developments almost entirely fail to take into account the requirements of social solidarity, instead placing their emphasis on individual human rights.

The Ukrainian recovery plan should be based on the RBC approach. For these purposes, following the UNGPs, the governmental agencies responsible for providing financial funds and other forms of cooperation with the private sector as part of the Ukraine's recovery effort should guide companies towards:

(a) publicly affirming their support for democracy, the rule of law, solidarity, fundamental human rights and territorial integrity;
(b) publicly committing to exercising their leverage responsibly, both within their value chains (supporting business partners in building human rights capacities) and in governmental relations (ensuring that companies do not lobby for policies that protect their operations while shifting burdens onto the most vulnerable), in particular by including in the company's human rights policy the commitment not to influence the political and regulatory sphere in an irresponsible way;
(c) having a responsible exit strategy as part of their human rights policy based on consultations with workers and external stakeholders, with disengagement as a last resort;
(d) developing and adopting policies on the work, family and volunteering balance.

In the recovery agenda of Ukraine, the BHR approach is important as it can provide a systematic framework for when and how a company has an obligation to do something more than simply provide respect or do no harm. The example of Ukraine is particularly telling because it creates a real sense of urgency to do something. In this regard, a coherent understanding of solidarity has a clear link with the concept of dignity, but also, arguably, a transnational and transgenerational dimension. This understanding should be reflected by all governmental recovery actions in Ukraine. In particular, ensuring competitive access to funding and growing value by adding sectors of the economy should be seen as critical projects in the recovery plan, which itself should be based on the RBC approach.

3.8. The Role of Cyber Defence and the Problems It Faces in the Context of Aggression

3.8.1. The Concept of Cybersecurity in the Conditions of War Within the Geopolitical Processes of Today

Cybersecurity (along with which the terms *cyber defence* and *cyber protection* are used interchangeably) is a relevant and extremely important component of the

modern national security of every state. In the modern world, in which the digital space has become a necessity for the functioning of all spheres of society as well as an object of interest for potential threats, the issues of cybersecurity and countering cybercrime acquire special importance. In the context of Ukraine, which is experiencing geopolitical instability and fighting for its territorial integrity in the conditions of a war of aggression, the problems of cyber defence become extremely urgent and difficult.

Cyber threats evolve constantly. Thus, understanding the problems of cyber defence and its role in Ukraine can determine the further direction of policy in this area and contribute to the preservation of national security and the country's sovereignty.

This analysis starts by assessing global cyber defence problems, including in Ukraine, before identifying modern threats, outlining the main challenges that Ukraine faces, and assessing the role and functions of cyber defence in managing these challenges at the legislative level, taking into account current norms and gaps in the legal framework.

The problem of cybercrime in Ukraine has been studied by many researchers. In particular, V. K. Kharchenko, O. M. Klymchuk, O. G. Korchenko, and Yu. P. Travnikov paid special attention to cyber terrorism and cybersecurity. I. O. Chernukhin, O. D. Dovgan, and V. M. Bogush studied the organisational and legal principles that underlie the organisation of the cyberattack protection systems that guard critical infrastructure.

Some aspects of the regulatory framework for combating cybercrime were studied and discussed in publications by K. Beliakov, V. Butuzov, A. Volevodz, D. Havlovskyy, V. Holubev, V. Huslavskyy, D. S. Klyotskin, M. Litvinov, E. Ryzhkov, V. Rozovskyy, T. Tropyna, V. Tsymbaliuk, O. Yukhno and others.

This part of the study aims to analyse and comprehensively investigate the problems of cyber defence by first assessing the insecurity associated with gaps in the current legislation and the crucially important role of cyber defence in war conditions. It then attempts to determine the possibilities of countering cybercrime in wartime conditions through the prompt exchange of experience at the international level and the improvement of current legislation.

3.8.2. Modern Concepts of the 'fourth branch of government' and Its Impact on the Global Social and Political Climate, Legal Control and the Regulation of the Virtual World

Concepts related to digital and electronic communications are closely intertwined with the global information infrastructure. More and more specialists,

lawyers, scientists and politicians are turning to issues of state cybersecurity. This is not surprising, since this is a new sphere of social relations in which the participants – the state and society – are inextricably linked. Regarding the definition of cyberspace, at the 32nd session of the UNESCO General Conference (2003), the Recommendation concerning the Promotion and Use of Multilingualism and Universal Access to Cyberspace was adopted, according to which cyberspace was defined as a virtual world of digital and electronic communication related to the global information infrastructure.

In global law enforcement practice, the concept of cyberspace began to appear at the end of the 20th century. In this context, the definition of cyberspace provided by the Supreme Court of the United States is indicative: this is a unique medium known to its users as cyberspace, which is not located in a certain territory but is accessible to everyone in any part of the world via the Internet (*Reno v. ACLU* 1997).

Finally, in 2013, the NATO published the Tallinn Manual on International Law on Methods of Conducting Cyber Warfare, which defines cyberspace as an environment made up of physical and non-physical elements and characterised by the use of computers and the electromagnetic spectrum to store, modify and exchange data using computer networks (Tallinn Manual on the International Law Applicable to Cyber Warfare 2013).

Therefore, cyberspace can be characterised as a specific environment, which, although created by a human, has received such significant and rapid development due to its globalisation that new forms of legal relations arise in it, which are currently insufficiently researched and regulated in either international or national law.

