DOI: 10.47743/eurint-2024-FOC • November 2024 • VOLUME 11

The impact of the Ukrainian-Russian war on European cybersecurity

Andreea-Cosmina Foca ✉
Alexandru Ioan Cuza University of Iași, Romania

Abstract: In recent years it has been observed that conflicts have changed in the context of globalization. The military strategies have been influenced by innovations in the field of communication and information technology, giving modern warfare a fresh boost. More specifically, the concept of military warfare experienced changes, as well as the military strategies, to reduce deaths and accomplish political and military objectives at minimal cost. In this sense, the Ukrainian-Russian war serves as the most recent example, where cyberspace was also used as a battleground. The fact that cyberattacks are used in coordination with conventional military attacks against the Ukrainian territories shows that they are an important component of the military strategy to win the war. At the same time, recent events have already shown us that as the conflict escalated, Russian cyberattacks also targeted European nations who openly backed the Ukrainian cause. The cyberspace has become a new battleground where states are not sufficiently prepared to prevent and stop such cyberattacks, especially as they become more complex. In this regard, the current paper analyses the parts of the literature review which describe to what extent the Ukrainian-Russian war affected European cybersecurity. This study also aims to highlight the dangers and vulnerabilities faced by European governments in this regard and provide specialized solutions for cyber security practitioners or policymakers. The main research question seeks to analyse to what extent the use of cyber-attacks in a Russian-Ukrainian war affects European cybersecurity.

Keywords: cyberspace, cybersecurity, cyberattacks, the European regulatory framework, cybersecurity perspectives, cybersecurity solutions, artificial intelligence

Introduction

Besides the traditional threats to security brought about by armed conflicts, the new social changes also provide several threats to security. “National security, which previously focused on defending the state against physical conditions, now also requires defense through networks due to the advancing digital era” (Budiman et al., 2023, p. 1791). The new challenges to security come from cyberspace which has become an important area of warfare.

✉PhD student at Doctoral School of Political Science, Alexandru Ioan Cuza University of Iași, Romania; e-mail: focaandreea11@gmail. com.

Cyberattacks and unlawful cyberactivity on the Internet can put people's safety and national security at risk. "These attackers have the resources and expertise to launch massive Internet attacks against other nations, to cause damage or disrupt services, such as shutting down a power grid, but also to gain strategic advances" (Gabrian, 2022, p. 44).

The Russian-Ukrainian war is a typical example of cyberconflict where attackers find it easier to access and compromise Ukrainian data systems. The daily reliance on the Internet and the the expansion of digitization in the most vital sectors allowed Russian cyber attackers to carry out the offensive plan by conducting initial cyberattacks on government institutions and other vital facilities, followed by military operations. „Cyberattack dynamics have demonstrated that they are utilized as acts that come before any other kind of action, and in order to accomplish the desired outcomes, they can either continue at a higher intensity or signify the start of a new phase of a military operation" (Radu, 2023, p. 45). So, to defend Ukraine's vital infrastructure against pro-Russian hackers, several partner countries have also become targets of cyberattacks. At the international level, European states emphasized the necessity for collaboration among alliances to ensure the security of NATO's eastern region. In order to effectively handle conflicts in a virtual world, coalitions must adjust to the new circumstances and overcome new types of obstacles.

The purpose of the present paper will be reached using content analysis - a qualitative research approach. Through the content analysis there was undertaken a literature review on how the Ukrainian-Russian war affected European cybersecurity. The content analysis focused on hybrid conflict and cyberattacks, European normative framework on cybersecurity, and multiple cases of cyber actions that targeted EU member states and NATO allies. In all, 21 sources were examined, including 7 books, 4 international reports, 5 journal articles, 2 bulletins, 1 strategy book, 1 policy paper, and 1 policy document. The primary keywords employed were cybersecurity; European legal framework; Russian Ukraine war; cyberattacks; cybersecurity strategies; European cybersecurity defense; cybersecurity policy, cyberspace; cybersecurity implications; cyber threats; Russian cyberattacks; EU cybersecurity strategy; regulations; cybercrime prevention; artificial intelligence;

