Zinchenko, O. I. (2024). Cyber terrorism: History of Ukraine and current trends. *Actual Issues of Modern Science. European Scientific e-Journal, 34*, __-__. Ostrava: Tuculart Edition, European Institute for Innovation Development.

DOI: 10.47451/soc2024-09-02

The paper is published in Crossref, ICI Copernicus, BASE, Zenodo, OpenAIRE, LORY, Academic Resource Index ResearchBib, J-Gate, ISI International Scientific Indexing, ADL, JournalsPedia, Scilit, EBSCO, Mendeley, and WebArchive databases.

Oleksandra I. Zinchenko, Ph.D. Student, Department of Political Science of School of Philosophy, V.N. Karazin Kharkiv National University. Kyiv, Ukraine.
ORCID: 0000-0003-1623-957X

Cyber terrorism: History of Ukraine and current trends

Abstract: This article aims to determine the essence and legislative framework of Ukraine's cyber security decision-making, like research prospects for improving cyber security and countering cyber terrorism in the country. The main research methods used in the article are induction, synthesis, comparison, and generalization. The essence of the "cyber security"concept, its features, and its legislative basis have been studied. The critical legislative acts of Ukraine, which consider provisions on cyber security and information protection, have been identified. The features of introducing international cyber security norms into Ukraine's legislation are characterized. An assessment of the progress achieved by Ukraine in fulfilling its international obligations in cyber security is provided, and further steps to implement global standards and best practices into Ukrainian legislation are determined. The level of awareness of the Ukrainian authorities regarding the NIS Directive and the level of reflection of its provisions in the country's laws and cyber security systems are characterized. The provisions of the Constitution of Ukraine, which protect information and the specifics of its disclosure, have been determined. The main points of the Ukrainian history of cyber security and its impact on it during the period of anti-terrorist operations and full-scale invasion have been identified. The peculiarities of Ukraine's cooperation with the EU and NATO in combating cyberterrorism are characterized by the effectiveness of the cyber police and other structural units created to protect cyberspace and counter hacker attacks.

Keywords: terrorism, cyber terrorism, cyberspace, information technologies, national security of Ukraine, information space, international norms of cyber security.

Introduction

Over the past few years, Ukraine has become one of the leaders in the number of cyberattacks of varying severity. The increase in the number of cyber-terrorist attacks is an urgent problem for our country today. It requires effectively developing a set of tools and measures to combat them, including at the legislative level. The legal framework for cyber security in Ukraine consists of international obligations and domestic legislation. The Budapest Convention and the Directive on Network and Information Security (NIS) are particularly noteworthy at the global level. Domestic legislation is stipulated by Ukraine not only as a signatory to international agreements and treaties but also as an obligation they should keep in mind if they continue to demonstrate their readiness to join the European Union. Specific issues and problematic aspects

of cyberterrorism and cyber security have been considered in the works of the following figures: I.A. Bilan, V.G. Drozd, O.Y. Drozd, D.V. Zhuravlev, Y.I. Kohut, S.V. Petkov, etc. However, despite numerous scientific papers on this topic, the problems that form a practical approach to assessing cyber security and its likely impact due to the rapid development of information technology remain unresolved and, therefore, require further study and research. The article aims to define the essence and legislative framework for regulating cyber security in Ukraine, like to study the prospects for improving cyber security and countering cyberterrorism in the country.

According to the purpose of this article, the following tasks need to be addressed:

- study the essence of the "cyber security" concept of its features and legislative framework;
- identify the key legislative acts of Ukraine that address the provisions on cyber security and information protection;
- characterize the peculiarities of the implementation of international cyber security norms into Ukrainian legislation;
- identify the provisions of the Constitution of Ukraine providing for the protection of information and peculiarities of its disclosure;
- identify the main points of Ukrainian cyber security history.