In recognising cyberspace as an environment for the application of geostrategies and the 'fifth bridgehead' for conducting hostilities, along with land, sea, air and space, more and more attention is paid to the development and protection of information resources, as well as opportunities to influence the information resources of other countries, which in general is described as a problem of ensuring the cybersecurity of the state. Now, the use of cyber armies and cyber weapons, cyber defence, cyber operations and cyberattacks by states is perceived as commonplace.

The analysis and generalisation of the approaches of the world's scientific institutions to the problems of the use of cyberspace allows us to state that the assessment of the capabilities of each country is carried out according to seven factors: (1) the presence of a national cybersecurity strategy; (2) the availability of structures responsible for incidents and their ability to respond to them; (3) the presence of a law enforcement cyber structure and the state of law enforcement practice; (4) the availability of an information exchange system; (5) the

availability of a system of personnel training, research and testing; (6) diplomacy and trade; and (7) defence and the availability of structures responding to crisis situations. The USA is identified as the leading country in the development of cyber capabilities around the world across all indicators.

Since 2014, Ukraine has been forced to retaliate against hybrid Russian armed aggression, including in cyberspace. State policy in the field of cybersecurity addresses a number of concerns. The main challenges relate to the legislative framework – namely, the inconsistency or lack of definition of cybersecurity terms, which creates problems in the regulation of such crimes in the legal field. Another important issue is the lack of progress on the part of the state in cyberspace defence systems, along with the lack of cooperation between the state and the private sector in the above-mentioned area. A rather important element of this lack of progressive development is the lack of initiative on the part of the state to create highly qualified personnel in the field of IT. Insufficient interest in the education of personnel leads to an outflow of personnel to foreign countries.

For a fully fledged analysis of this situation, it is also appropriate to recognise that today, along with unresolved personnel, financial, logistical and regulatory problems, there is another, more complex issue regarding the strengthening of the state's cyber defence and the creation of effective Cyber Troops of the Armed Forces of Ukraine. This problem concerns the rejection of the comprehensive consideration of cyber defence issues, mostly through the prism of the implementation of cyber protection and cybersecurity measures of the Armed Forces of Ukraine and their acquisition of capabilities to fulfil the tasks of the comprehensive defence of the state – primarily its cyber defence both within and through cyberspace (Ternovyy *et al.* 2023).

Cyber defence was recognised as an important new component of Ukraine's defence only in the Cybersecurity Strategy of Ukraine (2016). With the introduction of the new National Security Strategy of Ukraine (2020), a start was made on the preparation of drafts of a number of strategic documents, one of which is the Cybersecurity Strategy of Ukraine. This strategy, which was adopted by Presidential Decree No. 447/2021 (2021), implemented the decision of the National Skill Development Corporation (hereafter – NSDC) 'On the Cybersecurity Strategy of Ukraine' (NSDC 2021).

The Cybersecurity Strategy of Ukraine determines: the priorities of national interests in the field of cybersecurity; existing and potential cyber threats; the goals and tasks of ensuring the cybersecurity of Ukraine with the aim of creating conditions for the safe functioning of cyberspace; and the use of cybersecurity in the interests of the individual, society and the state (NSDC 2021).

This Strategy notes that 'ensuring cybersecurity is one of the priorities in the national security system of Ukraine. The implementation of the specified priority is carried out by strengthening the capacities of the national cybersecurity system to counter cyber threats in the modern security environment' (NSDC 2021). The implementation of the norms of the Strategy involved: the improvement of the operation of cyberspace; its control with the help of high-tech, innovative technical means and mobile responses in the preparation, processing and entry into force of improved norms, both in the current legislation and through the development of new normative legal acts in the area of cyber protection; ensuring maximum control; the implementation of the perfect means of deterrence; countermeasures; and the detection of criminals and bringing them to justice (NSDC 2021).

This Strategy is based on the provisions of the Constitution of Ukraine, the laws of Ukraine 'On the National Security of Ukraine' (2018) and 'On the Basic Principles of Ensuring Cybersecurity of Ukraine', the ECHR, the Convention on Cybercrime, the National Security Strategy of Ukraine, approved by the Decree of the President of Ukraine No. 392 (2020), the Concept of Combating Terrorism in Ukraine, approved by the Decree of the President of Ukraine No. 53 (2019), and other normative legal acts.

Thus, the Strategy provides for:

(1) the regulation of electronic evidence issues at the legislative level, using the best practices on these issues of the USA and EU Member States and taking into account modern challenges and trends in the field of cybersecurity;
(2) the regulation at the legislative level of the legal status of cryptocurrencies;
(3) the settlement at the legislative level of the issue of the comprehensive involvement of the private sector and civil society in the implementation of measures to curb destructive activities in cyberspace;
(4) the regulation at the legislative level of the issue of public-private partnership in the field of cybersecurity, determining the forms and methods of implementing such a partnership, strengthening mutual trust and foreseeing the possibility of introducing experimental projects in this area (Hutsalyuk 2023, p. 110)

The National Cybersecurity Manual of the NATO Cooperative Cyber Defence Centre of Excellence summarises the understanding of cybersecurity by NATO member states (Klimburg 2012).

