Multidisciplinary Reviews

REVIEW ARTICLE
Published Online: June 11, 2024
https://doi.org/10.31893/multirev.2024spe021

Global cybersecurity: Harmonising international standards and cooperation

Serhii Lysenko[a] ✉ | **Andrii Liubchenko**[b] | **Volodymyr Kozakov**[c] | **Yurii Demianchuk**[d] | **Yurii Krutik**[e]

[a]Interregional Academy of Personal Management, Kyiv, Ukraine.
[b]Law office, Kyiv, Ukraine.
[c]Department of Management and Administration, Elementary Science Institute of Information Protection, National University of Information and Communication Technologies, Kyiv, Ukraine.
[d]Department of Law, Faculty of Management and Law, Vinnytsia National Agrarian University, Vinnytsia, Ukraine.
[e]Department of Law and Law Enforcement, Faculty of National Security, Law and International Relations, Zhytomyr Polytechnic State University, Zhytomyr, Ukraine.

Abstract The growing dependence of modern society on digital technologies leads to an increase in cyber threats, which makes the issue of cyber security particularly relevant. The problem of the research is to determine the effective mechanisms of protection of information systems in the conditions of globalization and growing geopolitical challenges. The purpose of the article is to analyze the development of international data privacy standards, the role of the latest technologies in cyberspace protection, and the formation of an effective global network strategy. Special attention is paid to the directions of international cooperation in the development of technological innovations and the training of qualified personnel. The article examines the legal, technological and educational aspects of data security policy, analyzes the experience and practices of different countries, which allows determining effective directions for improving the effectiveness of protection against cyber threats. Based on the conducted research, the main challenges and prospects for the development of the global defense system were determined, including the need to integrate efforts at the international level and integrate into the rapidly changing conditions of cyberspace. The results emphasize the importance of creating a unified global network protection system that ensures the protection of relevant information resources and the privacy of personal data in the digital world. Outlined recommendations for the effective integration of countermeasures into national and international strategies can serve as a factor in ensuring a secure digital future and building an appropriate infrastructure. The results of the article highlight the critical role of global cyber security in ensuring stability and security in today's digital world, emphasizing the need for a comprehensive approach to its implementation.

Keywords: internet communication, cyber policy, personal data, cyber security, information security, public administration

1. Introduction

In today's world, the construction of digital infrastructure and the transition of business to a digital format is of crucial importance for ensuring competitiveness, optimizing processes and expanding market opportunities. According to (Shreve, 2023), digital transformation allows companies to reach a new level of interaction with customers through the introduction of innovative online services, the automation of internal processes and the processing of large volumes of data for making informed management decisions. The development of digital infrastructure, including broadband Internet, cloud technologies, relevant software, which is fundamental to the digital economy. Author (Reddi, 2023) emphasizes with these processes, the risk of cyber-attacks increases, which requires companies to pay more attention to data protection. Strategic planning and investments in digital infrastructure are becoming critical to ensuring business resilience in the face of rapid technological change.

The growth of cybercrimes and the manipulation of personal data is becoming a challenge in connection with the reorientation of financial flows and personal information into the digital space. According to (Tang, 2023), the digital economy, with its growing reliance on online transactions, e-commerce and digital services, creates an enabling environment for cybercriminals who use varied methods to commit fraud, extortion, intellectual property theft and data breaches. Data manipulation and financial fraud directly harm victims and undermine the trust in digital transactions that is the foundation of the digital economy. Ensuring the reliability of information flow is becoming a key risk management factor for business, creating demand for the development and implementation of information assets and systems.

Strengthening the infrastructure for deterring cyber threats, international cooperation and the integration of the latest technologies are leading elements in strengthening global security in the digital world. Opinions (Hassan, 2023) reflect the

development of digital monitoring mechanisms to analyze and neutralize cyber threats, ensuring data immutability and the expanded use of cryptography to protect information are an integral part of digital environment security strategies. International cooperation, in the form of exchange of information about threats, joint research and development of protection standards, helps countries and companies to more effectively resist cyber-attacks. Despite significant efforts in the development of software and data encryption, the constant development of technology and the evolution of cybercrime methods require all participants in the digital economy to continuously pay attention to counterattacks, as only rapid adaptation to new fraud methods is an effective means of combating digital crime.

