ppi 201502ZU4645
Esta publicación científica en formato digital es continuidad de la revista impresa
ISSN-Versión Impresa 0798-1406 / ISSN-Versión on line 2542-3185Depósito legal pp
197402ZU34

CUESTIONES POLÍTICAS

Instituto de Estudios Políticos y Derecho Público "Dr. Humberto J. La Roche"
de la Facultad de Ciencias Jurídicas y Políticas de la Universidad del Zulia
Maracaibo, Venezuela

Vol.41 | Nº 78
Julio
Septiembre
2023

Cuestiones Políticas Vol. 41, Nº 78 (2023), 326-344
IEPDP-Facultad de Ciencias Jurídicas y Políticas - LUZ

Identification of new threats to the national security of the state

DOI: https://doi.org/10.46398/cuestpol.4178.23

Ivo Svoboda *
Mykhailo Shevchuk **
Oleksandr Shamsutdinov ***
Pavlo Lysianskyi ****
Oleksii Voluiko *****

Abstract

The objective of the article was to identify new threats to the national security of countries and, at the same time, to determine the adaptation tasks related to their identification. The synergistic approach, comparative legal analysis methods and foresight were the main tools of this research. Manipulation actions involving deep forgeries are spreading rapidly. Autonomous weapons with artificial intelligence are used to create negative fake events. Criminal use of users' smart devices to create a unique behavioural profile has been detected. New cyber threats to Ukraine's national security during the military conflict are characterized by attempts to disrupt critical infrastructure. It is concluded that "cyber looting" has emerged with the use of social engineering methods. The activities of the Belgian Center for Cyber Security (CCB) are a positive example of the identification of new cyber threats in the countries of the European Union EU. Furthermore, CCB performs activities related to the identification, monitoring and analysis of online security issues. Coordination between relevant services and agencies, public authorities, private sector and academia is ensured.

Keywords: cyber warfare; deep forgery; cyber security; social engineering; cyber resilience.

* Associate Professor, Guarantor of Security Management Studies, Department of Security and Law, University of Regional Development and Banking Institute, AMBIS, a.s. Vyská škola, 180 00, Prague, Czech Republic. ORCID ID: https://orcid.org/0000-0002-0941-4686

** Candidate of Science of Law, Doctoral Student, Department of Constitutional Law, Administrative Law, Financial Law, Leonid Yuzkov Khmelnytskyi University of Management and Law, 29000, Khmelnytskyi, Ukraine. ORCID ID: https://orcid.org/0000-0001-7549-6344

*** Ph.D. in Law, Leading Researcher, Interagency Research Center on Problems of Combating Organized Crime at the National Security and Defense Council of Ukraine, 03035, Kyiv, Ukraine. ORCID ID: https://orcid.org/0000-0002-9325-9227

**** Graduate Student, Department of Political Theories, National University "Odesa Law Academy", 65009, Odesa, Ukraine. ORCID ID: https://orcid.org/0000-0003-3997-9335

***** Candidate of Juridical Sciences, Associate Professor, Head of the Department of Legal Support of the Activity of the National Guard of Ukraine, Kyiv Insitute of the National Guard of Ukraine, 03179, Kyiv, Ukraine. ORCID ID: https://orcid.org/0000-0002-0894-5004

Recibido el 25/04/23 Aceptado el 17/06/23

Identificación de nuevas amenazas a la seguridad nacional del Estado

Resumen

El objetivo del artículo fue identificar nuevas amenazas a la seguridad nacional de los países y, al mismo tiempo, determinar las tareas de adaptación relacionadas con su identificación. El enfoque sinérgico, los métodos de análisis jurídico comparado y la previsión fueron las principales herramientas de esta investigación. Las acciones de manipulación que involucran falsificaciones profundas se están extendiendo rápidamente. Se utilizan armas autónomas con inteligencia artificial para crear eventos de falsos de carácter negativo. Se ha detectado el uso delictivo de los dispositivos inteligentes de los usuarios para crear un perfil conductual único. Las nuevas amenazas cibernéticas a la seguridad nacional de Ucrania durante el conflicto militar se caracterizan por intentos de interrumpir la infraestructura crítica. Se concluye que ha surgido el "saqueo cibernético" con el uso de métodos de ingeniería social. Las actividades del Centro para la Seguridad Cibernética de Bélgica (CCB) son un ejemplo positivo de la identificación de nuevas amenazas cibernéticas en los países de la Unión Europea UE. Por lo demás, CCB realiza actividades relacionadas con la identificación, seguimiento y análisis de problemas de seguridad en línea. Se garantiza la coordinación entre los servicios y organismos pertinentes, las autoridades públicas, el sector privado y el académico.

Palabras clave: guerra cibernética; falsificación profunda; seguridad cibernética; ingeniería social; resiliencia cibernética.

Introduction

The evolution of information and cyberspace is the main factor in the development. Globalization has led to a strong dependence on electronic communications. The reshaping and redefinition of technological processes have caused large informational changes in different countries (Cristea, 2020). The consequences of the application of 5G technology, artificial intelligence, and the Internet of Things may become a threat to national security (Li and Liu, 2021).