In general, the term cybersecurity is understood to represent maintaining a state of readiness to repel potential threats with high intensity and the adoption of appropriate countermeasures. Experts from the NATO Cyber Defence Centre

consider the militarisation of the Internet as one of the main and most dangerous trends in the development of global cyberspace: 'Modern military structures are ready to use the information space as a "parallel battlefield" in future conflicts'. At the same time, confidence is expressed that a cyberattack 'in its pure form' is unlikely (Zavhorodnya 2022, p. 64).

In October 2017, the Law of Ukraine 'On the Basic Principles of Ensuring the Cybersecurity of Ukraine' entered into force, in which two key terms were established for the first time. Before this, there were no legal definitions of the terms *cybersecurity* and *cyber protection* in the current legislation of Ukraine. In accordance with the norms of this law, cybersecurity provides for the protection of the vital interests of a person, citizen, and society in cyberspace, and must ensure the sustainable development of the information society and digital communication environment. The legislator paid careful attention to the importance of a prompt response, the timeliness of detection, and the neutralisation of both real and potential threats to the national security of Ukraine in cyberspace.

The legislator formulates cyber defence as a set of measures aimed at preventing cyberattacks in cyberspace aimed at ensuring the protection of the sovereignty and defence capability of the state, preventing armed conflicts and repelling armed aggression.

In this way, a base of terms was systematised in accordance with those generally accepted on a global scale. The entry into force of this law has opened up great opportunities for the exchange of experience at the international level. Moreover, joining the global anti-terrorist movement has brought about the symbiosis of various fields in the legal space, since the fight against cybercrime is not the exclusive prerogative of law enforcement agencies.

Cybersecurity is provided by cybersecurity entities that take measures to prevent the use of cyberspace for military, intelligence-subversive, terrorist, manipulative, and other illegal and criminal purposes, identify and respond to cyber incidents and cyberattacks, eliminate their consequences, conduct information exchange regarding actual and potential cyber threats, develop and implement preventive, organizational, educational and other measures in the field of cybersecurity, cyber defence and cyber protection, ensure information security audits, including at subordinate facilities and facilities belonging to the sphere of their management, carry out other measures on ensuring the development and security of cyberspace (Potiy *et al*. 2021, p. 142).

This definition has a direct relationship with the legal and operational framework, as it defines the subjects and their functions in the field of cybersecurity. The above definition also indicates that cybersecurity actors must provide measures to prevent the use of cyberspace for various negative, illegal or criminal

purposes. They must also respond to cyber incidents and cyberattacks, perform information sharing on cyber threats, and develop and implement cyber protection, cyber defence and cyber security measures. At the same time, they must conduct information security audits and carry out other measures to ensure the development and security of cyberspace.

In order to increase the attention paid to cyber defence, in October 2017 the Law of Ukraine 'On the Defence of Ukraine' No. 1932-XII (1991) was amended, providing for the preparation of the state for defence in peacetime, during which measures regarding cyber defence (active cyber defence) should be implemented in order to protect the sovereignty of the state, ensure its defence capacity, prevent armed conflicts and repel armed aggression. In the future, the Law of Ukraine 'On National Security of Ukraine' No. 2469-VIII (2018) will become an equally important national regulatory act for guaranteeing cybersecurity. Its principles partially revealed the peculiarities of the Cybersecurity Strategy of Ukraine.

The Law contains only general provisions that do not contain specific measures. This led to shortcomings in the sphere of the security and defence of Ukraine, as a result of which disruptions in the work of the state authorities, private businesses, etc. took place and continue to do so. Therefore, in order to specify measures for the defence of the Ukrainian state and, in particular, cyber defence, the relevant Regulation was approved by the Decree of the President of Ukraine No. 23/2019 'On Regulations on the General Staff of the Armed Forces of Ukraine' (2019).

Thus, analysing the main tasks of the General Staff of the Armed Forces of Ukraine and the corresponding provisions, the following observations can be made:

1. With regard to the organisation of information protection and cyber protection, the General Staff of the Armed Forces of Ukraine are responsible for organising the deployment, management and functional existence of the information protection and cyber protection system in the information and telecommunication systems of the Ministry of Defence of Ukraine and the Armed Forces of Ukraine.
2. Concerning participation in the national cybersecurity system, the General Staff participate in the creation and review of the national cybersecurity system on a periodic basis.
3. The planning and implementation of cyber defence measures in order to prepare the state to repel military aggression in cyberspace (cyber defence) is also one of the tasks of the General Staff.

4. The coordination of the implementation of cyber defence tasks is also performed by the General Staff, overseeing the executive authorities, local self-government bodies and other components of the defence forces.
5. The tasks of the General Staff to ensure information security and counter cyber threats aim to ensure information security in the Armed Forces of Ukraine and counter systematic and large-scale actions against the interests of Ukraine in cyberspace, in particular by foreign states and their cyber units with special cyber weapons.

These provisions testify to the importance of interaction, coordination and active cybersecurity measures to ensure the national security and defence capacity of Ukraine in cyberspace. In addition, by Decree of the President of Ukraine No. 473/2021 'On the decision of the National Security and Defence Council of Ukraine' (2021) and 'On the Strategic Defence Bulletin of Ukraine' (2021), the next Strategic Defence Bulletin of Ukraine was approved. This defence planning document normalised the concepts of: military aggression in cyberspace, actions in cyberspace, cyber threats of a military nature, cyber warfare, cyber actions, cyber intelligence, cyber weapons, and cyber infrastructure. The Decree also emphasises that in order to counter the forces and means of the enemy, actions aimed at radio-electronic warfare and confrontation in cyber and information spaces must be combined.