1. Cyberspace - cybersecurity - conceptual boundaries

It is considered that cyberspace began to structure within the development of information and communication technologies (ITC), but it is more than that, including computer data and interactions between devices and their users (Jentkiewicz et al., 2022). The next level came with the emergence of the Internet that expanded information and communication technologies and made critical infrastructures increasingly Internet-based. Thus, „Technology in cell phones, the internet, and

computers has revolutionized various perspectives of human life over the last few decades" (Yarali et al., 2022, p. 1). In light of this, it is evident that the world has transformed in terms of efficiency, productivity, economic growth, and succeeded in transforming numerous facets of human existence. "Information and communication technologies (ICT) allow huge amounts of information to be stored, processed, accessed, searched, transmitted, exchanged, and disseminated, regardless of geographic distance" (Ghernaouti, 2013, p. 18). These profound changes have opened up new opportunities for the global economy, and in order to benefit from these opportunities, individuals and the corporate community have constructed the infrastructure and financial instruments required to increase profits. At the same time, the technological developments have given way to harmful activities. Therefore, it has become necessary to implement legal solutions which will make it possible to organize an effective and efficient system for protecting the information resources of public entities, entrepreneurs and also citizens (Jentkiewicz et al., 2022, p. 11).

Because of this, several cybersecurity specialists describe this area in terms reminiscent of the Wild West to draw attention to the lack of adequate cybersecurity measures in the midst of the digital era. Living in the postmodern age, brought a series of new problems, one of these consisting in the fact that more and more people become victims on the Internet. "Internet technologies are facilitators for many kinds of infringements: theft; sabotage of information; copyright infringements; breach of professional secrecy, digital privacy, or intellectual property; dissemination of illegal contents; competing attacks; industrial espionage; breach of trademark laws; dissemination of false information; denial of service; various frauds; money laundering - the list of possible offenses goes on" (Ghernaouti, 2013, p. 19). It became clear that an open and free cyberspace exposed individuals and societies to new risks and reveals vulnerabilities that did not exist until that moment. In this regard, the Internet altered also how individuals interacted with each other, and more than that, it allowed new types of crimes. „Criminals are now carrying out their activities using a unique perspective with the help of the internet" (Yarali et al., 2022, p. 3). The offenders can easily carry out illicit activities from any location worldwide under anonymity or fake accounts, decreasing the risk of being identified. "Frequently, fraudsters pose as entities known to the Internet user, such as a bank or a manager of his messaging service, and ask him - always with some credible justification - to communicate his personal data by phone, through a website or by mail" (Ghernaouti, 2013, p. 55). In terms of security threats, cyberspace is therefore an environment from which a series of risks arise. This happens because of "the generally poor awareness of cybersecurity and cyber hygiene, particularly amongst vulnerable users such as the elderly, has led to a dramatic increase in the number of cybercrime victims" (Interpol, 2021, p. 12).

In parallel, the cyberattacks that are specifically directed at the country's critical infrastructures have the potential to cause chain reactions in cyberspace, therefore, even if the attack was directed towards the state's vital infrastructure, it

has the potential to endanger human life. "Ensuring reliability against threats seems to dominate national security discussions today and raises concerns when thinking about future warfare" (Reveron, 2012, p. 14). Given this, the cybersecurity concept has been developed to protect data and control access to networked systems that contain data. "Cybersecurity refers in general to methods of using people, process, and technology to prevent, detect, and recover from damage to confidentiality, integrity, and availability of information in cyberspace" (Bayuk et al., 2012, p. 21). "Cybersecurity is typically defined as the protection of confidentiality, integrity and availability of computer data and systems in order to enhance security, resilience, reliability and trust in ICT" (Interpol, 2021, p. 10).

To respond to "social engineering" threats, it is important that proactive security measures detect attacks that are launched before they cause damage. Also, as part of security management, it is essential to recover damaged systems after attacks. "Because information technology allows diversity, redundancy, and reconstitution for the data and programs required to operate systems, information security professionals expect that damage can be completely allayed" (Bayuk et al., 2012, p. 21).

