https://doi.org/10.33271/nvngu/2023-5/165

I. Leroy[1,2],
orcid.org/0000-0003-3299-9149,
I. Zolotaryova[*3],
orcid.org/0000-0002-1553-2849

1 – Université de Lorraine, Nancy, the French Republic
2 – European Security and Defence College, Brussels, the Kingdom of Belgium
3 – Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine
* Corresponding author e-mail: iryna.zolotaryova@hneu.net

CRITICAL INFRASTRUCTURE DEFENSE: PERSPECTIVES FROM THE EU AND USA CYBER EXPERTS

Purpose. To examine the components of cyber autonomy according to the insights of seasoned professionals from the European Union (EU) and the United States of America (USA). The value of each element will be calculated by obtaining data from structured in-depth interviews.

Methodology. Through an investigation of different aspects of the research, we used the Delphi technique and research interviews include the option of the Interviewee Transcript Review (ITR). The Delphi method is processed in several rounds, usually three, with two rounds being considered as a minimum and in that respect the Delphi method helps our study explore, predict and identify the nature and fundamental elements of Cyber Autonomy.

Findings. The study findings demonstrate that elements such as "Policies", "Reputation management", and "Infrastructure and Architecture" hold substantial importance within Cyber Autonomy. These elements are considered critical for future perspectives. The research highlights the role of Cyber Autonomy in streamlining cybersecurity approaches, mitigating the impact of cyber-attacks, and safeguarding possible reputation damage. The study also highlights the importance of well-defined implementation methods and the organizational structure in successfully deploying Cyber Autonomy.

Originality. The research demonstrates the interdisciplinary nature of cybersecurity and applies a comprehensive approach covering information security, information security policy, technical and economic aspects, noting the important role of governance in the company share value recovery process. Cyber Autonomy could offer a concept of defense reputation that helps to identify potential cyber threats that are further intensified in connection with the development of various platforms for remote control of artificial intelligence, distance learning, and opportunities for autonomous operation of enterprise systems, the influence of multinational companies on financial markets, and automated decision-making systems.

Practical value. Experts' insights are analyzed that can help to provide practical solutions for the Cyber Autonomy and risk management methods for implementing cyber resilience strategy for critical infrastructure. The research provides adjustments to existing cybersecurity frameworks and directives which consider new cyber elements of information security realities. The current study can be used as a guide to confidence-building measures for possible reputation and financial loss, reinforces protection actions against disinformation or negative cyber impact.

Keywords: *cyber autonomy, critical infrastructure, cyber-attack, risk mitigation*

Introduction. Issues such as autonomous decision-making in cybersecurity protocols, the ethical considerations of autonomous cyber defense mechanisms, and the potential risks and benefits of cyber autonomy have been widely debated within the EU. This is because cyberattacks are often cross-border in nature and may have a physical impact on critical infrastructure in the EU. Significant cybersecurity incidents can be too disruptive for a single or several affected Member States to handle alone. They can also form part of larger hybrid attacks carried out by third countries with the aim to destabilize the economy [1]. Economic defense – like never before – means national security. For that reason, Cyber Security initiatives associated with digital transformations include a "testing mode" period, along with Cyber Autonomy functions that aim to support business critical infrastructures [2]. For that reason, the EU is putting in place a number of initiatives that ensure that all companies which are providers of essential services are well protected against cyber threats. Policy and legal obligations to immediately disclose attacks compel organizations to go public very quickly, hindering response efforts and risking significant reputational damage [3].

Cyber-attacks become increasingly difficult to bounce back from as customers become impatient with organizations that suffer either disruption or loss – especially when their rights and freedoms are directly impinged. Ignoring the specific multi-level relationships among information security, state policies, reputation management, technical aspects, and the economy can lead to systemic risks [4].

In critical infrastructure nowadays, it is common to use surveillance technologies for improvement in protection and prevention against attacks on critical infrastructure, but there is a lack of standardization, testing and accreditation in Europe that would greatly help users to ensure that products are fit for purpose [5]. Therefore, in the event of significant cyber breaches, such as those affecting critical infrastructure, it is imperative for companies to fulfil their obligation to inform the government about the incident. Subsequently, the investigation and mitigation efforts will involve close cooperation with various entities, including the Computer Security Incident Response Teams (CSIRT), the European Cybercrime Centre (EC3), The European Union Agency for Cybersecurity (ENISA), or the EU's Computer Emergency Response Team (CERT-EU). This collaborative approach is essential to ensure effective handling of cyber incidents and to leverage the expertise and resources of relevant organizations for swift and efficient resolution [6]. This multi-level relationships in different levels of information security give rise to the logical research question: what is the importance (weight) of each element within Cyber Autonomy? The other supportive question is: what are the implementation phases and their respective importance (weights)? To address this issue, we have utilized various research methods, including qualitative, quantitative, and structured in-depth interviews with experts from the EU and USA. These methods encompass a range of techniques, strategies, and tools that have been employed to conduct experiments and propose solutions to the research problem.