2. Literature Review

The issue of cyber security around the world is gaining relevance in connection with the rapid development of digital technologies and the increase in the number of cyber-attacks. Scientists and researchers are trying to find effective strategies to protect information systems from attackers. The work (Botta, 2023) analyzes the influence of international legislation on the development of data security, emphasizing the importance of harmonization of legal norms between different countries. The study (Cains, 2022) focuses on the technological aspects of cyber defense, the application of cloud technologies and cryptography to counter cyber-attacks, pointing to the potential of automated analysis and response to threats. The article (Aslan, 2023) highlights the problems of ensuring privacy in the context of the globalization of personal data, where every connected device can become a potential vector for an attack.

In the study (Khan, 2023), the issue of information protection was carried out on the basis of statistical information on cyber-attacks, their types, frequency and available software that allows effective protection of information systems. The author (Fan, 2023) provides an overview of incidents over the past decade, which demonstrates trends in the increasing complexity and scope of conducting digital investigations. The article (Marican, 2023) is devoted to the study of the effectiveness of anti-virus software and the development of new methods of cryptographic data protection.

The scientist (Cartwright, 2023) emphasizes the need to integrate web networks into the overall digitalization strategy of enterprises, analyzing cases of the implementation of complex security systems at different levels of the organizational structure. According to (Raju, 2022), the formation of a general cyber security strategy for the world in the conditions of growing geopolitical threats is a task for the international community. The work (Nguyen, 2023) examines various models of international cooperation in the direction of stabilizing information networks, including exchange of information about threats and coordinated response to incidents.

The study (Eze, 2023) highlights the role of national strategies in shaping global digital security, analyzing the successes and shortcomings of existing approaches in different countries. Statements (Muthuswamy, 2023) propose the concept of global cyber hygiene as a basis for the development of international standards of behavior in cyberspace, which includes educational programs, norms of conduct and technical requirements to ensure data security. A scientific view (Hasan, 2023) allows for the formation of an effective and flexible system of the digital environment, capable of adapting to the rapidly changing digital world.

According to recent studies (Azambuja, 2023), enterprises are at risk of sophisticated attacks due to phishing attacks, which requires the improvement of specialized software. The scientist (Bhol, 2023) emphasizes the importance of the development of international cyber security standards, which should serve as the basis for the creation of a single global system for the protection of information resources. Research (Shreve, 2023) due to the need to counter cross-border digital attacks that do not fall under the jurisdiction of certain countries.

The author (Safaei, 2023) highlights the potential of big data and cloud services in detecting and neutralizing cyber-attacks, emphasizing the need to develop an ethical framework for the use of technologies in cyber security. An article (Patterson, 2023) emphasizes the need to integrate technological innovation with legal and ethical principles to ensure personal and corporate privacy. According to (Vesić, 2023), one of the main challenges for global information security is the protection of critical infrastructure and digital services that are becoming integrated into the everyday life of society.

The author (Pöyhönen, 2023) points to the development of international mechanisms for rapid response to incidents of cyberattacks, the leveling of which is possible only under conditions of close cooperation between governments, the private sector and academic circles. The work (Zwilling, 2022) emphasizes the importance of developing universal training programs for training qualified specialists in the field of cyber security. The researcher (Wazid, 2022) emphasizes the role of global cooperation in solving the problems of cryptography, pointing to the need to join efforts to create a secure digital space based on encryption.

Therefore, the formation of a general cyber security strategy in the world in the conditions of growing geopolitical threats requires a comprehensive approach, which includes the development and implementation of innovative technologies, international legal regulation and training of specialists. Researchers say that efforts should be directed at raising awareness of cyber threats among the population, strengthening the international regulatory framework, and developing technological solutions that can adapt to the ever-changing conditions of cyberspace. indicating the need to join forces to create a secure digital space based on encryption.