In the same context, the role of interstate competition and conflicts worsened. The narratives have been denied with the use of digital diplomacy and subversive disinformation operations (Devanny *et al.*, 2022). A new battlefield was created, in which military operations involve sophisticated digital technologies (Ştefănescu and Papoi, 2020). The online activities of special services, armed forces and related non-state actors have become increasingly intense. Countries began to prepare guidelines for cyber war. Training has been conducted to practice cyber tactics such as espionage, information theft, disinformation, hacking, and malware.

Threats from the virtual environment are spreading to critical infrastructure, government bodies, communication systems, and citizens. Fake messages distributed via smart devices form a new space of conflict that does not depend on geographical location (Sługocki and Sowa, 2021). Deepfakes can contribute to pressure and shaping the process of making wrong decisions by individuals or organizations (Farid, 2021).

The Russian-Ukrainian war provides relevant information about what types of cyber threats will appear in future cyber conflicts (Guitton and Fréchette, 2023). The existing and emerging threats require the improvement of specific means of intelligence and response, continuous increase in their effectiveness. The response to hybrid threats is implemented through an integrated process. This process is influenced by the difficulties of their identification and forecasting because of their mobility and the intensity of their impact.

The main task of national security organizations is to guarantee the protection of citizens from relevant threats. The priority is also to preserve the economic sustainability of national institutions. The tasks of national security organizations are actions based on assistance to public authorities responsible for decision-making in the country. They are responsible for ensuring that the information is correct and up-to-date (Dobák, 2021). Activities in the field of national security protection should be based on timely identification of possible threats and preparation of appropriate countermeasures.

Particular attention should be paid to identifying vulnerabilities and strengths of the state and society. Priority should be given to the development of opportunities for further protection of national interests (Reznikova, 2022). At the same time, it is expedient to update the security environment transformation vectors. The result will be a statement of strategic goals and priorities of state policy in the field of national security.

The military conflict on the territory of Ukraine requires quality solutions in terms of the forms, methods and procedures of using state resources to achieve political goals in a cross-border context (Semenenko and Frolov, 2023). The Russian Federation uses military, informational and psychological, as well as economic and political resources to the maximum possible extent. The elements of the information technology component of the hybrid war on the part of the aggressor country are significantly strengthened.

The uncertainty of the situation related to the military aggression of the Russian Federation in Ukraine leads to significant difficulties in the process of policy making in the field of national security. Emerging and developing threats lead to the need to identify them, strengthen and revise traditional security mechanisms. The implementation of adaptive management in the field national security is becoming especially relevant.

In view of the foregoing, the aim of this research is to identify new threats to the national security of countries and new tasks related to their identification. The aim involved the fulfilment of the following research objectives:

1. Determine the current trends in the legislative regulation of national security protection using the example of cyber security in the EU and Ukraine;
2. Identify new types of cyber threats and the current state of their identification;
3. Analyse the implementation of mechanisms for identifying new cyberthreats using the example of Belgium for the possible implementation of relevant positive experience in Ukraine.

1. Literature review

The study by Cristea (2020) was used as a background for this research, which was focused on the role of the evolution of security threats in the national and international context. Particular attention is paid to the existing problems related to the implementation of the necessary measures, which aim to cover each control system. The paper concludes that the result should be a better understanding of the evolution of threats. The work also summarized conclusions about the future vision of the technological world. The need to stimulate users to analyse the components of information security is emphasized.

The study by Guitton and Fréchette (2023), who conducted a comprehensive analysis of crisis and post-crisis cyber threats, had an impact on the author's position on the issue under research. Attention was paid to the influence of the Russian-Ukrainian conflict on the nature of cyber threats. The study also took into account the findings obtained by Reznikova (2022) regarding the analysis of the security environment of Ukraine before the war in 2022. The importance of identifying the sources of the main threats to the national security of Ukraine for further forecasting the transformations of the sources of the main threats in the post-war period is emphasized. It was also emphasized that this activity is necessary for determining the strategic goals and priorities of the national security policy.

Devanny *et al.* (2022) studied the nature of modern threats and their impact on public administration. It was concluded that there is a need to focus on cyber security and resilience, and especially on effective cyber diplomacy. The study by Li and Liu (2021) on different types of cyberattacks of the new generation is worth noting. The authors present new trends and latest developments in the field of cyber security, as well as analyse security threats and challenges. An increased number of cases of cyberattacks, which may have military or political goals, has been noted.

Farid (2021), Boháček and Farid (2022) considered issues related to state and individual protection measures against deepfakes, ethical use of deepfakes as a weapon. Particular concern about the use of deepfakes against world leaders during armed conflicts has been noted. The importance of using an identity-based approach to protect world leaders from fake imposters was emphasized. It was concluded that this approach captures distinct facial features, gestures and voice.

The study by Dobák (2021), who emphasizes that the national security sector is connected with the world of ICT, was used when shaping the author's position. It is concluded on the developing transformation of intelligence technologies and methods, the emergence of cross-border solutions for data collection. The importance of comprehensive protection of state and national systems, critical infrastructure from cyber-attacks was noted.