Literature review. Heightened apprehensions regarding cyber threats have catalyzed an outpouring of security-related publications that offer comprehensive guidance and establish benchmarks for the adept management of cyber risks. This proliferation of literature, however, is predominantly centered on addressing risks associated with safeguarding information,

often encapsulated within the overarching framework of information security, or alternatively, information assurance.

It is paramount to underscore the nuanced distinction between these two processes. Information assurance embodies the strategic evaluation and meticulous management of risks pertaining to information assets on a higher echelon, encompassing a comprehensive perspective. Conversely, information security operates as a subset within the realm of information assurance, characterized by a pronounced emphasis on technical measures and countermeasures.

Yet, the parlance of the field frequently converges these terminologies, resulting in a colloquial amalgamation. In pragmatic application, the term "information security" often assumes a dual role, encompassing both the strategic orchestration of information assurance and the more technically oriented facets of safeguarding data assets.

The prevalence of this dual connotation yields a potentially intricate landscape, where the boundaries between information assurance and information security often meld. While distinct in their conceptual underpinnings, these processes often exhibit a symbiotic relationship in practice, intertwining their endeavors to fortify the cyber resilience of organizations.

In this backdrop, it becomes imperative to navigate this terminological duality with a comprehensive understanding. The strategic and technical dimensions coalesce to form a holistic approach to cyber risk management, encompassing both the safeguarding of information assets and the broader strategic calculus of information assurance. As the digital landscape continues to evolve, a nuanced comprehension of these intertwined processes remains pivotal for effectively mitigating the multifaceted challenges posed by contemporary cyber threats [4]. Ultimately, entities are required to develop a risk appetite and strategy going forward to manage their non-affirmative risk. The analysis performed should support this development by creating greater clarity to management so that they may make educated decisions reflecting the analysis performed [5].

Infrastructure comes to play a significant role in the context of Cyber Autonomy and could potentially increase the degree of information and data protection as well as fill in the current gaps of the cyber and information security industry as well as support Cyber Autonomy, which also includes reputation defense. All this will potentially strengthen the phase of the process, which is important for the formation of customer loyalty, affects the likelihood of purchasing goods and makes the purchase comfortable for the customer.

Mapping critical infrastructure and assessing cyber security risks along with a risk decision to mitigate should have a "steps-based" model that companies can use. These elements can have a complex structural environment, requiring a systematic approach to ensure effective cyber defense measures. Recently, academics, industrialists, and researchers have been actively exploring various aspects of autonomy, including its application in the field of cyber security.

The "Strategic Review of Defence and National Security" takes up a concept of National Strategic Autonomy which insists on the technical and human capacities of such autonomy [6]. Important strategic areas of industry and research consolidated resilience, exposed to the development of cyber threats and the associated risks, while some of them remain insufficiently protected and sensitive [7].

The European Union is pursuing technological autonomy from a position of relative weakness given the scarcity of European Big Tech companies, while American and Chinese giants occupy critical network nodes. Companies are able to leverage these nodes politically through "weaponized interdependence". These efforts have aimed to guide the development of effective directions for addressing the challenges of Cyber Autonomy, with a particular focus on cyber security and reputation considerations [8].

This dependence poses a substantial risk, as a failure in one critical infrastructure system can lead to cascading issues affecting other interconnected systems, potentially causing severe damage.

The concept of cyber autonomy has gained significant attention and is seen as a promising approach to enhancing the resilience and security of critical infrastructure. Since 2017, EU member states have been utilizing a cyber security toolbox as part of their efforts to provide a coordinated response to serious cyber operations within the framework of the EU's Common Foreign and Security Policy (CFSP). This toolbox serves as a comprehensive resource for implementing cyber security measures and promoting cyber autonomy principles at a national level. However, the implementation of a proportionate, coherent and, above all, legally secure response by the EU to such cyber-attacks is extremely challenging. Lessons learned from the major cyber-attacks that impacted critical infrastructure businesses come to the following conclusions: information about indicators of compromise (i.e., characteristics and data that indicate that a system or network has been compromised) must be passed through the Joint Cyber Unit in the EU and the EU INTCEN at the European External Action Service (EEAS). The collaborative efforts between these information security actors and organizations play a crucial role in fostering a secure digital environment for businesses and the economy across Europe.