3. Research Purpose

The purpose of the article's research is to develop effective strategies and mechanisms for ensuring cyber security in the conditions of a globalized digital economy, taking into account the rapid development of technologies and the growth of cyber threats. The key issue focuses on the need to protect information systems from cyber-attacks that threaten the confidentiality, integrity and availability of critical data. The tasks of the research include the analysis of the current state of cyber threats, the study of international practices in the field of data protection, the development of recommendations for increasing the effectiveness of cyber protection, and the integration of the latest technologies for preventive protection against potential cyber-attacks. The practical value of the research lies in the formation of a comprehensive approach to cyber security, which will contribute to strengthening the protective mechanisms of organizations and states, increasing the level of public education in digital literacy and ensuring the stable development of the digital economy.

4. Materials and Methods

The methodology chosen for the research is focused on the analysis of the legal foundations of the development of information security in the international environment and the study of the technological characteristics underlying modern cyber protection systems. A combined approach including quantitative and qualitative analysis was used to achieve this. Qualitative analysis consists in the study of international treaties, conventions and national legislative acts of leading countries in the field of data security to identify the main legal principles and regulatory mechanisms. Quantitative analysis includes the collection and processing of data on the technological characteristics of defense systems, using specialized databases, indices of cyber security and digitization.

The integrated approach made it possible to assess the effectiveness of existing information security mechanisms and determine directions for their improvement. The article focuses on the use of statistical information on cyber-attacks, the analysis of the development of software for the preservation of information and the assessment of the general state of digitization in countries with different levels of economic development. Statistical data are obtained from open sources, reports of international organizations and research institutes. The use of statistical analysis made it possible to identify trends and regularities in the spread of cyber-attacks, to assess the effectiveness of the application of modern policies of developed countries to ensure the protection of the Internet space. Special attention is paid to the assessment of the impact of the level of digitalization on the ability of countries to resist cyber threats and the creation of appropriate actions to ensure the development of digital literacy and the formation of policies to minimize digital attacks. On the basis of the interpreted data and the conducted analysis, recommendations were formulated for the formation of a general strategy for cyber defense of the world, which takes into account the existing geopolitical threats and challenges.

The recommendations included proposals for strengthening international cooperation in the field of building information networks, developing uniform standards for information protection, and optimizing the effectiveness of web resource systems. An important component of the strategy is to increase the awareness of citizens and organizations about cyber threats and methods of their prevention, the development of scientific research on network protection with the aim of identifying the latest protection technologies. The proposed measures should only minimize the risks of cyber-attacks and create conditions for the safe development of the digital economy at the global level.

5. Results

The development of innovative technologies and digitalization of society, business, and other spheres of life have become defining trends of recent decades, opening new horizons for progress and growth. The digitalization of society covers a wide range of aspects, starting with the everyday life of citizens, who now have the opportunity to use online services for making purchases, booking services, communicating with government institutions, and complex automation of production processes at enterprises. The introduction of innovative technologies strengthens business models, increases the efficiency of operations and creates new platforms for the commercialization of business processes. Cloud technologies are being used in healthcare through the development of personalized treatment plans, in the financial sector through the automation of credit scoring and risk management, and automated systems are transforming agriculture by innovating yield and resource management.

Along with the unprecedented opportunities opened up by digitalization, new challenges arise due to the spread of criminality into the digital sphere. Digital technologies give attackers the tools to develop sophisticated attack schemes, which complicates the process of tracking and monitoring them. Cybercrime covers a wide range of illegal activities, including phishing, credit card fraud, malware distribution, attacks on corporate networks, and extortion. The complexity of cybercrimes lies in the technical ingenuity of criminals and the international nature of their activities, which complicates the process of identification, tracking, and prosecution for law enforcement agencies. The investigation requires states, companies, and individual users to take enhanced security measures and develop comprehensive protection strategies to protect personal data and create specialized software.

The response to growing cyber threats was the formation of international institutions and legal frameworks aimed at strengthening cyber security and promoting international cooperation. The creation of the Budapest Convention on Cybercrime and the strengthening of intergovernmental initiatives in the form of UN cybersecurity experts play a key role in standardizing approaches to combating cybercrime and protecting critical infrastructure. The effort is complemented by international security standards ISO/IEC 27001, which provide organizations with guidance on implementing effective information security management systems. International cooperation is expanding through bilateral and multilateral agreements between countries aimed at sharing threat information, joint training and coordinating incident responses, which significantly strengthens global digital security. The main international standards and policies in the field of cyber security are listed in Table 1.