2. Cyberattack - definition and terminology issue

The word "cyberattack" lacks a widely accepted definition, thus the notion has been given a variety of interpretations. A cyberattack can refer to an attack on the health system, the power grid or a national defense system. Also, cyberattacks may also be conducted with the intent to cause harm to individuals or influencing public opinion (cyber propaganda). "Some have minor impacts and can often be attributed to straightforward delinquency, while others could have drastically negative effects on people, organizations, and states, and could be linked to crime, terrorism and war" (Ghernaouti, 2013, p. 160). Consequently, it's evident that due to its complexity, the term cannot refer to particular actions. "By definition, cyberattacks are directed against computers or networks" (Reveron, 2012, p. 49). Cyberattacks are mostly directed against computer and telecommunication systems involved in critical infrastructures of a state. They are more effective than conventional fighting techniques and can be used as military weapons. Hacking government websites and falsifying information with the intention of misleading the public and winning support are also examples of cyberattacks against states. Additionally, the fact that the ICT environment has been connected to the Internet without any prior safety precautions contributed to the weakening of the critical infrastructures that ICT supports. The attacks on vital infrastructure are intended to bring down state institutions and components that safeguard the national security, public safety, and economy of a state. "Communications, electricity or water distribution infrastructures, and the infrastructures for financial or health institutions, for example, can be considered as critical" (Ghernaouti, 2013, p. 152). Since

information and communication infrastructures are used to access vital infrastructures, such as banking, electricity, and telecommunication systems, an adversary state may use cyberattacks to obstruct government operations. "Opponents of states or organizations can attack systems or infrastructures in order to use them, destroy them, or find material for blackmail" (Ghernaouti, 2013, p. 152).

The experts in the field also address another topic that includes differentiating cybercrime activities from cyberattacks with clarity, initially determining whether the attack caused any specific offenses that are subject to legal punishment. "Cybercrime is defined as offenses committed against computer data, computer data storage media, computer systems, service providers" (Interpol, 2021, p. 10). "For an attack to be identified and treated as a crime that breaks the law, that law by definition must already exist" (Ghernaouti, 2013, p. 160). More specifically, referring to the cybercrime activities committed within Romanian borders, we note that the Romanian criminal law regulates and incriminates a number of illicit activities such as computer fraud, fraudulent financial operations, computer forgery, illegal access to computer systems, unauthorized transfer of computer data, and child pornography. At the same time, when it comes to cyber incidents, it is important to clarify if it is a cybercrime incident or cybersecurity incident in order to know where to look for a solution. Therefore, while a cybersecurity incident needs to be reported to a computer emergency response team (CERT), a cybercrime incident can be handled by the criminal justice system. "In some cyber incidents, it may be unclear at the start whether it is a cybersecurity incident affecting personal, corporate or national infrastructure, or if it is a cybercrime incident where an actual crime is being committed, or if it is a combination of the two" (Interpol, 2021, p. 11).

3. Cybersecurity under EU law - understanding the context

The Council of Europe Convention on Cybercrime provided a European legal framework that marked a significant advancement in the fight against international cybercrime. "The aforementioned Convention on Cybercrime was the first, and only, international treaty on crimes committed via the Internet and other computer networks" (Jentkiewicz et al., 2022, p. 57). In 2001, European and non-European countries developed and signed the Convention on Cybercrime, also known as the Budapest Convention, with the purpose to harmonize the domestic legislation, to provide necessary for the investigation and prosecution, and intensify cooperation between states in addressing the problem of cybercrime. "The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with offenses against and by means of computer systems and data, such as illegal access, illegal interception, data and system interference, computer-related fraud, child sexual exploitation material or other violations of network security" (Interpol, 2021, p. 26).

As part of this continuous effort, the European Union has implemented mandatory legal instruments to tackle computer crime, including the Council Framework Decision 2005/222/JHA on attacks against information systems, European Parliament and Council's Directive 2013/40/EU on attacks against information systems, which added solutions and new types of criminal offences, Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information system across the European Union and the Revised NIS Directive (NIS 2) in response to the COVID-19 pandemic's acceleration of the digital transformation (Jentkiewicz et al., 2022). Regarding the last document, "the second NIS Directive seeks to bolster cybersecurity requirements, address the security of supply chains, reinforce obligations for reporting, along with a general strengthening of enforcement procedures with better supervision, including through an improved harmonization of sanctions across countries" (Barichella, 2022, p. 19). Being also part of the European normative framework in cybersecurity, another reference document is represented by the original European strategy that was launched in 2013. Subsequently, at the end of 2020, the strategy was revised, focusing on securing essential services to bolster Europe's resilience against cyberattacks. "It also emphasizes collaboration with global partners to ensure cybersecurity and stability in the digital world" (Budiman et al., 2023, p. 1792).

