/10.31893/multirev.2025024.

ENISA's Threat Landscape and the Effect of Ransomware 2023.

Europol Press Release, 12 January 2024, 'Cryptojacker arrested in Ukraine over EUR 1.8 million mining scheme'. Internet Organised Crime Threat Assessment (IOCTA) 2024.

Galloro, Laura and Guida, Martina (2024): *Legal Status of Hackers under International Humanitarian Law: The Case of Anonymous.* Prague Law Working Papers Series, Imprint: Charles University in Prague.

Jensen, Eric Talbot (2016): "The Tallinn manual 2.0: Highlights and insights". In: Georgetown Journal of International Law, 4, pp. 735–778.

Leng, Yaxuan (2023): "When Can Cyberattack Constitute Use of Force: A Case Study of Cyberattack in the Russia-Ukraine Conflict". In: Lecture Notes in Education Psychology and Public Media, 17, pp. 201–207. DOI: 10.54254/2753-7048/17/20231249.

MacDonald, Abby (2022): "What About Cyber-War? What We Have Seen and Not Seen in the Russo-Ukrainian War". In: Policy Perspective, pp. 1–9.

Mazepa, Svitlana (2024): "War, Hate, Propaganda and the Internet: A Dangerous Combination". Springer Nature Switzerland, Imprint: Springer.

Pelih, Matvi (2024): "Mechanisms of Cyber Criminal Activity Development during Wartime". In: Development Service Industry Management 3, pp. 219–222. DOI: 10.31891/dsim-2024-7(32).

Raport CyberArk 2024 Identity Security Threat Landscape EMEA.

Stinissen, Jan (2015): "A legal framework for cyber operations in Ukraine". In: Kenneth Geers (ed.), Cyber War in Perspective: Russian Aggression, pp. 123–134.

Štrucl, Damjan. (2022): "Russian Aggression on Ukraine: Cyber Operations and the Influence of Cyberspace on Modern Warfare". In: Contemporary Military Challenges 24, pp. 103–124. DOI: 10.33179/BSV.99.SVI.11.CMC.24.2.6.

Tallinn Manual on the International Law Applicable to Cyber Warfare (2013). Prepared by the International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence, ed. Michael N. Schmitt. Publisher: Cambridge University Press.

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2017). Prepared by the International Groups of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence, ed. Michael N. Schmitt. Publisher: Cambridge University Press.

Websites (accessed April 4, 2025)

https://cip.gov.ua/ua/news/kiberataki-artileriya-propaganda-zagalnii-oglyad-vimiriv-rosiiskoyi-agresiyi

https://cyberpolice.gov.ua/article/xakerski-ataky-ta-yak-vid-nyx-zaxystytysya-rekomendacziyi-kiberpolicziyi-7865/

https://cyberpolice.gov.ua/news/zvitpro-diyalnist-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u--roczi-7074/

https://mvs.gov.ua/news/internet-saxraistvo-v-mvs-rozpovili-pro-metodi-protidiyi

https://www.bbc.com/news/technology-60780142?utm_source=chatgpt.com

https://www.businessinsider.com/volodymyr-zelenskyy-deepfake-video-surrendering-ukraine-russia-forces-20223?utm_source=chatgpt.com

https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime

https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024

https://www.hrw.org/news/2024/10/21/eu-member-states-should-vote-no-un-cyber crime-treaty

https://www.newsguardrealitycheck.com/p/a-well-funded-moscow-based-global