Table 1 International standards and cyber policy in the global environment.

International standards	Cyber policy	Cooperation between countries
ISO/IEC 27001 is an international standard for an information security management system (ISMS), which sets requirements for an organization to implement, maintain, and continuously improve an ISMS.	EU Cyber Security Strategy - Aimed at strengthening cyber resilience, combating cybercrime and developing international cooperation in the field of cyber security.	UN Global Compact on Cyber Security - Efforts to Develop an International Code of Conduct in Cyberspace.
NIST Cybersecurity Framework - Developed by the US National Institute of Standards and Technology to help organizations manage and reduce cyber risks.	China's Cyber Law - Includes the Cyber Security Law, which requires companies to store user data within the country and increases control over the internet space.	NATO-EU Cyber Defense Partnership - Cooperation aims to share best practices, threat intelligence and joint training.
GDPR (General Data Protection Regulation) - European standard regulating the processing of personal data, setting high data protection requirements.	US Cybersecurity Act - Provides the legal framework to protect infrastructure from cyberattacks, includes measures for cooperation between the government and the private sector.	International cooperation through INTERPOL - Facilitates global cybercrime information sharing and response coordination.
PCI DSS (Payment Card Industry Data Security Standard) - International data security standard for all organizations that process payment cards.	India's Cyber Security Strategy - Encompasses comprehensive measures to protect critical information infrastructure and enhance national cyber security.	ASEAN Multilateral Agreements - Aimed at improving cyber security and cyber resilience of member countries through joint initiatives and training.
The Budapest Convention on Cybercrime - The first international treaty aimed at combating cybercrime, contributes to the harmonization of national legislation and the improvement of international cooperation.	Australia's Cyber Security Strategy - Focused on strengthening cyber resilience, protecting critical infrastructure and developing national cyber capabilities.	G7 Cyber Expert Group - A working group on cybersecurity that develops joint approaches to strengthening financial stability through cyber resilience.

Source: NSCI (2023)

The period of the COVID-19 pandemic has become a time of unprecedented digitalization of society and business, which has led to a significant increase in cyber-attacks. The spread of the virus forced companies to switch to remote work en masse, creating new challenges for information security due to the need to secure the large number of remote connections and personal devices used to access corporate networks. Attackers quickly took advantage of the situation, increasing the volume of phishing attacks, malware distribution and ransomware-type attacks that blocked access to critical data and systems. These attacks caused direct damage to businesses and government institutions, which posed a number of potential threats to national security. The pandemic has highlighted the need for a more thorough approach to cyber security and the acceleration of digital transformation in the area of information protection.

European countries are actively working to strengthen their national cyber security strategies to respond to growing cyber threats. The European Union has adopted a number of initiatives aimed at increasing the level of cyber security among member states, including the Directive on the Security of Networks and Information Systems (NIS Directive), which requires critical infrastructures to ensure an adequate level of protection of their networks and systems. An important step was the introduction of the General Data Protection Regulation (GDPR), which sets strict requirements for the processing of personal data. The European Union emphasizes the development of cooperation between countries in the field of cyber security through the creation of a network of cyber security centers and the initiative of the Digital Single Market, which provides for the pooling of resources for the development of innovative and safe digital technologies. The measures are aimed at protecting against

cybercriminals and supporting innovative development, as it is critical for Europe's economic growth and competitiveness. The largest part of cyberattacks occurred in 2018-2020, which became a factor in the active development of global digital security networks, more details about the cost of crimes are shown in Figure 1.