The peculiarity of cyber defence, in contrast to cyber protection, is the presence of an active phase, where the vulnerabilities found in one's own system should become a projection of targets in similar enemy systems. Thus, in mission-critical systems during war, it is important to have procedures for monitoring the state of the system, scanning networks for vulnerabilities, deploying the infrastructure of false targets, and constantly exchanging information with active cyber defence forces. Therefore, the main task of cyber defence is to ensure the continuity of the functioning of systems of critical importance to critical infrastructure objects with the use of active countermeasures against the enemy (Davydiuk 2022, p. 51).

Since 2018, the Security Service of Ukraine has been operating the Cybersecurity Situation Centre. This structure was created with the help of the NATO, and technical equipment and software for the work of the Centre were provided as part of the implementation of the first stage of the Agreement on the implementation of the Ukraine-NATO Cybersecurity Trust Fund. The information security event management system operates on the basis of the Situation Centre, which monitors events in real time and allows the state of information security to be analysed. Moreover, this makes it possible to promptly detect,

respond to, and warn of threats in national cyberspace (Security Service of Ukraine, 2022). Every day, cybercriminals use dozens of new schemes and methods of personal enrichment at the expense of other citizens and businesses around the world via the Internet. According to Article 1(8) of the Law of Ukraine 'On the Basic Principles of Ensuring Cybersecurity of Ukraine', cybercrime (computer crime) is a socially dangerous criminal act in cyberspace, the responsibility for which is provided by the Code on Criminal Responsibility (hereafter – CCU) of Ukraine and is recognised as a crime by international treaties of Ukraine.

It should be noted that at the beginning of April 2022, Ukraine was accepted into the Joint Centre for Advanced Technologies in NATO Cyber Defence as a contributing member (Onyshchenko and Hlushko 2022, p. 16).

As recent events show, a war in the information space causes no less damage than a war on the battlefield. Understanding all this, in the first 2 months of hostilities, the Parliament of Ukraine promptly and unanimously optimised the legislation around criminal proceedings. It also improved the grounds and procedural mechanisms for bringing all cybercriminals to criminal responsibility. These changes were concentrated in several laws.

For instance, the law 'On Amendments to the Criminal Code of Ukraine to Increase the Effectiveness of Combating Cybercrime in the Conditions of Martial Law' No. 2149-IX (2022) aims to: strengthen the capabilities of the national cybersecurity system and optimise it to counter cyber threats; implement effective criminal and legal mechanisms for countering cybercrime; and ensure the reliability and safety of using digital services. This Law also provides that interference in the work of information and communication systems and electronic communication networks will not be considered unauthorised if such interference is carried out in accordance with the procedure for searching and identifying potential vulnerabilities of such systems or networks, the exact text of which the State Special Communications was working on at the time of preparing this Chapter.

Secondly, the Law 'On Amendments to the Criminal Procedural Code of Ukraine and the Law of Ukraine "On Electronic Communications" regarding increasing the effectiveness of pre-trial investigation "on hot tracks" and countering cyberattacks' No. 2137-IX (2022), albeit fragmentary, makes necessary and generally positive changes. Among other things, these changes introduced the terms *computer data* and *computer systems* in criminal proceedings and provided a new public investigative (search) action – the taking of evidence from technical devices and technical means that have the functions of photo and video recording. In addition, the name of the law has been changed and the legal regulation of the procedural issues for the implementation of such secret investigative

(search) actions as removing information from electronic communication networks and establishing the location of radio equipment (radio-electronic means) has been improved (Maltseva *et al.* 2022, pp. 37–44).

In early April, the Cabinet of Ministers of Ukraine issued resolution No. 299 on 'Some issues of response of cybersecurity entities to various types of events in cyberspace' (2023). This resolution defined the procedure for responding to cyber incidents and cyberattacks. The new resolution will allow for timely responses and the planning of cyber protection measures. It is normatively established that responding to cyber incidents/cyberattacks is carried out by cybersecurity entities by: taking cyber protection measures aimed at the rapid detection of and protection against cyber incidents/cyberattacks; gathering proper information about them; preventing minimising and eliminating negative consequences; correcting vulnerabilities; and restoring the stability and reliability of the functioning of electronic communication, information and communication, and technological systems and other objects of cyber protection (Krasnikov 2023, p. 122).

At the legislative level, the limits of the national police's activity in countering cyber fakes and threats in the information space, as well as the investigation of cybercrimes, provided for in Articles 361 and 361[1] of the CC, were expanded. It can be stated that the strengthening of sanctions, the additional criminalisation of certain acts related to the detection of fakes in social networks, and the prevention of cyberattacks are measures that are able to partially deter potential criminals from committing these and other crimes. State policy in the field of the legal regulation of cybersecurity is determined by the priority of national interests, aims to prevent the realisation of threats to information, and is carried out by implementing the provisions specified in the legislation (Kolesnyk and Plakhotnyy 2023, p. 51).