As for legal measures, it is worth mentioning the development of "Computer Security and Response Team" (CSIRT), requiring Member States to be well equipped to respond quickly to cyber security incidents. As part of this ongoing commitment, it is important to highlight the work of the European Cybercrime Center (EC3) and the European Agency for Cybersecurity (ENISA), which offer operational support, technical expertise, and assistance to EU member states in combating cybercrime. "However, much like the EU Agency for Cybersecurity, none of these various frameworks or institutions possess sufficient competences, like sanctions, to enforce compliance with EU-level cyber norms" (Barichella, 2022, p. 18).

3.1 Understanding the context

Given the increasingly digitized world, the development of new technologies presents threats to people's daily lives as well as a wide range of interests, being employed in harmful crimes or cyberattacks. "In recent years these cyberattacks, whether random or targeted, have become much more professional, and their targets manifold, ranging from states and public authorities to global enterprises, SMEs (small and medium - sized enterprises), critical infrastructure and individuals" (Bartsch & Frey, 2018, p. 65). This is because technological advancements have fueled the growth of the European economy and remain a vital resource upon which the key sectors depend. Being actually the other side of the coin where a number of cybercrime activities have targeted the private sector and Europeans, impacting the EU economy alike. "Cybersecurity incidents, be it intentional or accidental, are

increasing at an alarming pace and could disrupt the supply of essential services we take for granted such as water, healthcare, electricity or mobile services" (European Commission, 2013, p. 3). Besides this, new social events, such as the COVID-19 pandemic, caused a rise in the number of workers who work remotely and caused us to move many of our daily tasks online, increasing our vulnerability to cybercrime. "Law enforcement around the world has witnessed first-hand the unique criminal aspects the COVID-19 pandemic was breeding, especially the diversifying and growing impact of cybercrime" (Interpol, 2021, p. 3).

In the context of Russian aggression against Ukraine, the pro-Russian hacker groups had launched cyberattacks against European states and beyond, alarming European governments. "The pro-Russian hacktivist group Killnet, that ramped up its activities since the Russian war of aggression against Ukraine, claimed responsibility for the most DDoS (Distributed Denial of Services) attacks launched in 2022 against targets in EU and beyond" (Europol, 2023, p. 17). Fortunately, these DDoS attacks caused very little disruption, given the high cybersecurity measures at the level of the European institutions and states. "These attacks include the one launched against the European Parliament and many others targeting the infrastructure of EU countries" (Europol, 2023, p. 17).

3.2. Consequences of the Ukrainian-Russian war over Ukrainian cybersecurity

The use of cyberattacks and operations have increased during the Russian-Ukrainian war indicating that ICTs have generated new weapons with the same disruptive potential as conventional ones. In this respect, on February 24, 2022, Russian hacktivists launched cyber-attacks on Viasat's european KA-SAT satellite communications service network which didn't threaten government or military objects, but impacted mostly the civil population and other European broadband customers. Another example concerns the end of March 2022, when the cyberattack on the Ukrainian telecommunications company Ukrtelecom cut off access to internet and telecommunications services, causing a major internet outage in the country. Besides these, many others have targeted governments, local authorities, military and law enforcement field and telecommunications services. The majority of those cyberattacks were destructive attacks, using a series of "wiper" attacks to destroy data on targeted computers. "A malware wiper attack on 25 February 2022 against a border control station slowed the process of allowing refugees crossing into Romania" (Duguin & Pavlova, 2023, p. 11). An additional type of cyberattack known as disruptive attacks, consisted in launching DDoS attacks which affected the public and financial sectors. "These types of attacks have been particularly hard-felt by sectors related to critical infrastructure - such as public administration, energy, ICT, and finance - impacting the connectivity and availability of vital services" (Duguin & Pavlova, 2023, p. 17). Also, the Russian launched desinformation operations and propaganda in order to prevent public access to official information

or distort its meaning. “It is important to note that for the Russian Federation, ‘information confrontation’ or ‘information warfare’ is a broad concept and key enabler of its attempts to gain victory in current and future conflicts, and is not a separate function or domain from ‘cyber’ (Duguin & Pavlova, 2023, p. 13).