An article by Willett (2022) on the cyber dimension of the Russian-Ukrainian war is worth noting. The author emphasized the importance of the reliability of Ukrainian cyber security supported by Western aid. The researcher focuses on the fact that there is uncertainty about the true nature of cyber operations, their responsible use, and the application of international law to them.

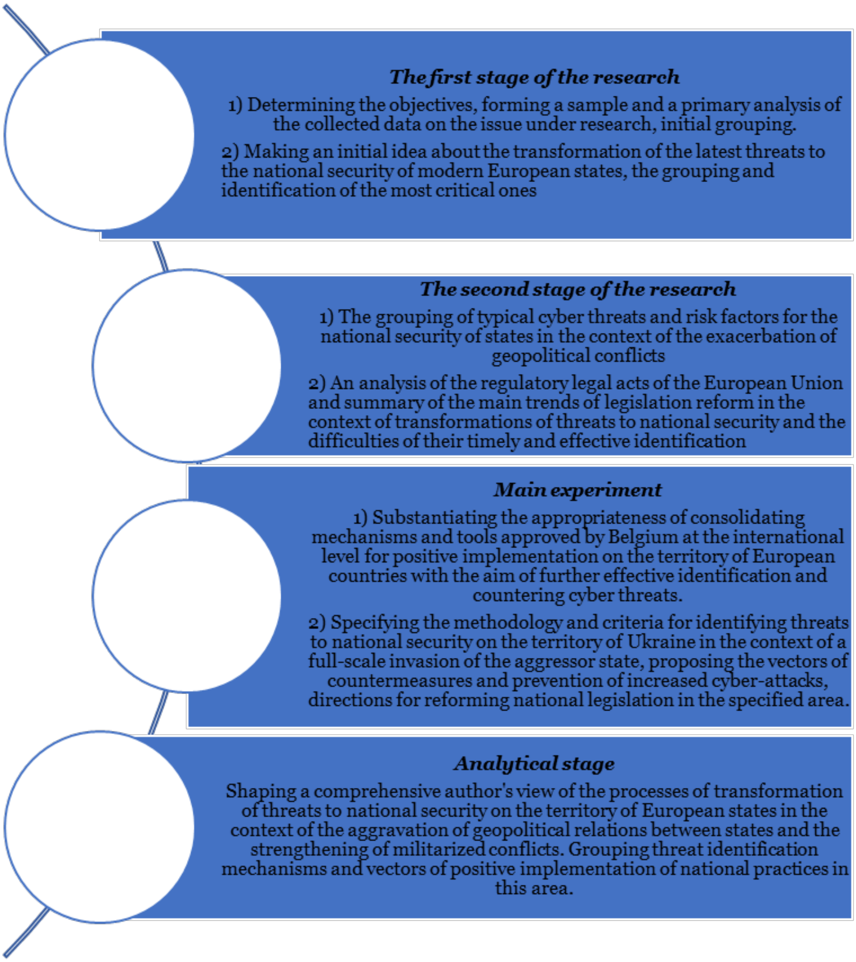
Urych and Matyasik (2022) compare military and defence training, education and socialization in a number of European countries. The need for the development of defence education in each country was noted. The authors analysed possible shortcomings in this area, which are related to the cyber space. The importance of each country's experience aimed at strengthening national security is clarified.

An active study of the issues under research points to the fact that identification of new threats to the national security of the country should be given special attention. The diversity of studies in this field is also noted. Therefore, it is necessary to carry out research according to new research criteria.

2. Methods

The research on the topic of the article involved a set of methodological tools aimed at fulfilling the objectives outlined by the aim of the study. Figure 1 shows the research design, which makes it possible to single out the main elements used to draw the author's conclusions. During the research, the authors studied and shaped their own position regarding regulatory documents and studies on the issue under research. The study comprises information from thirty-seven sources with relevant references in the text.

A synergistic approach was used to identify the high level of self-organization of states on the way to solving the issue of countering innovative threats to national security, as well as to shape the author's vision of strengthening interstate ties against the background of the exacerbation of militarized conflicts on the way to the prevention of the studied threats. This approach made it possible to minimize the multivariability of paths and accidents when identifying new threats, and determine universal packages of actions in the studied area. Some have been fragmentarily implemented into the EU legislation. This approach was also tested while considering the debatable positions of the representatives of legal schools and finding a single vector of agreement for supranational changes in the studied area.



The first stage of the research

1) Determining the objectives, forming a sample and a primary analysis of the collected data on the issue under research, initial grouping.

2) Making an initial idea about the transformation of the latest threats to the national security of modern European states, the grouping and identification of the most critical ones

The second stage of the research

1) The grouping of typical cyber threats and risk factors for the national security of states in the context of the exacerbation of geopolitical conflicts

2) An analysis of the regulatory legal acts of the European Union and summary of the main trends of legislation reform in the context of transformations of threats to national security and the difficulties of their timely and effective identification

Main experiment

1) Substantiating the appropriateness of consolidating mechanisms and tools approved by Belgium at the international level for positive implementation on the territory of European countries with the aim of further effective identification and countering cyber threats.