Behind the strategic steps and the legislative framework of cybersecurity is the need to interact with the private sector, which is an important actor in this space. In the context of general strategies and laws, the private sector, which includes businesses and organisations, is also becoming an object of increasing risk from various cyber threats in the conditions of the war in Ukraine. From cyberattacks on corporate networks to cyber fraud, businesses and industrial entities are currently facing various challenges and threats in the digital environment. Effective protection against these threats requires the private sector not only to comply with established norms and standards, but also to actively participate in the implementation of innovative solutions and technologies for cyber protection. Thus, the interaction between the state, the public sector and private business is a key element in creating a sustainable and secure digital ecosystem.

Legal aspects of interdepartmental and public-private interaction in the national cybersecurity system provide for the establishment of mechanisms for cooperation and information exchange in detecting and responding to cyber incidents. Legislation can establish procedures for joint analysis and response to cyberattacks, the exchange of technical information about new threats and vulnerabilities, as well as the coordination of measures to prevent and neutralise cyber threats.

It is quite obvious that cyber threats are not diminishing. In fact, new cyber threats emerge every day, and cybercriminals will always find new ways to break into systems and steal information. It is for this reason that cybersecurity is becoming increasingly important and companies need to be aware of existing threats in order to understand how to better protect their organisation. Below are just a few main examples of the latest cybersecurity threats, of which we are likely to see more this year.

3.8.2.1. Phishing and SMiShing

Phishing is one of the most commonly reported cybercrimes in the USA, resulting in countless financial losses every year. The goal here is to steal sensitive data and credentials, such as login credentials or credit card details, and trick people into allowing malware to be installed. Phishing techniques can disable security controls while an attacker browses company data undetected.

Smishing works on the same principles as phishing, but the decoy messages are sent via SMS rather than email. An attacker poses as a trusted person and targets mobile devices to gain access to sensitive information. When these mobile devices connect to the company's network, an attacker gains access, stealing customer and employee data and the organisation's source (Art. 200 of the CC of Ukraine).

3.8.2.2. Malicious Software

Malware (malicious software) comes in many forms. Attackers develop malware to create permanent, hard-to-detect backdoor access to company devices. They can then remotely control the device and use it to steal data, explore the local network, or send spam from the infected device. A staggering 91 % of cyberattacks start with a phishing email, so phishing and malware often go hand in hand (Art. 361 of the CC of Ukraine).

3.8.2.3. Ransomware

This form of malware can cause catastrophic damage to a business. Once the malware enters a system, it locks it down and deprives the owner of access to

critical data until they pay a ransom to retrieve their sensitive information and regain control of their systems (Art. 189 of the CC of Ukraine).

3.8.2.4. Compromise of Corporate e-Mail

Also known as email account compromise, Business Email Compromise (hereafter – BEC) is one of the costliest cybercrimes. This is manifested in attackers compromising corporate emails to defraud companies (Art. 182 of the CC of Ukraine).

3.8.2.5. Internal Threats

Many people in a company have access to sensitive information. Whether stemming from current or former employees, partners or contractors, 25 % of data breaches are due to insider threats. Bad actors act out of greed, or sometimes disgruntled employees act out of bitterness. In any case, their dissemination of important information can cause significant financial losses (Art. 147–263 of the CC of Ukraine).

According to Article 190 of the CC of Ukraine, fraud committed on a large scale (from 250,000–300,000 hryvnias, approx. 6,250–7,500 EUR) with the use of electronic computing equipment is punishable by imprisonment from 3 to 8 years. If Internet fraud is committed by an organised group or in particularly large amounts (from 635,000 hryvnias), it is punishable by imprisonment for a term of 5 to 12 years with confiscation of property.

A criminal case on fraud is initiated if the amount involved exceeds a minimum of 0.2 of the tax-free income of citizens. If the fraud involved is less than this amount, an administrative penalty is applied.

After the open aggression of the Russian Federation in 2022, new challenges related to cyber warfare emerged. It should be noted that the Russian Federation began the active phase of the hybrid war in the information space of Ukraine after the annexation of Crimea. After 2014, cyberattacks performed by various cyber groups supported by the government structures of the aggressor state began to be carried out on the critical infrastructure of Ukraine (Leonov and Seryogin 2019, p. 57).

It is possible to state that many cyberattacks organised by Russian hacker groups began even before the start of the large-scale war – that is, before 24 February 2022. The first phishing campaigns against Ukraine were recorded by Google specialists back in April 2021. In 2022, the number of cyberattacks on Ukraine increased by 3.5 times compared to 2020, and the number of attacks on NATO countries quadrupled. Google analysts reported that Ukraine and NATO

countries were mainly being cyberattacked by five hacker groups: Frozen Lake, Coldrive, Summit, Frozen Barentz and Frozen Vista, some of which cooperate with the FSB and the GRU (the Main Intelligence Directorate) of the Russian Federation. All of these groups, according to the US Treasury Department, are part of the Trickbot cybercriminal group, which was engaged in the development and implementation of computer viruses that were used to steal financial data.

If the actions of these groups are directed against Ukraine or NATO countries, the following aspects of responsibility are possible:

1. International reaction: cyberattacks, especially those with international implications, can provoke a response from NATO and other allies. This could include diplomatic measures, economic sanctions, or even a cyber response.
2. Legal responsibility: if the individuals or organisations responsible for cyberattacks can be identified, legal liability may be considered. They may be charged with cybercrimes or violations of cybersecurity laws.
3. International discussions: states can conduct discussions and consultations in international forums, including the UN or the EU, in order to respond to cyber threats and develop international standards in the field of cybersecurity.
4. Cooperation in the field of cybersecurity: states can strengthen cooperation in the field of cybersecurity by sharing information and developing measures to increase cyber resilience and protect critical infrastructure.