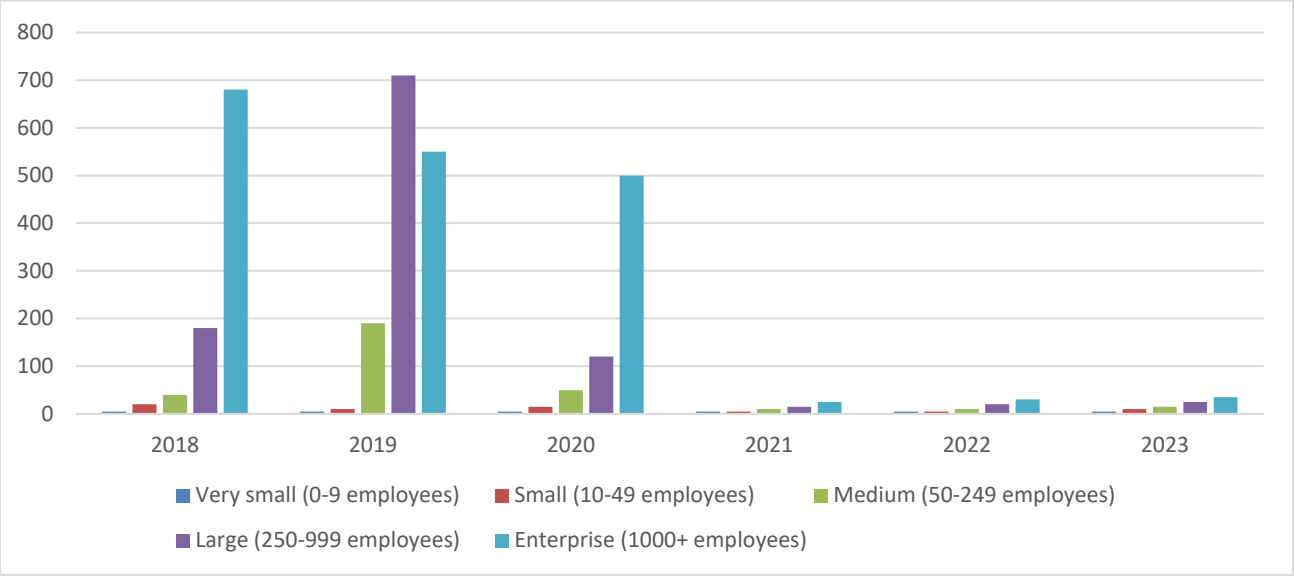

Figure 1 Average cost of all cyber attacks to European and North American firms from 2018 to 2023, by size (in 1,000 US dollars).
Source: Statista (2023)

Strengthening cooperation between countries in the field of cyber security is becoming a decisive factor in ensuring resilience to cyber threats on a global scale. A central aspect of the cooperation is the sharing of advanced technologies and developments that can detect and neutralize cyberattacks before they cause damage. Includes joint development and implementation of early warning systems, use of big data to analyze cyber threats, blockchain technologies to ensure data security. Global cooperation involves the standardization of cyber security protocols and ensuring the compatibility of technological solutions between different countries, which allows to effectively combat cybercrime at the international level. The integration of efforts in the field of cyber security forms the development of training programs and the exchange of expertise between specialists, which serves to increase the general level of awareness and preparedness for cyber challenges among partner countries.

Effective digitalization of enterprises is critical for increasing their competitiveness and efficiency, but it also opens up new vectors for potential cyber-attacks. In order to reduce these risks, companies implement comprehensive cyber security strategies that cover the technical aspects of protecting information systems, organizational measures in the form of regular staff training and the development of incident response plans. The use of modern infrastructure designed to analyze anomalies in network behavior, encrypt data to protect against unauthorized access, ensure immutability of records, allows enterprises to ensure a high level of protection of their digital assets. A key aspect of effective digitalization is the development of a cyber security culture within the organization, which involves the awareness of each employee of his role in ensuring the security of information resources. The most powerful European countries in the field of cyber security are shown in Table 2, which is explained by their effective approach to digitalization and provision of the corresponding infrastructure.

Table 2 National cyber security index in European countries, 2023.