2) Specifying the methodology and criteria for identifying threats to national security on the territory of Ukraine in the context of a full-scale invasion of the aggressor state, proposing the vectors of countermeasures and prevention of increased cyber-attacks, directions for reforming national legislation in the specified area.

Analytical stage

Shaping a comprehensive author's view of the processes of transformation of threats to national security on the territory of European states in the context of the aggravation of geopolitical relations between states and the strengthening of militarized conflicts. Grouping threat identification mechanisms and vectors of positive implementation of national practices in this area.

Figure 1. Research design on the topic being studied. Own elaboration.

The observation method was applied to identify the criteria for the riskiness of making a unique behavioural profile of each network user in the current realities. This methodological tool also made it possible to monitor the decrease in the level of cyber security in the EU in the context of full-scale military operations in Ukraine.

The method of comparative legal analysis was used to reveal the essence and content of risk assessment and threat monitoring, as well as outline the primary vectors of the planning strategy of preventive security measures of the EU member states. This method helped to determine the positive practice of Belgium in the field of increasing protection against cyber threats at all levels. The results of prevention and effective protection developed and implemented by this state deserve attention and further testing.

The forecasting method helped to specify the vectors of adaptation of the Belgian practice of identifying the latest threats on the territory of European countries, determine the mechanisms of identifying fake information. It was established that the Bug Bounty Programme for detecting vulnerabilities in technologies initiated by Belgium has been implemented in Ukraine despite the challenges of the martial law in the country.

The historical method was applied when tracking the genesis of the emergence and identification of threats to the national security of states in recent years, and proving the accelerated pace of growth in the number and complexity of new threats.

The statistical method identified trends in the transformations of current threats. This methodological tool also made it possible to analyse the National Cyber Security Index. The clustering method was also used in the analysis of the sample in this study. It was used when studying the classifications of cyber threats, cyber incidents and possible response measures.

3. Results

The identification of threats involves the assessment of events, phenomena, processes, and other factors that lead to the danger of realizing vital national interests. Cyber threats have the following basic components: collection, modification, leakage, and destruction. Internal threats spread from employees of organizations, software, and hardware. External sources of threats can be represented by computer viruses and malware.

Incident categories contain malicious (offensive) content and distribute spam. Malicious software code provokes malware infection and distribution. The attacker collects information using scanning, sniffing, and phishing. Incident categories also include attempts to interfere by exploiting a vulnerability and logging into the system.

The availability violation category is characterized by a denial-of-service attack, sabotage, and failure. Violation of information properties is possible with unauthorized access to information and modification. Fraud is carried out through the use of a fraudulent website. Known vulnerability is also a characteristic category.

Digital technologies have changed the dynamics of conflict. Cyber war has evolved from propaganda to espionage, from defacing websites to disrupting power grids and water systems. Threats related to information activities and cyberspace have got a military-political orientation. The information and technical threats, as well as information and psychological influences have become part of military strategies.

Lethal autonomous weapons based on artificial intelligence have become a particular threat. Their use leads to new ethical problems. An example would be the substitution of human ethical judgments during conflicts. Artificial intelligence algorithms that focus on attracting people's attention use human cognitive abilities. A social media post containing an indignant disagreement based on moral emotional words gets a lot more reposts. This can spread both economic and political discontent in countries with the help of artificially created negative events.

Many social consequences of new technologies began to be stated only as they expanded. Quantum computers have significant computing capacity. It became possible to use them for hacking encryption algorithms of Internet websites, for attacks on state systems and institutions.

Social networks are increasingly becoming the target. Methods and tools with different levels of complexity and innovation are used. Solutions based on deep learning techniques use generative adversarial networks (GAN).

Two systems of competing artificial neural networks —a generator and a discriminator — make it possible to create hyperrealistic videos, audio, images or text. Relevant digital content is determined to be unreliable only using sophisticated forensic methods. Once created, the content, known as synthetic media or deepfake, can be used as a threat to national security. Another example of a malicious use of GAN could be targeting servers that distribute patches to disrupt scheduled updates. In general, the list of identifiers of new threats and their manifestations can be replenished daily with the latest developments, but it is proposed to single out the basic ones (Figure 2).

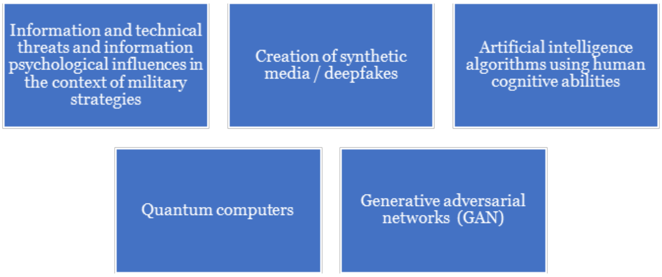

Information and technical threats and information psychological influences in the context of military strategies
Creation of synthetic media / deepfakes
Artificial intelligence algorithms using human cognitive abilities
Quantum computers
Generative adversarial networks (GAN)

Figure 2. The main threats to the country's national cybersecurity. Own elaboration.

The process of identifying deepfake videos can be divided into three types. The first type is based on learning, where features that make it possible to distinguish the reality from a fake are learned explicitly. The second type is based on artifacts in which low- to high-level features are designed to distinguish real from fake.