This data is made available to all stakeholders so that everyone can participate in the solutions offered [9]. The term *critical infrastructure* means systems and assets, whether physical or virtual. Critical infrastructures are complex, which means they depend on each other and at the same time are continuously changing and adapting to many changes in the economy, legislation, technology, etc. Their interdependence represents a great danger because a failure of one critical infrastructure system may cascade to another and cause even greater damage [9]. Cyber Autonomy could be also linked to the importance of preventing critical infrastructure from cyber-attacks and the reputation damage associated with it. As indicated by the "Finnish Institute of International Affairs" response, the EU has come to view external influence and dependencies as a national security threat and seeks to reclaim control over key critical technologies and infrastructures. Current digital challenges emphasize the increased dependency on IT technologies, and the rapidly changing nature of the technology [10].

Given the financial, legal, and reputational harm, no organization benefits from a cyber-attack [11]. The potential for damage to company reputation and credibility raises the concern about reputation defense and need to establish the right strategies and rules for protecting it. According to various reports and studies, the cost of cyber-attacks for businesses in the EU can be significant. For example, the European Union Agency for Cybersecurity (ENISA) estimated that the average financial impact of a cyber-attack on a medium-sized enterprise in the EU could range from €30,000 to €50,000, and for a large enterprise, it could reach millions of euros [12]. That is why it is so important for Cyber Autonomy to propose to form opportunities and the rights to determine, prevent, defend and develop sovereignty, as well as to create the resilience of infrastructure. Another study by the Ponemon Institute found that the average cost of a data breach for companies in the EU was €3.59 million in 2020 [13].

The role of technology has recently undergone a shift, resulting in significant disadvantages for those who are unable to keep up. Technology no longer merely supplements our real-life interactions; instead, our real-life experiences now depend on and supplement our technological interactions across all areas of activities [14]. Consequently, companies can enhance their organizational resistance without necessarily changing the existing structure or management "traditions" by adopting Cyber Autonomy. By embracing Cyber Autonomy, companies can utilize a new set of effective guidelines to enhance their cyber resilience.

The purpose of the paper is to investigate the significance of each element within Cyber Autonomy and examine the respective importance or weights associated with them. Furthermore, the study aims to analyze the implementation phases of Cyber Autonomy. The perspectives and insights of cyber experts from the European Union (EU) and the United States of America (USA) will be utilized to gather valuable data, employing structured in-depth interviews. By doing so, the article seeks to contribute to a better understanding of Cyber Autonomy and its role in enhancing defense against cyber-attacks on critical infrastructure.

Methods. The existing concepts are analyzed and the analysis also considers the definitions of the existing concepts suggested by scientists and official institutions working in related domains, including EU and international standards and regulations such as ISO/IEC 27001, which specifies the requirements for an information security management system (ISMS), ISO/IEC 27001: Information security management standard, NIS Directives, and ISO/IEC 27002:2022 Information security, cybersecurity, and privacy protection – Information security controls for critical infrastructure. The methodology is a systematic and theoretical approach to collect and evaluate data for our research. For the search of experts' opinions for an investigation of different aspects of the research we used the Delphi technique, a widely-used qualitative method which includes unstructured open-ended interviews, direct observation, participant observation, and document analyses. The technique is commonly used in risk management for risk probability and impact assessment [15]. It is believed that the Delphi method is useful especially when dealing with complex problems. This research interview includes the option of the Interviewee Transcript Review (ITR). Interviews were taken from March 2020 till July 2022 to assess the logical nature of the responses received. All the experts are using project management tools in their daily life and have deep knowledge in the IT domain. Considering that our area of research is in fact quite narrow, we have chosen a total of 8 experts who reflected to our requirements.

The advantages of the ITR are that it gives interviewees the opportunity to edit or clarify information provided in the original interview, with many interviewees providing corrections, clarifications, and in some cases, adding new material to their transcripts. There are also potential disadvantages, such as a bias created by inconsistent data sources or the loss of data when an interviewee chooses to remove valuable material [16]. Discretion is provided with verbatim transcripts of interviews for the purposes of verifying accuracy, correcting errors or inaccuracies and providing clarifications.