The following research methods were used in this scientific article:

- induction to study the essence of the "cyber security" concept, its features, and legislative framework;
- identification of critical legislative acts of Ukraine that address the provisions on cyber security and information protection;
- synthesis method to study the peculiarities of implementing international cyber security norms into Ukrainian legislation;
- identification of the provisions of the Constitution of Ukraine providing for the protection of information and the peculiarities of its disclosure;
- comparison to identify the main points.

The results of the study

It is worth noting that positive developments have been made in cyber security. Thus, several regulatory acts are devoted to the issue of cyber security in Ukraine, in particular:

- On Security Services in Ukraine, Law No. 2229-XII, dated March 25, 1992;
- On Operational and Investigative Activities, Law No. 2135-XII, dated February 18, 1992;
- On the State Service for Special Communications and Information Protection of Ukraine, Law No. 3475-IV, dated February 23, 2006;
- On the Organisational and Legal Framework for Combating Organised Crime, Law No. 3341-XIII, dated June 30, 1993;
- The Criminal Code of Ukraine dated April 05, 2001.

In addition, cyber security and information protection issues are addressed in the following legislative acts (*Table 1*).

In 2005, Ukraine ratified the Budapest Convention, the only legally binding international instrument on cyber security, which establishes a standard criminal policy to protect against

cybercrime by adopting relevant national laws and promoting international cooperation. However, not all of its provisions have been integrated into national legislation, and their full implementation will require further significant changes to the criminal procedure code. In 2016, the European Parliament adopted the NIS Directive, the first part of the EU's single law on cyber security. As Ukraine is not a member of the EU, the NIS Directive is not binding on our country, but it does provide good practice recommendations. Some of its provisions are voluntarily implemented in Ukrainian legislation, but others are ignored. In recent years, Ukraine has adopted several acts that regulate cyber security issues and constitute the country's legal framework in cyber security. For example, to support the previous point, 2016, the National Cyber security Strategy of Ukraine set cyber security goals and priorities for up to 2020. This law defines critical timelines, delineates responsibilities between cyber security agencies, and sets out the principles of full regulation of critical infrastructure (CI) protection and public-private partnerships. While adopting the cyber security law was a positive step, significant efforts are still needed to implement all aspects of it fully. Most importantly, within the timeframe established by law, the government has not yet adopted bylaws on cyber security, including those regulating the protection and audit of cyber security facilities. As a result, many of the law's provisions remain vague and do not specify the necessary procedures.

Ukraine has signed several international treaties, committing itself to ensuring security in cyberspace. These international obligations have become the basis for further legal regulation of cyber security issues. By signing these agreements, Ukraine promised to adhere to certain standards and enshrine them in its legislation.

It is worth noting that the Constitution of Ukraine reflects the main provisions protecting information and the specifics of its disclosure, such as defining security and defense requirements (*Table 2*).

It is worth noting that the National Security and Defence Council is a coordinating body for national security and defense under the President of Ukraine. The President personally forms the composition of the National Security and Defence Council. The activities of the National Security and Defence Council of Ukraine are determined by the Law "On the National Security and Defence Council," which provides the legal framework for cyber security in Ukraine.

According to the Military Security Strategy of Ukraine, dated March 25, 2021, the Comprehensive Defence of Ukraine is a set of measures, the main content of which is preventive measures and sustainable resistance to invaders on land, at sea, and in Ukraine's airspace, counterattacks in cyberspace, and imposing one's will in the information space.

At the state level, the Russian Federation remains Ukraine's military adversary, conducting an armed attack against Ukraine, occupying the country's territories, and systematically using military, political, economic, informational, psychological, space, cyber, and other means. This threatens the independence, national sovereignty, and territorial integrity of Ukraine.

The development of cyber security and cyber defense capabilities as part of the preparation and implementation of Ukraine's comprehensive defense is essential in the event of emergencies, mass terrorist acts that cause loss of life, or destruction of vital infrastructure. As part of its international relations, Ukraine participates in various global initiatives. It has cyber security cooperation agreements with other countries and international organizations that help exchange information and coordinate actions in the event of cyber threats (*Figure 1*).