Due to the previously established security measures, the vital infrastructure of the Ukrainian state has not been affected by these attacks, despite their increasing frequency. ,,Ukraine’s experience defending against Russian cyber operations in the past decade has therefore formed a critical component of the country’s national cyber resilience” (Austin & Khaniejo, 2023, p. 6). Being the subject of cyber attacks even before the military invasion of 2014, Ukraine strengthened the resilience of its ITC infrastructure through cooperation with international partners and public-private partnership. “Since the 2014 Russian annexation of Crimea, Ukraine has significantly improved its cybersecurity posture, including with recent assistance from the European Union (EU) and Five Eyes (Australia, Canada, New Zealand, United Kingdom, and US or FVEY)” (Cyber Threat Bulletin, 2022, p. 3). At the same time, Ukraine’s IT army played an important role in preventing as well as launching thousands of cyber-attacks on the defense industry. “Once the war began, the cybercrime ecosystem shifted to targeting Ukraine in particular, creating a Ukrainian IT army estimated at around 215.000 volunteer affiliates targeting Russian state-sponsored media outlets” (Gabrian, 2022, p. 48). It is thus observed that in this conflict the hybrid threats have been fully exploited by the Russian armed forces, giving them a considerable advantage in taking over more Ukrainian territory. “Cyberattacks and operations are now an established type of military operation, and are being coordinated with, or synchronised around, kinetic military operations” (Duguin & Pavlova, 2023, p. 10).

3.3. Consequences of the Ukrainian-Russian war over European cybersecurity

Apart from Ukraine, Russian cyberattacks have targeted states that supported the Ukrainian cause, in this context, cyberattacks targeting American and European networks have been launched. “Both government and industry data have indicated increased cyber espionage efforts from Russian state-sponsored threat actors targeting the United States and European countries in response to its effort for Ukraine - indicating that while kinetic combat has not been directed at NATO countries, cyberspace for that purpose is already being used” (Kaushik, 2023, p. 5). In this regard, to further their cyber operations, Russian hacktivist sussed various cyber tools such as DDoS attacks against government websites (over Romania, Slovakia and the Czech Republic), spear-phishing emails, satellite communications service network attack (for instance, the attack over Viasat’s European KA-SAT satellite communication service network disrupted the activity in France, Germany, Greece, Hungary, Italy and Poland) or ransomware (for example, the Prestige ransomware attack disrupted the transport and logistics networks in Ukraine and

Poland). According to the Canadian Cyber Security Center's June 2022 Cyber Threat Bulletin, "Russian cyber actors have targeted government, academic, private sector, and critical infrastructure entities in Denmark, Latvia, Lithuania, Norway, Poland, the US, and Turkey for cyberespionage purposes, as well as entities in Finland and Sweden, both of whom applied for NATO membership following the Russian invasion of Ukraine in February" (Cyber Threat Bulletin, 2022, p. 5). Additionally, since the start of the invasion, nations in Eastern Europe like Romania and Poland have been the targets of Russian cybercriminals because they assisted the fleeing Ukrainians and acted as transit routes for NATO's supplies and weapons. Regarding this, "on 25 February, a destructive cyberattack targeted a border control station with the objective of hampering the flow of refugees into Romania, forcing local officials to manually process people crossing the border" (Barichella, 2022, p. 11).

Following a request from the Ukrainian government, the European Union activated the Computer Emergency Response Team to support Ukraine's cyber defense. As a result, at least 23 EU member states organizations were the target of cyberattacks according to the CERT-UE Report, most targeted being Poland, Latvia, Estonia and Lithuania. At the same time, non-EU countries such as the UK were targeted by pro - Russian hacktivists who launched DDoS attacks, disrupting the functioning of web pages, as happened with the UK charity art sale. In addition to the European and non-European member states, the US was under DDoS attacks claimed by pro-Russia hacktivists, as a form of revenge towards the harsh sanctions imposed on the Russian government and for supplying military equipment to Ukrainian forces. "Killnet has claimed to carry out DDoS attacks against US airports, the White House, StarLink, various European governments websites, among others" (Kaushik, 2023, p. 4).