The third type is identity-based, in which biometric style features are applied to detect whether the person depicted in the video is who he/she says he/she is. The difficulty of implementing these methods is that they require an individual model created from several hours of authentic video record. An integrated model of the face, gestures and voice should be prepared, which captures the distinctive features of the person's speech. Approximately 700-800 behavioural features are needed to achieve the identification accuracy. (Figure 3).

Learning-based videos
Artifact-based videos
Identity-based videos

Figure 3. Deepfake video identification process. Own elaboration.

The attackers' task is to collect data from all aspects of life to create an accurate and unique behavioural profile of each user. By 2030, the volume of behavioural data collection will increase exponentially (ENISA, 2023). Criminal activities can be aimed at gaining access to data arrays to adapt social engineering attacks based on a user's behavioural profile. Adversely impacting users through collected behavioural profiles may pose a threat to national security.

The combination of software, hardware, and component-based code began to create uncontrolled interactions and interfaces, disrupting the respective supply chains. Cyberattacks are becoming more sophisticated, and may be combined with physical or offline attacks. Hybrid operations are characterized by the difficulty of detection and protection due to their complexity and insufficient training of specialists who are trained to consider each attack separately.

A lack of skills and personnel is the cause of most cybersecurity threats, which can negatively impact businesses, governments, and citizens. It is also possible to note the fact of the growth of cybercrime with the use of digital currencies, the use of data from the electronic healthcare database and genetic data.

As of April 2023, there were 5.18 billion Internet users worldwide. A total of 4.8 billion of the population were social media users (Statista, 2023). Global costs from cybercrime could reach $10.5 trillion annually by 2025 compared to $3 trillion in 2015 (CompTIA, 2023).

After the beginning of the aggression of the Russian Federation against Ukraine, cyber-attacks on energy networks, transport infrastructure and space facilities of the EU showed the relevant risks and threats. The EU's cyber defence policy aims to expand the EU's cyber defence capabilities and strengthen coordination and cooperation. Back in 2019, the European Parliament and the Council adopted the Cybersecurity Act (European Parliament and of the Council, 2019).

The main goals of cyber security are information security, access control, vulnerability assessment, monitoring of user activity, cyber resilience. The EU Agency for Cybersecurity Security (ENISA) has been given permanent powers. It takes into account the most relevant and widespread standards in the field of risk management. The international ISO/IEC 27002, the American NIST Cybersecurity Framework are applied. The EU supports the US Information Sharing and Analysis Centres (ISAC) model.

In the EU, it is proposed to impose cybersecurity obligations on all products with digital elements (European Parliament and of the Council, 2022) It is also proposed to increase the level of preparedness, detection and response to threats and attacks in the field of cybersecurity in the EU (European Parliament and of the Council, 2023). As a result, the European Cyber Shield should be created. It is planned to introduce operational security centres in it, which should be interconnected throughout the EU.

A positive example of the implementation of the identification of new cyber threats is the relevant activity in Belgium. According to the National Cyber Security Index (NCSI), Belgium has a score of 94.81, which equates to No. 1 in the ranking (NCSI, 2021a). The Centre for Cyber Security Belgium (CCB) is the national cybersecurity authority (CCB, 2023). Belgium has a federal CCB cyber emergency response team (CERT.be).

The CCB site Safeonweb.be informs and advises Belgian citizens in their daily life on cyber security issues and the main current digital threats. The Cyberfundamentals Framework created by CCB helps Belgian citizens in the workplace. The Cyberfundamentals Framework includes well-known cybersecurity frameworks: NIST CSF, ISO 27001/ISO 27002, CIS Controls, and IEC 62443.

The Cyber fundamentals Framework has prepared four levels, the purpose of which is to respond to the severity of the threat. The Baseline Security Guidelines (BSG), the Executive Summary (FR) for the public sector contain different levels of guidance. Federal Public Services (FPS) Policy and Support offers cybersecurity training for federal government employees.

In Belgium, the identification of operators of essential services operating in critical infrastructure is legislated (Chancellerie du Premier Ministre, 2019). An Early Warning System (EWS) has been established for CCB's critical infrastructure. Authorized businesses have access to filtered cyber threat alerts through a common platform.

Belgian organizations widely use a coordinated vulnerability disclosure policy (CVDP), as well as the Bug Bounty Programme for identifying vulnerabilities in technologies. CCB conducts various classes, courses, training and academic research on cyber security in Belgium.

Despite the martial law introduced in Ukraine, the state continues to implement the necessary legislative initiatives. The National Security Strategy of Ukraine (Decree of the President of Ukraine No. 392/2020, 2020) is based on the principle of deterrence through the improvement of defence and security capabilities, stability and interaction with key foreign partners.

The Law of Ukraine No. 2163-VIII "On the Basic Principles of Ensuring Cyber Security of Ukraine" dated October 5, 2017 defines the legal and organizational foundations of ensuring the protection of the vital interests of citizens, society, the state, and national interests of Ukraine from cyber threats.