It is worth noting that these international treaties, agreements, and initiatives will help Ukraine jointly combat cyber threats and strengthen cyber security and international cooperation in countering cyberspace threats.

It is also worth noting that Ukraine is the only country legislating the cyberterrorism concept, defining it as terrorist activities performed in or using cyberspace (*On the Main Principles…, 2017*). However, this definition is very general and does not allow for an accurate and complete description of the actions that fall under this concept. In other words, to develop a set of practical measures to combat cyberterrorism, it is necessary to determine the list of crimes that can be considered cyberterrorism and assess the degree of criminal liability for committing such crimes.

The Ukrainian history of cyber security and its impact is best viewed from 2014 when the Russian invasion of Ukraine began. Thus, the chronology of cyber-terrorist attacks is as follows:

- on 4 February 2014, an anonymous hacker from the "Cyberberkut" group posted on YouTube a telephone conversation between the US Ambassador to Ukraine and the US Assistant Secretary of State, which contained derisive comments about the EU;
- on March 5, 2014, a recording of a telephone conversation between the foreign ministers of Estonia and the EU was posted on the Internet, which suggests that Ukrainian opposition forces were behind the sniper shooting on Maidan. This was the point of view actively promoted by Russian propaganda at the time;
- in March 2014, from the beginning of the occupation of Crimea, the Russian secret service blocked communication between Ukrainian MPs and SBU units in Crimea by attacking IP phones;
- on May 21-25, 2014, during the presidential elections, DoS attacks and hacking of the CEC website took place, resulting in the publication of fake results on the website. Despite reports of the hacking, these data were reported on Channel One news in Russia as the actual results of the elections in Ukraine;
- in June 2014, malicious cyber-espionage software was detected on the servers of private companies in Ukraine and NATO countries, and analysis showed that the software was developed in Russia;
- since 2014, the radar intelligence of terrorists fighting in Donbas has been hacking into the database on the location of telephone networks and Wi-Fi and obtaining data on the location of Ukrainian troops;
- in October 2015, a private investigation revealed that Russian cyber-espionage targeted data obtained during the investigation of the MH17 disaster by the authorities of the Netherlands, Malaysia, Australia, Belgium, and Ukraine;
- in December 2015, a Trojan horse previously used by Russian hackers disconnected about 30 substations of Prykarpattyaoblenergo, leaving more than 200,000 residents of Ivano-Frankivsk region without electricity for 1-5 hours. At the same time, Kyivoblenergo and Chernivtsioblenergo were attacked;
- on December 6, 2016, there was a hacker attack on the internal communication network of the Ministry of Finance, the State Treasury, and the Pension Fund, which resulted in the

disabling of several computers and the destruction of significant databases, which delayed the payment of hundreds of millions of hryvnias from the budget;

- in December 2016, Ukrainian hackers ordered by an unidentified person from St Petersburg carried out a DOS attack on the website of Ukrzaliznytsia, which resulted in its work being wholly blocked for a day. According to the minister in charge, the attack was aimed at stealing data on passenger traffic;
- in the same December 2016, a cyber-attack on the Pivnichna substation of Ukrenergo resulted in a malfunction in the control system, which caused a power outage in the Northern District of the Right Bank of Kyiv and adjacent areas of the region for more than 1 hour;
- on June 27, 2017, a large-scale hacker attack was performed using a program called Petya. This malware interrupted and blocked the work of Boryspil airport, Ukrtelecom, the Chornobyl nuclear power plant, Ukrzaliznytsia, the Cabinet of Ministers, and several media outlets. SBU claims Russian special services were involved in the terrorist attack (*Largest cyberattacks…, 2014*).