We can therefore conclude that cyberconflicts show us the complexity of new weapons and the evidence that cyberattacks combined with the deployment of conventional armed forces may be disruptive, and also using them irrationally could bring humanity dangerously close to the first worldwide conflict in cyberspace. We also noted that the rise of cyber conflict has accelerated the assimilation of cyber defense into national security plans. However, in this joint effort to ensure cybersecurity at the international level, it is essential that this regional conflict ends and leaves room for peace negotiations. In order to do this, major players and organizations on the global scene ought to participate more actively and promote peace agreements.

4. New perspectives on defending against cyberattacks

As we already saw in the case of cyberattacks on Ukraine, regarding its ability to withstand cyberattacks launched by Russian attackers, this was primarily due to the assistance provided over time by the international partners, especially after the annexation of Crimea. Also, the measures aimed at increasing the resilience of its

ITC infrastructure, improved its cybersecurity in the midst of military conflict. Even though it is a hard lesson, the ongoing Russia - Ukrainian war shows us that national cyber defense strategies alone do not provide sufficient protection against critical national infrastructure. ,,The strategic challenge for cyber defense is that the Internet is developing at such speed that it is almost impossible for any organization to master all the latest development situations" (Lakusic & Baltezarevic, 2022, p.150). The context in which we find ourselves is quite favorable for cyber attackers in the sense that it offers them multiple levers to carry out remote operations under a certain protection of their identification data. What I want to stress is that, in addition to international assistance, which, in the case of Ukraine, has truly protected the country's critical infrastructure, the private - public cooperation is also required to counter significant cybersecurity threats. To make the digital world safer, businesses and governments must work together and share relevant information in this regard. ,,Within any given nation state, adequate cybersecurity will require effective coordination and cooperation among governmental entities on the national and sub-national levels as well as the private sector and civil society" (Appazov, 2014, p. 66).

At the same time, it is imperative for states to allocate resources toward the specialization of personnel working inside their special structures, so they can get expertise and understanding of cutting-edge technologies employed in cybercrimes as well as cyberattacks. As modern technology advances, it will provide new opportunities to cyber attackers, increasing their operations. Currently, there is a lack of specialization among law enforcement officers regarding criminal networks which adapt to new environments and modern technical means much more quickly than authorities do. ,,This emphasizes the increasing need to provide specialized training, often of an interdisciplinary nature, for judges, magistrates, lawyers, and police officers" (Ghernaouti, 2013, p. 278). Also, human capacity development is necessary to prevent attacks in the digital environment; the problem here is informing users about cyberspace security measures, to be more aware of their actions in the online environment and to use appropriate cyber hygiene measures. By placing individuals at the center of security issues, information security can be strengthened, as criminal activity in the digital arena increasingly relies on users' deception and ignorance. Additionally, with artificial intelligence's promising potential, a fresh approach to stopping cyberattacks appears to be emerging.

5. Contrasting views on Artificial Intelligence assisting cybersecurity

Cybersecurity experts have included artificial intelligence (AI) in their analysis, trying to use the promising capabilities of emerging technologies in order to prevent cyberattacks. Thus, in the cybersecurity field, artificial intelligence is seen as a friend as well as a threat. On the one hand, cybersecurity analysts believe that there is need for more advanced measures to protect against cyberattacks as long as hackers have adapted their operating systems and communication networks to high