According to the National Standard of Ukraine ISO/IEC 27032:2016, cyber threats affect digital assets. In Ukraine, a list of categories of cyber incidents has been developed, and the TLP Protocol, which contains general rules for exchanging information about cyber incidents, has been in effect since February 2023.

According to the National Cyber Security Index (NCSI), Ukraine has a score of 75.32, which equals 24th place in the ranking (NCSI, 2021b). Table 1 provides a detailed information on Ukraine's cyber security indicators (NCSI, 2021b).

Table 1. Indicadores de seguridad cibernética de Ucrania según el ranking del Índice Nacional de Seguridad Cibernética (NCSI).

General cyber security indicators	Basic cyber security indicators	Indicators of incident and crisis management
Cyber security policy development - 100% Analysis and information about cyber threats - 80% Education and professional development - 89% Contribution to global cyber security – 33%	Protection of digital services - 20% Protection of basic services - 100% Electronic identification and trust services - 100% Personal data protection - 100%	Responding to cyber incidents - 67% Cyber crisis management - 60% Combating cybercrime – 100% Military cyber operations – 17%

The given data indicate that Ukraine currently needs to improve the protection of digital servers, response to cyber incidents, and cyber security management. Special attention needs to be paid to improving the level of incident management related to military cyber operations. A total of 1,374 cyber incidents in 2021, and 2,194 cyber incidents and cyber-attacks in 2022 were processed manually (CERT-UA, 2023). A more destructive nature of the attacks was recorded. New cyber threats were noticed during the military aggression of the Russian Federation.

This is the first military cyber conflict in which the respective capabilities of the two countries are almost identical. Most of this conflict in the field of cyber technologies consists of information operations, which are based on cognitive components. Hacking and disruptions of critical national infrastructure of Ukraine became a characteristic feature.

New cyberattacks are being carried out with the aim of revenge or attempts at informational and psychological influence to convince the population that the state is not capable of protecting them. Critical “silent” attacks are also committed. They are aimed at military espionage, the main targets of which are high-ranking officials, diplomats and other professionals who have access to the most sensitive information.

The most popular methods of penetration are phishing, using known vulnerabilities. The cyber techniques are shifted from destructive attacks to attacks aimed at obtaining information, and the interest is shifted to new industries.

Table 2 contains groups of the most frequent combined cyberattacks of the Russian Federation during hostilities in Ukraine (CERT-UA, 2023):

Table 2. The vectors of cyber-attacks committed by the Russian Federation during a full-scale invasion of Ukraine

Operations of information influence	Cyber espionage	Technical vulnerabilities
- mass media; - civil infrastructure websites (state institutions and critical infrastructure facilities (especially the energy sector); - websites of defence organizations.	- "silent" operations; - phishing.	- destruction of data, infrastructure.

Source: according to CERT-UA data (2023).

The scope of cyber fraud using social engineering techniques significantly expanded in Ukraine during the wartime, when the citizens needed social assistance. The population's demand for military- and electricity-related goods has grown. Cash payments from the state and international organizations have become the subject of close attention of fraudsters. "Cyber looters" started issuing loans for missing servicemen and citizens who went abroad (EMA, 2023).

The draft Ukraine Recovery Plan has been developed. Much attention is paid to increasing the cyber resilience of the state and the effective response to cyber security incidents.

4. Discussion

It can be stated that digitization, generation of more data and expansion of connectivity leads to the emergence of new threats to national security. Globalization and the development of ICT have affected national security as threats have become much more abstract and complex (Abd Al Ghaffar, 2020). A new approach to predicting and identifying cyber-attacks at an early stage is needed, which is based on a preventive approach to identifying security threats, especially in the field of critical infrastructure (Alqudhaibi *et al.*, 2023).

The researchers propose to ensure the accuracy of forecasts through the minimization of false-positive alarms. The identification mechanism can be based on the specifics of the attacker's motivation and the nature of the critical infrastructure.

Tested on several hours of authentic video, the identification-based deepfake detection approach was found to capture distinct gestures, facial and voice features. In this way, the use of deepfakes against world leaders during elections or during armed conflicts is minimized (Boháček and Farid, 2022).

The responsibility for the danger of programmes that can later simulate deepfakes should rest with the inventors of the software. It should occur before the release of the technology into open access, as the corresponding software can be used as a cyber threat (Farid, 2021).

It can be stated that the identification of a cyber threat is an effort that requires serious analysis. Reports from people using radio intelligence tools can help gather evidence to support attribution analysis (Devanny *et al.*, 2022). According to the researchers, an understanding of the technical operational methods of the alleged criminal will be ensured.

It can be concluded that the scale, variety and complexity of cyber threats are growing significantly. The existing security strategies, which are mandatory to combat cybercrime, will not be able to meet the future requirements that will arise in the post-war crisis era (Guitton and Fréchette, 2023). The researchers state that network dynamics with the help of artificial intelligence for specific tasks should be implanted in the process of exchanging accumulated experience between experts.

It was established that the positive example of Belgium indicates the need to implement constant tracking and use of advanced technologies in the field of cyberspace. Socialization, education and training of young people to ensure national security is becoming extremely important (Urych and Matyasik, 2022). Countries need to increase their spending on developing infrastructure such as firewalls and developing cybersecurity talent (Hung, 2022). A serious task in this field is the employment of the younger generation, which better perceives the digital world (Dobák, 2021).