The next method that was applied during the research is the Delphi method [17]. The Delphi method is processed in several rounds, usually three, with two rounds being considered as a minimum and for that reason the Delphi method helps our study to explore, predict and identify the nature and fundamental elements of Cyber Autonomy for future use by companies or any other organizations [18]. Thus, in the next part, both stages will be described in terms of methodology as well as the method used for compilation of the final proposal of indicators. The method was applied based on the requirements of the method, which imply correspondence, structure, regular feedback, multilevel, anonymity. Therefore, unlike survey research methods, the validity of the Delphi method does not depend on the number of participants in the research but the scientific validity of the experts participating in the study [19]. The number of participants in the Delphi study varies from 5 to 20 individuals. In our work Delphi research method and procedure are divided into a few stages, namely:

1. The analysis of the experts' Curriculum Vitae (CVs) from the European Union (EU) and the United States of America (USA), as well as their relevant work experience, was conducted to inform the research design strategy. There were selected experts with experience in the field of information and cyber security with over 15 years of international experience working or owning companies or serving clients in critical infrastructure and having an economic and technical background. All experts are using project management tools in their daily life and have deep knowledge in the IT domain. Considering that our area of research is in fact quite narrow, we have chosen a total of 8 experts who reflected our requirements. That is why we can consider that overall, the sample was sufficient.

2. This study has a three-stage design (Figure).

3. The first stage: we selected a group of experts and conducted interviews separately, each with an expert to identify the main concerns and problems in the cyber security domains, give the feedback about elements weight and phases, seeking expert opinions.

4. The second stage: experts were asked to indicate the importance (weight) of Cyber Autonomy elements assigned 1 to 5 points to each, where 5 is the highest degree of importance.

5. The third: experts were asked to indicate the importance (weight) of the Cyber Autonomy concept and assigned 1 to 5 points to each where 5 is the highest degree of importance.

Calculation method: Calculations of mean, variance, and standard deviation. Calculation of the mean and random error based on Student's test – "hypothesis test statistic" when

$$n1 = \frac{29}{7} = 4.14;$$

$$X = \frac{\sum_{i=0}^{n} Xi}{n}.$$

Depression

$$Dx = \frac{\sum_{i=0}^{n} Xi}{n} - \underline{x}^2; \quad Dx = \frac{123.94}{7} - 17.71 = 17.14 = 0.57.$$

The root-mean-square deviation

$$\sigma = \sqrt{Dx}; \quad \sigma x = 0.76.$$

Results. In general, three experts had more than 15 years of experience in the field of cybersecurity, including over 15 years of international experience working in or owning companies both in European Union (EU) and the United States of America (USA). Additionally, three experts had 15 years of experience of managing their own companies. This confirms that the respondents can be considered subject matter experts in the field.

The second column of Table 1 contains the total weight (ranging from 1 to 5 points) of each element in the model. Importantly, few of them have a high ranking, that is over 4.8

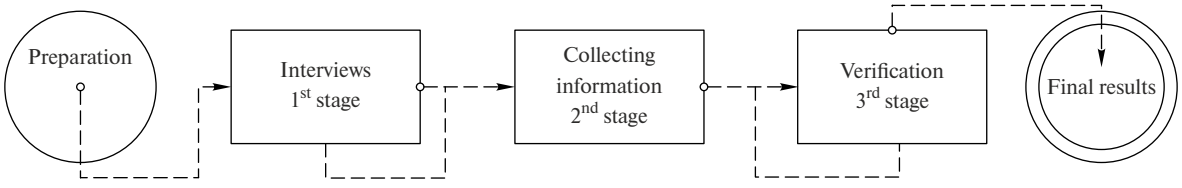

Fig. Schematic example of Delphi method

Table 1

Cyber Autonomy model elements

Cyber Autonomy model elements	Total Weight (from 1 to 5 points)	Number of experts evaluated
Policies	4.8	8
Implementation	4	8
Reputation management (RM)	4.8	8
Resources	3.1	8
Infrastructure and Architecture	5	8
Management and governance	3.1	8
Methods	42	8

which is: "Policies", "Reputation management" and "Infrastructure and Architecture". It is noticeable, that experts perceive challenges of new architecture, changes in the policies areas and reputation management to be more important for the future perspective.