technologies. They have the advantage of performing operations at a low cost that generate high profits. At the same time, under anonymity, they can perform countless attacks. It is clear that for all the sophisticated tools acquired by attackers, the security officers do not have enough technique and skills to prevent potential attacks. In light of this, artificial intelligence and machine learning solutions can be used to improve cyber defense. New findings over the artificial intelligence impact on cybersecurity affirm the positive influence of AI-based technologies on organizational cybersecurity, helping organizations (such as firms, institutions) to protect their digital assets. Moreover, the benefits could be the ability to detect malware as well as other intrusion incidents. Given that human error is a primary vulnerability in the cybersecurity chain, introducing AI - driven task automation can solve this problem. „This objective is achievable through improved threat detection methods, where using unsupervised machine learning intrusion detection systems (IDS) enables the identification of even the smallest threats or attacks before they happen" (Jada & Mayayise, 2023, p. 6). „As stated by (Hariyanti et al., 2021), the automation of cybersecurity tasks reduces the need for human intervention, minimizes human intervention, and subsequently reduces the potential for human error throughout the entire security life cycle" (Jada & Mayayise, 2023, p. 6).

On the other hand, other cybersecurity analysts believe that artificial intelligence can cause adversarial attacks, increasing the threat of cyberattacks (Jada & Mayayise, 2023). Hackers can use AI technologies to carry out malicious attacks by sending personalized phishing emails to individuals and businesses or create chatbots in order to impersonate a famous person or someone in an influential position to trick victims to perform certain tasks. Thus, the risk of data privacy increases as long as individuals cannot discern between chatbot scams and real persons. „Other dangers that arise include deceptive trade practices, desinformation, resource depletion, and data sets" (Kaushik, 2023, p. 4). Another aspect consists in the fact that the implementation of AI solutions in organizations faces some limitations, requiring certain infrastructure and hardware components to function properly. „Another challenge lies in the compatibility issues caused by the continued use of outdated systems, programming languages, and overall technological infrastructure in many organizations " (Jada & Mayayise, 2023, p. 6). Thus, implementing AI solutions in organizations can be a very difficult task for some businesses, requiring a more complex organizational data management process. It is important to note that cyber - AI solutions do not fit all situations, being rather a matter of matching security solutions to the specific nature of each organization.

Therefore, it can be concluded that AI technologies can be a more appropriate solution to constantly evolving threats. To increase the level of protection, there is a need for issues related to the use of AI technologies to go beyond the decision-making level and materialize in a framework that regulates the use of these technologies. Meanwhile, policymakers and cybersecurity experts must work closely together to address the new challenges of AI technologies.

Conclusions

The globalization process and its latest phase of digitization have made the world economy more reliant on ITC infrastructures. In light of this, new opportunities have opened up new possibilities for criminal activities that have expanded in cyberspace, making it more difficult to identify and punish the perpetrators of these acts. Cybercrime has become one of the fastest-growing types of transnational crime that states are currently dealing with. Because of this, states are now more exposed to danger because these activities have the potential to jeopardise the critical infrastructure of the states. At the same time, cyberspace has become a new place of confrontation between states and non-traditional actors. In the context of the Russian-Ukrainian war, new complex weapons have been used by the Russian military, such as spear phishing attacks, wiper attacks, DDoS attacks and disinformation operations in order to further the military assault.

The fact that cyberattacks and its specific operations are not are not subject to international legal regulation, continue to be a major worldwide vulnerability. The absence of global consensus allows states and non-state actors to go ahead with their malicious intentions. In this given situation, NATO member states are unable to initiate a coordinated response against cyberattacks, placing them in a difficult position to act in accordance with Article 5. Like an allarm, the conflict the conflict made it clear to everyone the importance of cybersecurity measures in ensuring the security of critical infrastructure. Yet it is also essential to note that since 2014, Ukraine has received assistance in the field of cyber security that has contributed to the country's defense efforts in the area of cybersecurity. Therefore, bolstering cyber resilience and stepping up peace talks seem to me better measures to meet the right measures to meet the future security challenges.

Russian cyber attacks against European member states were unexpected, managing to disrupt for a short period of time government websites, the European network of satellite communication services and other key sectors. As a result, the attacks managed to threaten Europe's cybersecurity, forcing European governments to react in certain ways. At the same time, this draws attention to the need to intensify proactive cybersecurity measures, considering the benefits of newly developed, cutting-edge technologies like machine learning and artificial intelligence.