It can be concluded that the components of cyber-attacks against Ukraine are new hybrid threats with characteristic criteria. Ukraine has shown sufficient capacity to recover from detected cyber intrusions and develop cyber resilience (Willett, 2022). In Ukraine, it is necessary to develop a programme of state strategic forecasting and planning (Bondarenko *et al.*, 2022). According to researchers, it should be related to the entire structure of state activity, be based on models of the future security environment, and correspond to the national interests of the state.

It can be stated that the identification of informational fakes and deepfakes is one of the main tasks of the state in ensuring the information and cyber security of the Ministry of Defence of Ukraine and the Armed Forces of Ukraine. This will contribute to counteracting adverse informational and psychological influences on the personnel of the Armed Forces (Semenenko and Frolov, 2023).

Conclusions

New information technical threats and information psychological influences are becoming components of military strategies. An autonomous weapon with artificial intelligence appeared to simulate and create negative events. Deepfakes become a tool used to deceive in order to influence the decision-making processes of community members. The increasing malicious use of quantum computers is recorded. The criminal use of users' smart devices to create a unique behavioural profile has emerged. Cyber threats have become hybrid. New threats require an urgent evaluation of events, phenomena, and processes.

The EU's cyber defence policy has set the expansion of cyber defence capabilities, strengthening of coordination, cooperation as its goal through the proposed laws regarding cyber solidarity and cyber resilience. A characteristic feature of the future European Cyber Shield will be a comprehensive mechanism for responding to relevant emergency situations.

The activities of the established Centre for Cyber Security Belgium (CCB) are a positive example of the implementation of the identification of new cyber threats. CCB centrally carries out activities related to the identification, monitoring, and analysis of online security problems.

States need to step up efforts to improve targeted interventions in national education to ensure future skilled cybersecurity professionals. It is also necessary to pay attention to the issue of involving the capabilities of national intelligence special services for the processes of identifying cyber threats to national security.

New cyber threats to national security in Ukraine are characterized by attempts to disrupt critical national infrastructure. New cyberattacks are being carried out with the aim of revenge, attempts at informational and psychological influence, military espionage. Phishing attacks and the use of known vulnerabilities are being improved. "Cyber looting" with the use of social engineering techniques has emerged.

Ukraine still needs to strengthen the levels of protection of digital servers, response to cyber incidents, and cyber security management. The positive example of Belgium indicates the need for continuous monitoring and application of advanced technologies in the relevant field. It can be implemented in the relevant activity in Ukraine.

Bibliographic References

ABD AL GHAFFAR, Hedaia-t-Allah Nabil. 2020. "Government Cloud Computing and National Security" In: Review of Economics and Political Science. https://doi.org/10.1108/REPS-09-2019-0125. Consultation date: 08/04/2022.

ALQUDHAIBI, Adel; ALBARRAK, Majed; ALOSEEL, Abdulmohsan; JAGTAP, Sandeep; SALONITIS, Konstantinos. 2023. "Predicting Cybersecurity Threats in Critical Infrastructure for Industry 4.0: A Proactive Approach Based on Attacker Motivations" In: Sensors. Vol. 23, No. 9, pp. 4539.

BOHÁČEK, Matyáš; FARID, Hany. 2022. "Protecting world leaders against deep fakes using facial, gestural, and vocal mannerisms" In: Proceedings of the National Academy of Sciences of the United States of America. Vol. 119, No, 48, pp. e2216035119.

BONDARENKO, Svitlana; BRATKO, Artem; ANTONOV, Volodymyr; KOLISNICHENKO, Roman; HUBANOV, Oleh; MYSYK, Anatoliy. 2022. "Improving the State system of strategic planning of national security in the context of informatization of society" In: Journal of Information Technology Management. Vol. 14, Special Iss.: Digitalization of Socio-Economic Processes, pp. 01-24.

CCB. 2023. The Centre for Cybersecurity Belgium. Organisation. Available online. In: https://ccb.belgium.be/en/organisation. Consultation date: 03/02/2023.

CERT-UA. 2023. Russia's Cyber Tactics: Lessons Learned in 2022 — SSSCIP analytical report on the year of russia's full-scale cyberwar against Ukraine. Available online. In: https://cip.gov.ua/en/news/russia-s-cyber-tactics-lessons-learned-in-2022-ssscip-analytical-report-on-the-year-of-russia-s-full-scale-cyberwar-against-ukraine. Consultation date: 03/03/2023.

CHANCELLERIE DU PREMIER MINISTRE. 2019. Loi établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique. Dossier No. 2019-04-07/15. Available online. In: http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2019040715&table_name=loi. Consultation date: 08/04/2023.

COMPTIA. 2023. Top 50 Cybersecurity Statistics, Figures and Facts. Available online. In: https://connect.comptia.org/blog/cyber-security-stats-facts. Consultation date: 03/03/2023.