First of all, the events of 2014 severely shook the state of cyber security in Ukraine. Thus, to protect Ukraine's cyberspace, on 05.10.2015, the Cyber Police was established as part of the criminal police structure of the State Police, which, according to the laws of Ukraine, ensures the implementation of the state policy in combatting cybercrime, organizes and carries out operational and investigative activities. This agency aims to ensure Ukraine's cyber security in the information space and to respond immediately to cyber threats, cybercrime, and their most serious form, cyberterrorism. In addition, the unit's mandate includes international cooperation to neutralize transnational criminal groups in this area. Thus, in 2018, the work of the cyber police of Ukraine exposed more than 800 people involved in committing crimes in the field of advanced information technology. During the full-scale invasion, these units were most effective in revealing the attackers who transmitted data on the location of the Armed Forces and various critical infrastructure facilities (*Official website…, 2024*).

A significant step for Ukraine in countering cyber-terrorist attacks and ensuring cyber security was the signing by the President of Ukraine of the Decree "On the Strategy of Cyber security of Ukraine." The document stipulates that modern information and communication technologies can be used to commit terrorist acts, particularly by disrupting the regular operation of automated process control systems at infrastructure facilities. Politically motivated activities in cyberspace are becoming increasingly common in the form of attacks on government and personal websites on the Internet. The purpose of Ukraine's cyber security strategy is to create conditions for the safe functioning of cyberspace and its use for the benefit of individuals, society, and the state. The national cyber security system is based on the Ministry of Defence of Ukraine, the State Service for Special Communications and Information Protection of Ukraine, the Security Service of Ukraine, the State Police of Ukraine, the National Bank of Ukraine, and intelligence services. The Strategy envisages a set of measures, priorities, and directions to ensure cyber security in Ukraine, in particular, to develop cyber space and promote the development of the relevant EU and NATO countries; to increase the digital literacy of citizens and the culture of safe behavior in cyberspace; to develop international cooperation and support global initiatives in the field of cyber security (*The President approved…, 2016*).

It is important to note that on 1 July 2015, the State Centre for Cyber Defence and Counteraction to Cyber Threats (SCCT) began its work. It was established by the State Service for Special Communications and Information Protection of Ukraine based on the State Centre for the Protection of Information and Telecommunication Systems of the State Telecommunications Service (*The State Center…, 2015*) and is envisaged by the Law of Ukraine «On Protection of Information in Information and Telecommunication Systems» of July 05, 1994. The Centre performs the following tasks:

- ensuring the functioning of the Ukrainian computer emergency response team CERT-UA;
- providing state information in information and communication systems of state institutions;
- professional expertise in integrated systems and means of information protection in state institutions, as well as software and hardware in information protection of Ukraine in the European information space in connection with Ukraine's integration with the EU.

In the context of European integration, it is significant to note that one of the elements of cooperation is ensuring an adequate level of personal data protection and state information security. According to the highest European and international standards, Ukraine has automatically complied with the terms of the Association and ensured all possible security measures to protect information and counteract all possible cyberattacks (*Ministry of Foreign Affairs of Ukraine, n.d.*). In addition, in 2017, Ukraine signed a cooperation agreement with Europol. The agreement aims to establish cooperation between Ukraine and Europol to support Ukraine and the member states of the European Union in preventing and eradicating organized crime, terrorism, and other forms of international crime (*Agreement between Ukraine…, 2017*). Therefore, today, the Ukrainian authorities are trying to implement the norms set out in the agreement into the national security system to continue its integration into the European information space and to be able to withstand cyberattacks, the outcome of which is quite unpredictable, as can be seen from the latest cyberattacks that have taken place since February 2022, one of the largest of which was a cyberattack on the Kyivstar mobile network.