In light of the results obtained from this study, several key recommendations are proposed to enhance cybersecurity resilience. Firstly, it is recommended to accelerate the specialization of personnel in structures that fight against cybercrime, the procurement of modern technologies and equipment, as this could address the problem of the increase in cybercrime and cyberattacks. Secondly, policy makers should consider a cloose cooperation with private sector**,** given the evidence that private-public cooperation has the capacity to counter significant cybersecurity threats. Finally, further research is need to explore artificial intelligence solutions**,**

which remains underexplored and critical for improving proactive cyber security measures.

References

Appazov, A. (2014). *Legal aspects of cybersecurity*. University of Copenhagen, Faculty of Law. https://www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf

Austin, G., & Khaniejo, N. (2023). *Impact of the Russia - Ukraine war on national cyber planning: A survey of ten countries*. The International Institute for Strategic Studies, pp. 1–21. https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2024/01/impact-of-the-russiaukraine-war-on-national-cyber-planning_a-survey-of-ten-countries.pdf

Barichella, A. (2022). *Cyberattacks in Russia's hybrid war against Ukraine* (Policy Paper No. 281). Europe in the World, Jacques Delors Institute. https://institutdelors.eu/wp-content/uploads/dlm_uploads/2022/09/PP281_The-cybersecurity-dimension-of-the-war-in-Ukraine_Barichella_EN.pdf

Bartsch, M., & Frey, S. (2018). *Cybersecurity best practices*. Wiesbaden: Springer Vieweg.

Bayuk, J. L., Healey, J., Rohmeyer, P., Sachs, M. H., Schmidt, J., & Weiss, J. (2012). *Cyber security policy guidebook*. New Jersey: John Wiley & Sons, Inc.

Budiman, I., Salsabila, A. F., Mubarok, C. I., Rustiawan, N. F., & Zulfikar, R. A. (2023). Cybersecurity analysis in the context of the Russia-Ukraine conflict: Challenges, threats, and defence strategies. *Journal Ekonomi*, *2*(2), 1790–1796.

Cyber Threat Bulletin. (2022). *Cyber threat bulletin: Cyber threat activity related to the Russian invasion of Ukraine*. Canadian Centre for Cyber Security.

Duguin, S., & Pavlova, P. (2023). *The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict*. European Parliament, Directorate General for External Policies of the Union, Policy Department, Workshop.

European Commission. (2013). Joint communication to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions: Cybersecurity strategy of European Union: An open, safe, and secure cyberspace (JOIN/2013/01). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013JC0001

Europol. (2023). *IOCTA report: Cyber attacks—The apex of crime as a service*.

Gabrian, C. A. (2022). How the Russia-Ukraine war may change the cybercrime ecosystem. *Bulletin of "Carol I" National Defence University*, *11*(4), 43–49. https://doi.org/10.53477/2284-9378-22-92

Ghernaouti, S. (2013). *Cyberpower: Crime, conflict, and security in cyberspace*. Lausanne: EPFL Press.

Interpol. (2021). *National cybercrime strategy guidebook*.

Jada, I., & Mayayise, T. O. (2024). The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. Data and Information Management, 8(2), 100063. https://doi.org/10.1016/j.dim.2023.100063

Jentkiewicz, K. C., Radoniewicz, F., & Zielinski, T. (2022). *Cybersecurity in Poland: Legal aspects*. Warsaw: Springer.

Kaushik, A. (2023). *The war on Ukraine: A look at (underemphasized) Russian cyber operations*. GLOBSEC.

Kaushik, D. (2023). The impacts of cybersecurity and AI on businesses and individuals. *Journal of Student Research*, *12*(4), 1–10. https://doi.org/10.47611/jsr.v12i4.2282

Lakusic, M. M., & Baltezarevic, I. Z. (2022). National security and the challenges of the digital age. *Megatrend Revija*, *19*(2), 145–154.

Radu, C. C. (2022). Războiul ruso-ucrainean și impactul său asupra securității cibernetice în NATO și în UE. *Gândirea Militară Românească, 4,* 38–55. https://doi.org/10.55535/gmr.2023.4.01

Reveron, D. S. (2012). *Cyberspace and national security: Threats, opportunities, and power in a virtual world*. Washington: Georgetown University Press.

Yarali, A., Joyce, R., & Sahawneh, F. (2022). *Cybersecurity and digital forensics: Challenges and future paradigms*. New York: Nova Science Publishers.