CRISTEA, Cristea Lavinia. 2020. "Current security threats in the national and international context" In: Accounting and Management Information Systems. Vol. 19, No. 01, pp. 351-378.

DECREE OF THE PRESIDENT OF UKRAINE No. 392/2020. 2020. "On the decision of the National Security and Defense Council of Ukraine 2020 "On the National Security Strategy of Ukraine"" Available online. In:

https://zakon.rada.gov.ua/laws/show/392/2020#n5. Consultation date: 08/03/2023.

DEVANNY, Joe; GOLDONI, Luiz Rogerio Franco; MEDEIROS, Breno Pauli. 2022. "Strategy in an Uncertain Domain: Threat and Response in Cyberspace" In: Journal of Strategic Security. Vol. 15, No. 02, pp. 34-47.

DOBÁK, Imre. 2021. "Thoughts on the evolution of national security in cyberspace" In: Security and Defence Quarterly. Vol. 33, No. 01, pp. 75-85.

EMA. 2023. Payment Fraud Matrix. Reboot: Analysis, Trends and Forecasts, 2022/2023. Available online. In: https://www.ema.com.ua/news/matricja-platizhnogo-shahrajstva-perezavantazhennja-analiz-trendi-ta-prognozi-2022-2023/. Consultation date: 03/06/2023.

ENISA. 2023. Identifying emerging cyber security threats and challenges for 2030. Available online. In: https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030. Consultation date: 08/03/2023.

EUROPEAN PARLIAMENT AND OF THE COUNCIL. 2019. Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Available online. In: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG&toc=OJ:L:2019:151:TOC. Consultation date: 08/03/2023.

EUROPEAN PARLIAMENT AND OF THE COUNCIL. 2022. "Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020." COM/2022/454 final. Available online. In: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0454. Consultation date: 08/03/2023.

EUROPEAN PARLIAMENT AND OF THE COUNCIL. 2023. Proposal for a Regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents. COM (2023) 209 final. Available online. In: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52023PC0209. Consultation date: 03/06/2023.

FARID, Hany. 2021. "The Weaponization of Deep Fakes: Threats and Responses" In: The Journal of Intelligence, Conflict, and Warfare. Vol. 04, No. 02, pp. 87–94.

GUITTON, Matthieu; FRÉCHETTE, Julien. 2023. "Facing cyberthreats in a crisis and post-crisis era: Rethinking security services response strategy" In: Computers in Human Behavior Reports. Vol. 10, pp. 100-282.

HUNG, Ho Ting (Bosco). 2022. "A Critical Moment of Taiwan's Security - Taiwan Has to Sharpen Its Cybercapacity in Response to China's National Rejuvenation" In: ITSS Verona Magazine. Vol. 1, No. 2, pp. 01-13.

LI, Yuchong; LIU, Qinghui. 2021. "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments" In: Energy Reports. Vol. 7, pp. 8176–8186.

NCSI. 2021b. 24. Ukraine 75.32. Available online. In: https://ncsi.ega.ee/country/ua/. Consultation date: 08/02/2023.

NCSI. 2021a. 1. Belgium. 94.81. Available online. In: https://ncsi.ega.ee/country/be/585/#details. Consultation date: 08/02/2023.

REZNIKOVA, Olga. 2022. "Strategic Analysis of Ukraine's Security Environment." In: Strategic Panorama. Available online. In: https://doi.org/10.53679/2616-9460.specialissue.2022.05. Consultation date: 14/01/2023.

SEMENENKO, Viacheslav; FROLOV, Valery. 2023. "Military Aspects of Countering Hybrid Aggression: Ukrainian Experiences" In: National Security and the Future. Vol. 01, No. 24, pp. 55-65.

SŁUGOCKI, Wojciech Łukasz; SOWA, Bogdan. 2021. "Disinformation as a threat to national security on the example of the COVID-19 pandemic" In: Security and Defence Quarterly. Vol. 35, No. 03, pp. 63-74.

STATISTA. 2023. Number of internet and social media users worldwide as of April 2023 (in billions). Available online. In: https://www.statista.com/statistics/617136/digital-population-worldwide/. Consultation date: 08/02/2023.

ŞTEFĂNESCU, Daniel-Cornel; PAPOI, Alina. 2020. "New threats to the national security of states – cyber threat" In: Scientific Journal of Silesian University of Technology. Series Transport. Vol. 107, pp. 1773182.

URYCH, Ilona; MATYASIK, Grzegorz. 2022. "Preparing youth for defence: Socialisation, education, and training of young people in Europe for national security" In: Security and Defence Quarterly. Vol. 38, No. 02, pp. 01-15.

WILLETT, Marcus. 2022. "The Cyber Dimension of the Russia–Ukraine War" In: Survival. Vol. 64, No. 05, pp. 07-26.

UNIVERSIDAD
DEL ZULIA

CUESTIONES
POLÍTICAS

Vol.41 Nº 78

*Esta revista fue editada en formato digital y publicada
en julio de 2023, por el **Fondo Editorial Serbiluz,
Universidad del Zulia. Maracaibo-Venezuela***

**www.luz.edu.ve
www.serbi.luz.edu.ve
www.produccioncientificaluz.org**