Conclusion

Thus, in the current era, Ukraine is deeply cognizant of the perils associated with cybercrime and cyberterrorism, acknowledging these as grave manifestations that carry far-reaching, transnational consequences. Even though numerous measures have been put into place, the nation remains exposed to substantial risks stemming from potential cyberterrorist assaults. As a result, a clear and pressing necessity exists, recognized at the highest levels of government, to confront and effectively counteract the menace posed by cyberterrorism. At this critical moment, the overarching goals centered around fortifying cyber security infrastructures stand out as indispensable. The situation has deteriorated to a point of crisis, presenting dangers not solely to the sovereignty of individual countries but also to imperil the broader landscape of regional security. Hence, it becomes essential for Ukraine to forge a tight-knit alliance with the European Union (EU), aiming to erect a formidable coordination entity. This coalition would not merely concentrate on the legal dimensions involved. Still, it would also prioritize the creation and execution of sophisticated technical security strategies, all geared towards thwarting cyberterrorism across the region. This expanded collaboration signifies a pivotal shift towards a more integrated and comprehensive approach to cyber security. By leveraging the collective

expertise and resources of Ukraine and the EU, this initiative aims to bolster defensive capabilities against the evolving threats of cybercrime and cyberterrorism. Through the establishment of this coordination group, the focus extends beyond mere reactionary measures, emphasizing proactive strategies that anticipate and mitigate potential cyber threats. This collaborative endeavor underscores the importance of international cooperation in safeguarding against cyber aggression, highlighting the shared responsibility in maintaining cyber security and regional stability amidst an increasingly digital world.

References:

Agreement between Ukraine and the European Police Office on operational and strategic cooperation, No. 984_001-16, dated July 12, 2017. (In Ukrainian). https://zakon.rada.gov.ua/laws/show/984_001-16?find=1&text=%EA%B3%E1%E5%F0

Bilan, I. A. (2023). Osoblyvosti zastosuvannia shkidlyvoho prohramnoho zabezpechennia spetssluzhbamy krainy-ahresora [Peculiarities of the use of malicious software by the special services of the aggressor country]. *Information and Law*, *2*(45), 139-152. (In Ukrainian)

Constitution of Ukraine. (1996). Website Verkhovna Rada of Ukraine. (In Ukrainian). http://zakon5.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80

Doctrine of Information Security. (2016). Website of the Verkhovna Rada of Ukraine. (In Ukrainian). https://zakon.rada.gov.ua/laws/show/47/2017#Text

Kogut, Y. I. (2023). *Kiberteroryzm (istoriia, tsili, obiekty)* [Cyberterrorism (history, goals, objects)]. Kyiv: Consulting company "SIDCON". (In Ukrainian)

Largest cyberattacks against Ukraine since 2014. Infographics. New time. – 2017. (2014). (In Ukrainian). https://nv.ua/ukraine/events/krupnejshie-kiberataki-protiv-ukrainy-s-2014-goda-infografika-1438924.html

Ministry of Foreign Affairs of Ukraine: Association agreement between Ukraine and the EU (abstract of the main sections of the agreement). (n.d.). (In Ukrainian). https://mfa.gov.ua/ua/about-ukraine/european-integration/ua-eu-association

Official website of the Cyber Police of Ukraine. (2024). (In Ukrainian). https://cyberpolice.gov.ua/contacts/

On Approval of General Requirements for Cyber Protection of Critical Infrastructure Objects. (2019). Resolution of the Cabinet of Ministers of Ukraine. Website of the Verkhovna Rada of Ukraine. (In Ukrainian). https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text

On Information. (1992). Law of Ukraine. Website of the Verkhovna Rada of Ukraine. (In Ukrainian). https://zakon.rada.gov.ua/laws/show/2657-12#Text

On National Security". (2018). The Law of Ukraine. Website of the Verkhovna Rada of Ukraine. (In Ukrainian). https://zakon.rada.gov.ua/laws/main/2469-19#Text

On Protection of Personal Data. (2010). The Law of Ukraine. Website of the Verkhovna Rada of Ukraine. (In Ukrainian). https://zakon.rada.gov.ua/laws/card/2297-17