The final results shows that cyber-Autonomy harmonizes elements approaches for cyber security and can removes obstacles, and improves the establishment and functioning of internal response teams to mitigate the negative cyber attach impact and possible reputation loss. This is achieved through consistent rules applicable in the areas of information security, risk and project management, IT, and the policy implementations. Moreover, Cyber Autonomy recognizes the significance of multi-level relationships among information security, state policies, technical aspects, the economy, and the crucial role of Infrastructure and Architecture and Reputation management (RM) in the process of recovering the company's share value. Importantly, "Management and Governance" with a rating of 3.1 does not appear to be as critical as "Policies", despite being considered mandatory for implementation within a company's security measures according to the EU and US information security standards.

The table results highlight Cyber Autonomy phases as a need to explore technologies and development-related steps that will support Cyber Autonomy in general. Despite the apparent significance of human and technological resources, experts did not assign substantial weight to this parameter. As a result, "Resources" emerged as one of the least important factors in the third stage of the study. This may be attributed to the progressive reorganization of work processes and the increasing integration of artificial intelligence technologies into business operations. The study results, as presented in Table 2, demonstrate the stages of Cyber Autonomy and emphasize the significance of the "Organization" business model, which experts assigned a weight of 5. Additionally, the "Implementation Methods" of Cyber Autonomy also play a crucial role in the overall framework.

Table 2

Cyber Autonomy phases

Cyber Autonomy phases	Weight (from 1 to 5 points)	Number of experts evaluated
Goal of Cyber Autonomy	4.8	8
Strategy of Cyber Autonomy	4	8
Implementation Methods	4.8	8
Technology	3.1	8
Organization	5	8
Reputation defense	4.1	8
Result of Cyber Autonomy	3.1	8

Results from all stages of the research underscore the importance of such an element as "Methods" and phase "Implementation Methods" within the context of Cyber Autonomy, as indicated by the high scores given by the EU and USA experts. This finding aligns with the presence of cyber response teams operating at national, organizational, and business levels, who play a pivotal role in implementing effective information security strategies.

So, the samples are the same $t = 0 < t_{kp}$ Student's t-test.

$$\bar{y} = 4.14; \quad Dy = 0.57; \quad \sigma = 0.76.$$

This result suggests that the organizational structure and business model have a substantial impact on the successful implementation of Cyber Autonomy elements. Furthermore, the study underscores the significance of well-defined implementation methods to ensure the successful deployment and integration of Cyber Autonomy practices within an organization.

Conclusions. By conducting structured in-depth interviews, the study was able to delve into and analyze the various factors that contribute to Cyber Autonomy. Through this rigorous methodology, the researchers were able to identify and quantify the significance of these elements, providing a comprehensive understanding of this emerging field.

The findings of the study have significant implications for policymakers and stakeholders in the cybersecurity domain. By shedding light on the critical aspects of cyber autonomy, policymakers can make informed decisions and develop effective strategies to address the challenges and opportunities presented by this evolving field. Additionally, stakeholders can gain valuable insights from this research, enabling them to better navigate the complex landscape of cyber autonomy.

Furthermore, the study's empirical findings provide concrete evidence and data-driven insights into the underlying components of cyber autonomy. This empirical basis strengthens its credibility and makes it an invaluable resource for discussions within the cybersecurity community. Policymakers and stakeholders can rely on this research as a foundation for their decision-making processes, ensuring that their actions are grounded in evidence-based knowledge.

In conclusion, through its use of structured in-depth interviews, this study has successfully examined and quantified the diverse elements contributing to cyber autonomy. Its findings offer crucial insights into this emerging field and serve as a valuable resource for policymakers and stakeholders in the cybersecurity domain. The rigorous methodology employed ensures that these insights are robust and reliable, making them essential contributions to discussions surrounding cyber autonomy.

The insights gained from this research not only provide a valuable framework but also serve as a crucial stepping stone for understanding and enhancing Cyber Autonomy in critical infrastructure businesses. By delving into the complexities of cyber threats and vulnerabilities, this research sheds light on the various factors that contribute to the effectiveness of cybersecurity measures.

Policymakers and industry leaders now have access to knowledge that can help them develop effective strategies and policies to safeguard against cyber threats. With a better understanding of the challenges faced by critical infrastructure businesses, they can proactively implement measures to strengthen overall cybersecurity resilience.

However, it is important to acknowledge that cybersecurity is an ever-evolving field. As technology continues to advance at a rapid pace, new threats and challenges constantly emerge. Therefore, continuous efforts and collaboration among stakeholders are necessary to stay ahead of these emerging challenges in the digital landscape.