It is important to note that identifying and establishing responsibility for cyberattacks is a complex task and may require time for careful analysis and investigation.

From a technical point of view, the aggressor state systematically implements the latest developments in order to spread malicious software in domestic cyberspace. For example, the Nodaria hacker group, which is closely associated with the Russian Federation, actively uses new malicious software during cyberattacks aimed at Ukraine. The Graphiron malware program is a modern piece of spyware development. This malware system was distributed to collect a wide range of information from infected computers, including system information, credentials, screenshots, and access to individual files. The program uses filenames designed to masquerade as legitimate Microsoft Office files and is similar to other TA471 tools such as GraphSteel and GrimPlant. Previously, they were used as part of a phishing campaign specifically targeting Ukrainian government bodies, in particular in January 2022.

Graphiron is designed to extract much more data, including screenshots and Secure Socket Shell (hereafter – SSH) private keys (Poliakov 2023, pp. 125–138). The information presented may be relevant from the point of view of

demonstrating the diversity, high sophistication and seriousness of the harmful effects of enemy cyberattacks. New methods of such crimes emerge every day in cyberspace. Thus, the current legal norms of any country, and even more so of Ukraine, which is in a state of war, should anticipate, identify, resist and provide safeguards in the fight against such a serious global crime more promptly and flexibly.

In March 2023, the State Special Communications Service presented an analytical report on Russia's cyber aggression against Ukraine 'Russia's Cyber Tactics: Lessons Learned 2022' (2022).

Based on the results published by the State Intelligence Service, it is possible to state the main trends and dynamics of the Russian cyber threat. Cyberattacks are a fully fledged component of the Russian war against Ukraine. The goals of Russian hackers correspond to the overall goals of Russian military aggression. Civilian infrastructure is the primary target of Russian cybercriminals, and the hackers' priorities throughout the full-scale invasion have shifted according to military needs. Although state structures have consistently remained key targets of cyberattacks, media and telecoms were important targets early in the invasion, as Russian authorities counted on a quick victory and hoped to influence and intimidate Ukrainians through the media (Analytical report of the State Intelligence Service on the year of Russia's full-scale cyber war against Ukraine 2023, p. 30).

During 2022, Ukraine faced 7,000 cyberattacks on its information infrastructure. In addition, from 24 February to the end of 2022, the government's CERT-UA computer emergency response team processed 2,194 cyber incidents. Of these incidents, 120 were related to the financial sector, 156 to commercial organisations, and 92 to the telecommunications and software development sector. At the same time, since the beginning of 2023 (compared to the fourth quarter of 2022), cyberattacks from pro-Russian groups have decreased, but they remain systematic and intense. During 2023, in addition to banks, cybercriminals attacked insurance companies and bank software developers.

The State Security Service suggests that the increase in phishing attacks and account compromises targeting the Ukrainian banking system indicates that the Russians are planning to hack commercial organisations and attack them in order to steal resources (European Business Association, 2023).

Despite numerous public calls for the peaceful use of cyberspace in the interests of all people and nations, the governments of many leading countries have actively joined the cyber arms race, recreating the classic security dilemma on a qualitatively new basis. This means that against the background of complex and contradictory global processes of political, economic and social development,

cyberspace is playing host to a new Cold War – that is, it is serving as the basis of a new confrontation between key geopolitical actors (Horinov and Drapushko, p. 268). However, Ukraine is forming its own model of strengthening the state of cybersecurity in the conditions of war, which requires, first of all, that the development and approval of relevant normative acts that meet the conditions of today is hastened. In early April 2023, the Cabinet of Ministers of Ukraine issued a resolution defining the procedure for responding to cyber incidents and cyberattacks.

The new Resolution of the Cabinet of Ministers of Ukraine No. 299 on 'Some issues of response of cybersecurity entities to various types of events in cyberspace' (2023) will allow for the timely response to and planning of cyber protection measures.

This Resolution approved the Procedure for the response by cybersecurity entities to various types of events in cyberspace. The algorithm for the response of cybersecurity entities to cyber incidents/cyberattacks begins with the preparation stage, during which measures are taken to research modern types of cyber incidents/cyberattacks and develop methods and mechanisms for preventing and countering possible cyber incidents/cyberattacks.

It is also important to note that the EU has supported Ukraine in countering cyberattacks by launching a cyber dialogue between the EU and Ukraine in 2021, strengthening the operational capacity of Ukraine's telecommunications services and helping to combat disinformation. In addition, at the request of the Ukrainian government, for the first time in an operational context, the EU activated rapid response teams for cyber incidents within the framework of PESCO (Committee on Digital Transformation, Information management 2022). Cybersecurity experts help identify, recognise and mitigate threats. Earlier, in July 2020, the EU introduced the first ever sanctions against the organisers of cyberattacks, including NotPetya. The recently approved Strategic Compass aims to strengthen the cyber resilience of the EU (proposing, in particular, a new law on cyber resilience and the further strengthening of the cyber diplomacy toolkit) and the EU's Eastern partners through cooperation in countering hybrid and cyber threats, as well as disinformation (Y. Pshetachnyk *et al.* 2022). In February 2022, the US Cyber Command team assisted cyber incident response teams in searching for active threats. For its part, the USA has allocated 40 million dollars since 2017 for the development of the IT sector of Ukraine. NATO member states are also investing in Ukraine's cyber defence through information sharing and support at the local level. In March 2022, Ukraine became a contributing member of NATO's Joint Advanced Technologies Centre for Cyber Defence. In addition, private companies such as Microsoft, Amazon, and Google

are assisting Ukraine in detecting and countering cyberattacks during the invasion. The European Centre of Excellence for Countering Hybrid Threats has also increased cooperation with Ukraine since the beginning of the war, monitoring the situation and organising training on identifying, stopping, destroying and countering cyber threats, creating new ways of countering them.