On State Secrets. (1994). The Law of Ukraine. Website of the Verkhovna Rada of Ukraine. (In Ukrainian). https://zakon.rada.gov.ua/laws/show/3855-12/find?text=%EA%F0%E8%F2%E8%F7#Text

On the Basic Principles of Ensuring Cybersecurity in Ukraine. (2017). The Law of Ukraine. Website of the Verkhovna Rada of Ukraine. (In Ukrainian) https://zakon.rada.gov.ua/laws/main/2163-19#Text

On the Main Principles of Ensuring Cyber Security of Ukraine. (2017). The Law of Ukraine No. 2163-VIII dated October 05, 2017. (In Ukrainian). https://zakon.rada.gov.ua/laws/show/2163-19

On the Protection of Information in Information and Telecommunication Systems. (1994). Law of Ukraine. Website of the Verkhovna Rada of Ukraine. (In Ukrainian). https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80/find?text=%EA%B3%E1%E5%F0#Text

Petkov, S. V., Zhuravlyov, D. V., Drozd. O. Y., & Drozd, V. G. (2022), *Kiberbezpeka v Ukraini: normatyvna baza, komentari ta roziasnennia, aktualna sudova praktyka* [Cybersecurity in Ukraine: regulatory framework, comments and clarifications, current case law], Kyiv: TsUL.

Strategy of Military Security of Ukraine No. 121/2021, dated March 25, 2021. Website of the Verkhovna Rada of Ukraine. (In Ukrainian). https://zakon.rada.gov.ua/laws/show/121/2021#Text

The President Approved the Cyber Security Strategy of Ukraine. (2016). President of Ukraine Petro Poroshenko. Official online representation. (In Ukrainian). https://www.president.gov.ua/news/prezident-zatverdiv-strategiyu-kiberbezpeki-ukrayini-36856

The State Center for Cyber Protection and Countermeasures against Cyber Threats has been established at the State Intelligence Service. (2015). State Service of Special Communications and Information Protection of Ukraine. (In Ukrainian). http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=156473&cat_id=119123

Zhora, V. (2022). State service of special communications and information protection of Ukraine. Russia's cyber tactics: Lessons learned. *CIP*. (In Ukrainian). https://cip.gov.ua/en/news/russia-scyber-tactics-lessons-learned-in-2022-ssscip-analytical-report-on-the-year-of-russia-s-full-scale-cyberwaragainst-ukraine

Appendix

Table 1. Legislative Acts of Ukraine that address cybersecurity and information protection issues

Name of the legislative act	Acceptance date	Key points of cybersecurity in the legislative act
The Law of Ukraine "On Information" (*1992*)	dated October 02, 1992	The law defines the legal framework for the dissemination of information in Ukraine. It not only guarantees citizens the right to receive, disseminate and search for information, but also establishes transparency and openness in relations between the state and society. The law also regulates the protection of personal data, including the need to ensure confidentiality and security of processing. It establishes liability for violations of the rules of information dissemination and data protection, including administrative and criminal sanctions.
The Law of Ukraine "On Protection of Information in Information and Telecommunication Systems" (*1994*)	dated July 05, 1994	The Law establishes the legal and organisational framework for the protection of information in information and communication systems. Its main purpose is to ensure the confidentiality, integrity and availability of information in these systems. The law defines the rights and obligations of subjects of information relations and establishes requirements for information protection, including cryptographic protection measures, access control, technical and organisational measures. In addition, the law establishes procedures for organising information protection in government agencies, enterprises, institutions and organisations, regardless of ownership. An important part of the law is the definition of liability for violation of information protection rules, including administrative and criminal sanctions.
The Law of Ukraine "On State Secret" (*1994*)	dated January 21, 1994	The Law establishes the legal basis for the protection of information having the status of a state secret. The main purpose of this law is to ensure the confidentiality and inviolability of information constituting a state secret, i.e. information to which access is restricted and which may harm national interests, national security or other important areas. The main aspects of the law include the definition and classification of information as a state secret, and the establishment of procedures for its identification, registration, use, storage and disclosure. The law also establishes liability for non-compliance with the requirements for the protection of state secrets, as well as for procedures for their disclosure and investigation of violations.
The Law of Ukraine "On the Basic Principles of Cybersecurity in Ukraine" (*2017*)	dated October 05, 2017	The Law establishes the general principles, goals and organisational framework for ensuring cybersecurity in Ukraine. It defines the responsibilities of state institutions, operators of critical information infrastructure and users of information and communication systems.