Further research in cybersecurity practices will play an instrumental role in maintaining a secure and robust critical infrastructure environment. By continuously evaluating existing

practices and identifying areas for improvement, businesses can adapt their strategies to effectively mitigate evolving cyber threats.

The insights gained from this research act as a foundation for policymakers and industry leaders to enhance Cyber Autonomy in critical infrastructure businesses. However, it is essential to recognize the dynamic nature of cybersecurity and the need for constant innovation and collaboration among stakeholders.

Through ongoing research and evaluation of cybersecurity practices, critical infrastructure businesses can maintain a secure environment while adapting to emerging cyber threats.

The study results included in Tables 1 and 2 allow for a few implications for the conclusion. The research results obtained from experts from the European Union and the United States of America give important wide perspectives on Cyber Autonomy. Our work highlights several important aspects of information security: government, security, and defense levels, economic levels, and business levels. Cyber Autonomy plays a crucial role in the EU's security strategy, which may not be immediately apparent from civilian and military perspectives but is increasingly critical for information security professionals.

Business infrastructures of organizations cannot solely rely on securing their own activities; they can adopt an approach that incorporates Cyber Autonomy elements, including Infrastructure and Architecture, as well as reputation management. The Cyber Autonomy model offers two advantages. Firstly, it demonstrates that policy decisions made at the company level are interconnected with national security and economic considerations, providing an operational and pragmatic approach to safeguarding critical assets from both technical and non-technical perspectives.

Secondly, it helps maintain the resilience of infrastructure and information security architecture to ensure rapid recovery in the event of an incident. Furthermore, it is crucial to investigate the efficacy of risk assessment methodologies and the integration of risk management frameworks in the implementation of Cyber Autonomy. Gaining a deep understanding of accurately assessing risks and customizing autonomous cybersecurity measures will play a pivotal role in achieving comprehensive protection against cyber threats.

This article addressed the research objective of examining the significance of elements within Cyber Autonomy and evaluating the implementation phases. By incorporating insights from cybersecurity experts in the EU and USA, the study revealed the prominence of elements such as "Policies", "Reputation management", and "Infrastructure and Architecture" within the Cyber Autonomy framework. The research emphasized the importance of consistent rules and multi-level relationships encompassing information security, state policies, technical aspects, and the economy. Furthermore, the study highlighted the critical role of "Methods" and "Implementation Methods" in successful Cyber Autonomy deployment, along with the significance of the "Organization" business model in the implementation process. In order to effectively apply information security in government and businesses, specialists must have a shared and consistent understanding of requirements from technical, social, process, and business perspectives.

Further development of this research could include a comparative analysis of Cyber Autonomy perspectives and implementations in different industries or sectors that could provide valuable insights. Moreover, exploring the practical implications and challenges of implementing Cyber Autonomy in real-world scenarios would contribute to a deeper understanding of its effectiveness and potential limitations. As future development, it can include studying the effectiveness of risk assessment methodologies and the integration of risk management frameworks in implementing Cyber Autonomy. Additionally, exploring the specific challenges and regulatory considerations related to EU critical infrastructure defense would provide valuable insights into tailoring Cyber Autonomy approaches to address regional requirements and enhance resilience against cyber threats. Such research can contribute to the development of comprehensive risk management frameworks and guidelines for EU critical infrastructure sectors.

Cyber Autonomy is an innovative and forward-thinking approach to cybersecurity that aims to strengthen the protection of critical infrastructure within the European Union (EU). By granting autonomy to directives, frameworks, and guidelines, this approach ensures a consolidated cyber policy and operational guidance. This comprehensive overview allows for effective measures to be implemented, ultimately improving the overall level of cybersecurity in the region.

One key aspect of Cyber Autonomy is the implementation of the NIS Directives, which are designed to enhance national capabilities, promote cross-border collaboration, and establish national supervision of critical sectors. These directives demonstrate the importance of having an EU certification system for information security as a carrier. This system ensures that all entities responsible for safeguarding critical infrastructure meet specific standards and requirements, ensuring a consistent level of security across member states.

In addition to EU certifications, internationally recognized information security certifications such as CISSP (Certified Information Systems Security Professional) and CISM (Certified Information Security Manager) are widely adopted by EU information security experts. This adoption highlights the significance of standardization and expertise in managing cybersecurity teams. Having professionals with these certifications further strengthens the ability to effectively respond to cyber threats and mitigate risks.