Therefore, the key legal aspects that relate to the abovementioned context require legal regulation in various fields.

Firstly, at level of international law, the assistance that the USA and NATO member countries provide to Ukraine falls under the principles of international law – in particular, in the case of cooperation between countries or military blocs. This covers arrangements, agreements or certain standards of interaction in the field of cybersecurity.

Secondly, the allocation of financial resources from the USA and other countries for the development of cyber infrastructure in Ukraine falls under laws on development financing, trade and investment.

Thirdly, partnerships in the field of cybersecurity may involve joint agreements and principles for ensuring security in the digital space. This may include mutual assistance and information sharing to detect and counter cyber threats.

Fourthly, legislation on cybersecurity and data protection that is specific to each country is needed in this field.

Fifth, as concerns the private sector and cybersecurity, the involvement of private companies such as Microsoft, Amazon and Google in cybersecurity may take into account laws and standards regarding the protection of confidential information and cooperation with governmental structures in the field of cybersecurity.

Sixth, with regard to international organisations, Ukraine's participation in NATO's Joint Advanced Technologies Centre for Cyber Defence may be subject to regulation by the organisation's regulations and agreements.

Lastly, in the context of hybrid war and threats of a hybrid nature, the legal framework for cooperation in the field of cybersecurity can be supplemented by international standards and conventions on cybersecurity.

Considering all these aspects, the legal context of cooperation in the field of cybersecurity can be explored and defined at different levels: national, international and multilateral. Therefore, in its Resolution the European Parliament called for the immediate and full implementation of all decisions that will strengthen the EU's contribution to strengthening Ukraine's defence capabilities, including in the field of cybersecurity. In addition, the Parliament called on the EU, NATO and other interested partners to strengthen assistance to Ukraine in the field of cybersecurity. MEPs called for the full application of the EU cyber

sanctions regime against individuals, legal entities and institutions responsible for or involved in cyber attacks against Ukraine (European Parliament, 2022, pp. 27–30).

Ukraine, taking into account the importance of interagency and public-private cooperation in the field of cybersecurity, is constantly improving its legal framework. The process of development and implementation of new legal acts is aimed at creating a favourable and effective system of cooperation between state bodies and private entities in the field of cybersecurity. For Ukraine, there are only two main problems in the field of cybersecurity: internal and external.

The internal problem is that commercial structures and individuals are not aware of cyber problems. First of all, it is necessary to work on the interaction between law enforcement agencies and those commercial organisations that can provide this service to overcome problems during attacks, hacks, etc. In addition, there should be reforms in the field of education to ensure the sufficient awareness and professional literacy of university graduates. It is clear that cybersecurity professionals will be able to explain the need for cyber protection, and accordingly will develop cybersecurity services. The presence of such specialists is important from the point of view of the protection of state objects and state secrets, in connection with the low level of implementation of innovative technologies in the field of the protection of information of state importance. In the context of foreign policy in this regard, the protection of state objects and state secrets should also be supported by fundamental informational provisions regulated by the laws and by-laws of the state (Bilenchuk and Obikhod 2018, p. 238).

From a legal point of view, among the tasks of the state in the conditions of martial law in the field of cybersecurity there are several key aspects that could be emphasised. Firstly, regarding the creation and optimisation of the national cybersecurity system, possible legal measures could include the development and implementation of legislation aimed at ensuring effective cybersecurity. This may include the creation of security standards, the regulation of cyber protection and cyber defence, and mechanisms for cooperation between the public and private sectors.

Legal measures may also provide for the creation of a legal environment for the development and maintenance of the necessary cyber capabilities. This may include financial incentives, tax breaks and other measures to support cybersecurity initiatives. The creation of prerequisites for mastering modern forms and methods of preparing and holding events is also relevant. This may include the regulation of cybersecurity training programs, certifications, and licensing. Requirements for conducting regular training and activities in the field of cybersecurity may also be established.

A timely response to current threats is also needed. Legal remedies can provide mechanisms for the timely detection, response and elimination of cyber threats. This may include developing standards for sharing information about cyber threats and implementing procedures to coordinate the actions of various actors. Lastly, the creation of effective management and cooperation systems is necessary. Legal measures can define mechanisms for creating effective cybersecurity management systems and ensuring cooperation between various national security actors, as well as with international partners.

The overall goal of such legal measures is to create a transparent, effective and well-coordinated mechanism for the protection of cyberspace under martial law. It is also important to ensure that these measures comply with the principles of human rights and privacy protection.

3.8.3. Interim findings

Cybercrime is a completely new type of crime which is constantly being updated, transformed, and has no permanent features, and against which standard approaches do not work.