The Law of Ukraine "On Protection of Personal Data" (*2010*)	dated June 01, 2010	The law establishes rules for the collection, storage and processing of personal data, which are important for ensuring the confidentiality and security of information in cyberspace.
The Law of Ukraine "On National Security" (*2018*)	dated June 21, 2018	The Law establishes that the state policy in the field of national security and defence includes military, foreign policy, national, economic, information, environmental security, security of vital infrastructure, and cyber security in Ukraine.
Resolution of Cabinet of Ministers of Ukraine "On Approval of the General Requirements for Cybersecurity of Critical Infrastructure Facilities" (*2019*)	dated June 19, 2019	It is worth noting that this resolution establishes certain standards and requirements for the protection of facilities considered important for the functioning of the state. These requirements include mandatory measures to monitor, detect and respond to cyber threats, ensure data and infrastructure backup, and improve the skills of cybersecurity personnel. This resolution is an important document for ensuring the resilience of critical facilities to cyber attacks.

Source: compiled by the author based on the references.

Table 2. Provisions of the Constitution of Ukraine that provide for the protection of information and peculiarities of its disclosure

Article of the Constitution of Ukraine	Its provisions on data protection
Article 17	says that information security protection is one of the most important functions of the state and is the business of the entire Ukrainian people.
Article 18	requires that Ukraine's foreign policy activities be aimed at ensuring national interests and security by maintaining peaceful and mutually beneficial cooperation with members of the international community in accordance with generally accepted principles and norms of international law.
Article 106	stipulates that the President plays an important role in ensuring national security, including cybersecurity, in particular as the chairman of the National Security and Defence Council, which is responsible for national security and defence and which submits proposals to the Parliament on the appointment and dismissal of the head of the Security Service of Ukraine.

Source: compiled by the author based on the reference (*Constitution…, 1996*)

1. Council of Europe Convention on Cybercrime.
   - Ukraine is a signatory to this Convention and has committed to cooperate with other parties in the fight against cybercrime and cybersecurity.

2. European Union Cybersecurity Strategy.
   - Ukraine cooperates with the European Union within the framework of its cybersecurity strategy to share experiences and jointly respond to cyber threats.

3. The UN Cybernorms.
   - Ukraine participates in the UN initiative to develop international norms and rules in cyberspace to ensure international cybersecurity and stability.

4. Joint NATO and Ukraine Cyber Security Strategy.
   - Ukraine cooperates with NATO in the field of cybersecurity to strengthen its defence capabilities and protect critical information infrastructure.

5. Confidence building in OSCE cyberspace.
   - Ukraine engages in dialogue and cooperation within the OSCE to build confidence and security in cyberspace.

6. The International Code of Cyber Research.
   - Ukraine may participate in the development and maintenance of international norms and rules for cyber research to ensure the stability and security of cyberspace.Ukraine may participate in the development and maintenance of international norms and rules for cyber research.

7. International initiatives in the field of cyber defence.
   - Ukraine can participate in various cyber defence initiatives and programmes initiated by various international organisations and partners.

Figure 1. International treaties and agreements of Ukraine in the field of cyber security
Source: compiled by the author based on the references (*Bilan, 2023*; *Petkov, 2022*)