Overall, Cyber Autonomy presents a promising approach to enhancing cybersecurity in the EU by providing comprehensive policy oversight, operational guidance, and legal measures. The incorporation of EU certification systems and internationally recognized qualifications demonstrates the commitment towards standardization and expertise in managing cybersecurity within the region. Furthermore, the adoption of internationally recognized information security certifications like CISSP and CISM by EU information security experts signifies the significance of standardization and expertise in managing cybersecurity teams.

The practical value of the study lies in the analyses of experts' insights, which offer actionable solutions for implementing Cyber Autonomy and risk management strategies in critical infrastructure businesses. The research provides adjustments to existing cybersecurity frameworks and directives, considering new cyber elements and information security realities. As a result, it serves as a guide for developing confidence-building measures to mitigate possible reputation and financial losses and reinforce protective actions against disinformation or negative cyber impacts.

By incorporating these findings into their practices, policymakers and industry leaders can enhance their cybersecurity strategies, ensuring robust protection against cyber threats and strengthening overall resilience. With cyber threats continuously evolving, a holistic and adaptive approach is necessary to maintain cyber security and safeguard critical infrastructure businesses effectively.

References.

1. European Commission (2017). *Joint Communication to the European Parliament and the Council: Resilience, Deterrence, and Defence: Building Strong Cybersecurity for the EU. Brussels: European Commission*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017JC0450.

2. Leroy, I. (2021). Cyber Autonomy Toolbox – Project Management Digital Transformation. *AARMS – Academic and Applied Research in Military and Public Management Science*, (pp. 95-110). ISSN 2498-5392. https://doi.org/10.32565/aarms.2021.2.ksz.7.

3. Leroy, I. (2021). *Cyber autonomy for business: building a European cyber resilience. Views on the progress of CSDP*. Luxembourg: Publications Office of the European Union. ISBN: 978-3-902275-48-6.
4. Knowles, W., Prince, S., Hutchison, D., Pagna Disso, J. F., & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection, 9*, 52-80. https://doi.org/10.1016/j.ijcip.2015.02.002.
5. Cartagena, S., Gosrani, V., Grewal, J., & Pikinska, J. (2020). Silent cyber assessment framework. *British Actuarial Journal, 25*, E2. https://doi.org/10.1017/S1357321720000021.
6. Fondation pour la Recherche Stratégique (n.d.). *FRS: The European Union between strategic autonomy and technological sovereignty: impasses and opportunities*. Retrieved from https://www.frstrategie.org/en/publications/recherches-et-documents/european-union-between-strategic-autonomy-and-technological-sovereignty-impasses-and-opportunities-2021.
7. *Ministère des Armées France: REVUE STRATÉGIQUE DE DÉFENSE ET DE SÉCURITÉ NATIONALE* (n.d.). Retrieved from https://www.viepublique.fr/sites/default/files/rapport/pdf/174000744.pdf.
8. FIIA (2021). *Report Strategic Autonomy and the transformation of the EU new agendas for the security, diplomacy, and trade technology. Finnish Institute of International Affairs*. Retrieved from https://www.fiia.fi/wp-content/uploads/2021/04/fiia-report-67_niklas-helwig-et-al_strategic-autonomy-and-the-transformation-of-the-eu.pdf.
9. Reinhold, T., & Reuter, C. (2023). *Preventing the escalation of cyber conflicts: towards an approach to plausibly assure the non-involvement in a cyberattack*. *Z Friedens und Konflforsch*. https://doi.org/10.1007/s42597-023-00099-7.
10. EPRS (2016). *European Parliament: CSDP. Cybersecurity in the EU Common Security and Defence Policy (CSDP). Challenges and risks for the EU. EPRS, European Parliamentary Research Service*. https://doi.org/10.2861/853031.
11. Kruszka, L., Klósak, M., & Muzolf, P. (2019). *Critical Infrastructure Protection: Best Practices and Innovative Methods of Protection*. Amsterdam: IOS Press. https://doi.org/10.3390/s23052415.
12. Danet, D., & Desforges, A. (2021). Souveraineté numérique et autonomie stratégique en Europe: du concept aux réalités géopolitiques. *Hérodote, 177-178*(2-3), 179-195. https://doi.org/10.3917/her.177.0179.
13. D'Ambrosio, A. (2014). *Cybersecurity: Executive Order 13636 and the Critical Infrastructure Framework*. Nova Science Publishers, Inc. ISBN-13: 978-1631176715.
14. Talesh, S. (2018). Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Businesses. *Law & Social Inquiry*, *43*(2), 417-440. https://doi.org/10.1111/lsi.1230.
15. European Union Agency for Cybersecurity (2015). *For Digital Service Providers (NIS Directive) – ENISA (europa.eu)*. Retrieved from https://www.enisa.europa.eu/topics/incident-reporting/for-digital-service-providers-nis-directive.
16. Ponemon Institute (2020). *Cost of a Data Breach Report: European Union. Ponemon Institute LLC*. Retrieved from https://www.ibm.com/security/data-breach.
17. Linstone, H.A., & Turoff, M. (2021). Introduction, *In Delphi method: Techniques and applications*. Addison-Wesley, 12. https://doi.org/10.2307/3150755.
18. COUNCIL DECISION, CFSP 2020/1127: Amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. *Official Journal of the European Union*. Brussels: 2020, Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020D1127&from=E.
19. Jamshed, S. (2014). Qualitative research method-interviewing and observation. *Journal of Basic and Clinical Pharmacy*, *5*(4), 87-88. https://doi.org/10.4103/0976-0105.141942.