As Interpol notes, cybercrime is currently developing at an incredible speed, and cybercriminals can coordinate a complex attack in a matter of minutes. This is why it is important for law enforcement officers to stay abreast of new technologies while understanding the opportunities they create for criminals and the potential for their use to combat cybercrime. A comprehensive approach which includes measures of both a legal and an educational, scientific nature is needed.

The regulation of cybercrime is usually based on a combination of national legislation and international agreements and standards. As cybercrime is becoming increasingly complex and global, regulation must meet these challenges. Many states are parties to the Convention on Cybercrime (Budapest Convention), which defines cybercrime and sets standards for cybercrime and extradition legislation. The EU also develops and implements strategies and legislative measures to ensure the cybersecurity of its members.

International organisations such as Interpol conduct joint operations and provide a platform for information sharing between countries. Some countries are creating special cyber police units and centres to fight cybercrime, and cybercriminals can now be tried and prosecuted by national and international courts either under the laws of the country in which they commit crime or in the country which apprehends them.

In this direction, Ukraine has undertaken positive steps in the legal field, including by defining cybercrime in its CC (including articles about unauthorised

access to computers, spreading viruses, the theft of electronic information and other types of cybercrime) and adopting cybersecurity strategies and policies. Because cybercrime is of a flexible nature, the process of improving the legislation should be continuous and prompt.

Ensuring the effective fight against cybercrime requires the constant updating of legislation and technological measures and the cooperation of national and international organisations, taking into account the global nature of cyber threats.

In the conditions of martial law and given the accelerated development of digital technologies, cyber defence should be considered comprehensively. After all, the loss of funds and the leakage of information are only two examples of scenarios that the implementation of a cyberattack could create, and critical elements of the country's infrastructure are under threat. For these reasons, the prevention and elimination of threats to the digital transformation of cyber defence is the basis of both the competitiveness of business activity and the success of the state in general.

Considering the situation in the international arena and the constant improvement of the skills of Russian cybercriminals and hackers, it is necessary to pay sufficient attention at the state level to the issues of strengthening cybersecurity and data protection. Resilience against hacking and cyberattacks is important in any field, and digital security will only continue to grow in importance in the coming years. The state is taking important steps to strengthen cybersecurity at both the regulatory and methodological levels, which will allow the response to various types of events in cyberspace to be regulated and will significantly strengthen the protection of information resources and objects critical to the information infrastructure against cyberattacks. In order to ensure the cybersecurity of Ukraine, it is necessary to strengthen the interaction between the main subjects of the national cybersecurity system and to establish constructive cooperation. Strengthening the state of cybersecurity also involves the implementation and adaptation of EU legislation into national standards in the field of cybersecurity. Further efforts are also needed with regard to active work with the private sector, creating partnerships to share information and jointly fight cybercrime.

3.9. Legislative Challenges in Neighbouring Countries as a Consequence of the War of Aggression Against Ukraine: The Example of Poland

3.9.1. General Remarks

The Russian aggression against Ukraine which began on 24 February 2022 has had a demolishing effect on the Ukrainian state. The population has been

Lyra Jakulevičienė / Patrick R. Hugg /
Dmytro Luchenko (eds.)

The Impact of War and Extraordinary Situations on Law in the Context of Agression against Ukraine

PETER LANG

Berlin - Bruxelles - Chennai - Lausanne - New York - Oxford

Library of Congress Cataloging-in-Publication
A record in the CIP catalog has been requested for this book.
of the Library of Congress.

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek collects this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available on the Internet at .Nationalbibliografie; detailed bibliographic data are available on the Internet at http://dnb.d-nb.de.

Copy-editor: MB "Kopis"

Approved by Mykolas Romeris University Law School Council on 5 June 2024 by resolution No. 1T-13 (1.12 E-20401).

ISBN 978-3-631-92350-4 (Print)
E-ISBN 978-3-631-92813-4 (E-PDF)
E-ISBN 978-3-631-92814-1 (E-PUB)
DOI.10.3726/b22448

© Collective of authors, 2024
© Mykolas Romeris University, 2024

Lyra Jakulevičienė / Patrick R. Hugg / Dmytro Luchenko (Eds.), 2024
Published by Peter Lang GmbH, Berlin, Deutschland
info@peterlang.com - www.peterlang.com



Open Access: This work is licensed under a Creative Commons Attribution CC-BY-NC-ND 4.0 license.
To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/.

Mykolas Romeris University

Reviewers:

Prof. dr. Jesús Verdú Baeza (University of Cádiz)

Prof. dr. Iman Prihandono (Universitas Airlangga)

Prof. dr. Teresa Gardocka (SWPS University of Social Sciences and Humanities)

Prof. dr. Kristian Bankov (New Bulgarian University)

Prof. dr. Edita Gruodytė (Vytautas Magnus University)

Prof. dr. Toma Birmontienė (Mykolas Romeris University)

Assoc. Prof. dr. iur. Jānis Pleps (University of Latvia)

Assoc. Prof. dr. Pavlo Romaniuk (Yaroslav Mudryi National Law University)

Assoc. Prof. dr. Jolanta Apolewicz (Mykolas Romeris University)

Dr. Filip Cyuńczyk (SWPS University of Social Sciences and Humanities)

Dr. Dovilė Pūraitė-Andrikienė (Law Institute of the Lithuanian Center for Social Sciences)

Dr. Agnė Limantė (Law Institute of the Lithuanian Center for Social Sciences)