Захист критичної інфраструктури: бачення кібер-експертів ЄС і США

І. Лерой[1,2], *І. Золотарьова*[*3]

1 – Університет Лотарингії, м. Нансі, Французька Республіка
2 – Європейський коледж безпеки та оборони, м. Брюссель, Королівство Бельгія
3 – Харківський національний університет імені Семена Кузнеця, м. Харків, Україна
[*] Автор-кореспондент e-mail: iryna.zolotaryova@ hneu.net

Мета. Аналіз елементів кібернетичної автономії на основі досвіду висококваліфікованих і досвідчених експертів з Європейського Союзу (ЄС) і Сполучених Штатів Америки (США). Розрахунок цінності кожного елемента шляхом отримання даних зі структурованих глибинних інтерв'ю.

Методика. Під час вивчення різних аспектів дослідження був застосований метод Дельфі, а дослідницькі інтерв'ю включали опцію перегляду транскрипту інтерв'ю респондента (ITR). Метод Дельфі оброблявся в кілька раундів, зазвичай три, причому два раунди розглядалися як мінімум, і в цьому відношенні метод Дельфі допоміг дослідженню, що пропонується, вивчити, спрогнозувати й визначити природу та основні елементи кібернетичної автономії.

Результати. Результати дослідження демонструють, що такі елементи, як «Політика», «Управління репутацією» та «Інфраструктура та архітектура» мають суттєве значення для кібернетичної автономії. Ці елементи вважаються критично важливими для майбутніх перспектив. Дослідження підкреслює роль кібернетичної автономії в оптимізації підходів до кібербезпеки, пом'якшенні наслідків кібератак і захисті від можливої репутаційної шкоди. Дослідження також підкреслює важливість чітко визначених методів імплементації та організаційної структури для успішного розгортання кібернетичної автономії.

Наукова новизна. Дослідження відображає міждисциплінарний характер сфери кібербезпеки та застосовує комплексний підхід, що охоплює інформаційну безпеку, політику інформаційної безпеки, технічні та економічні аспекти, і зазначає важливу роль управління репутацією у процесі відновлення вартості акцій компанії. Кіберавтономія може запропонувати концепцію захисту репутації, яка допомагає виявити потенційні кіберзагрози, що ще більше посилюються у зв'язку з розвитком різноманітних платформ для дистанційного керування штучним інтелектом, дистанційним навчанням і можливостями автономної роботи корпоративних систем, впливом транснаціональних компаній на фінансові ринки, та автоматизовані системи прийняття рішень.

Практична значимість. Проаналізовані інсайти експертів, що можуть допомогти знайти практичні рішення для забезпечення кіберавтономії та методів управління ризиками при реалізації стратегії кіберстійкості для критичної інфраструктури. Дослідження пропонує коригування існуючих рамок і директив із кібербезпеки, що враховують нові кіберелементи реалій інформаційної безпеки. Дане дослідження може бути використане як посібник для заходів зі зміцнення довіри до можливих репутаційних і фінансових втрат, посилення заходів захисту від дезінформації або негативного кібервпливу.

Ключові слова: *кібернетична автономія, критична інфраструктура, кібератака, зменшення ризиків*

The manuscript was submitted 03.06.23.