Rank	Country	National Cyber Security Index	Digital Development Level
1	Belgium	94.81	74.07
2	Lithuania	93.51	67.34
3	Estonia	93.51	75.59
4	Czech Republic	90,91	69.21
5	Germany	90,91	80.01
6	Romania	89.61	59.84
7	Greece	89.61	64.02
8	Portugal	89.61	68.46
9	United Kingdom	89.61	79.96
10	Spain	88,31	72.21

Source: NSCI (2023)

The intensification of geopolitical competition in recent years has led to an increase in the number of cyberattacks aimed at the virtual assets of states and large corporations. Attacks are aimed at economic damage, political influence, espionage, or even undermining state sovereignty. The use of cyberspace as an arena for geopolitical confrontations requires countries to develop effective national cyber security strategies and active international cooperation to counter common threats. International agreements and regulatory initiatives are gaining importance, which will try to harmonize the legislation of different countries in order to more effectively bring perpetrators to justice. Given the continuous development of technology and the changing tactics of cybercriminals, countries must be ready to quickly adapt their defense mechanisms and strengthen international cooperation to ensure effective protection against cyber threats in a complex geopolitical space.

Strengthening diplomacy and digitization strategies plays a fundamental role in the formation of a sustainable and secure digital space. The development of international norms and standards of cyber security is an example of effective international cooperation, which contributes to the creation of a unified legal framework for combating cyber threats. Diplomatic initiatives and bilateral and multilateral agreements between countries are aimed at exchanging threat information, coordinating actions to improve infrastructure protection, and jointly developing technological solutions. Modern international cooperation makes it possible to effectively counter common challenges in the field of cyber security and promotes the development of the digital economy, opening up new opportunities for technological progress and economic growth of countries.

6. Discussion

In the conditions of global digitalization, scientists emphasize the critical importance of international cooperation and the development of common standards for countering cross-border threats. The article (Aslan, 2023) points to a growing community awareness of the need for collective action in the field of building secure information networks, which corresponds to the results obtained. According to (Reddi, 2023), observations indicate the increasing role of digital assets and the strengthening of mechanisms for monitoring their circulation. The author (Patterson, 2023) points to the need for a balance between innovativeness and ethical considerations in cyber security strategies. An analysis (Zouqiong, 2023) regarding the impact of cyberattacks on critical infrastructure and digital services reflects the results of his own conclusions about the importance of protecting information systems in the context of growing digitalization. The article (Galinec, 2023) emphasizes the importance of adapting international response mechanisms to the modern challenges of cyberspace and building new points of interaction in conditions of geopolitical confrontation.

Special attention to the training of qualified specialists in the field of data security is indicated by statements (Klien, 2022), which coincide with our results regarding the strengthening of human capital as the basis of effective cyber defense. Opinions (Catal, 2023) reflect a common understanding of how educational programs and international cooperation can significantly enhance global security. According to (SEKİ, 2023), the discussion of global information security strategies and its role in countering geopolitical threats reflects the gradual creation of effective software. The obtained results confirm theses (Jamil, 2023) regarding the importance of the development of international legal frameworks in the sphere of the functioning of the economic environment and the circulation of digital assets. The hypothesis (Bjelajac, 2023) is confirmed by the results regarding the harmonization of international legislation for the effective fight against cybercrime, which is complicated by its transnational nature.

According to (Ugwu, 2023), investments in the latest technologies should be divided between the digitalization of public institutions and ensuring the conduct of safe commercial activities of the corporate sector, which indicates the increased development of European markets. Thus, the research's own results not only reflect general trends in the field of cyber security, but also emphasize the need for further research to develop more effective and adaptive protection strategies.

7. Conclusion

Thus, the processes of discussing the importance of cyber security in global digitalization relate to modern society, which is faced with cases of cyber-attacks and the impact on privacy. The development of innovative technologies and digitalization open up new opportunities for the development of business, education, medicine and many other spheres of life, contributing to the improvement of efficiency, availability and quality of services. However, in parallel with the positive factors, the growing dependence on digital technologies increases the vulnerability of society in the face of information networks that are becoming more and more extensive and complex. Strengthening cybersecurity cooperation between countries, businesses, and international organizations, building modern infrastructure, and adapting to rapid software development are critical to a secure digital future.

In the digital environment, there are significant challenges and global challenges that extend to financial systems and virtual assets. Among them is the growth of digital crime, which is becoming organized and technologically equipped, capable of using weak points in information systems to carry out large-scale attacks. There is a risk of geopolitical conflicts moving into the digital plane, where cyberspace is used as a field for waging hybrid wars. Ensuring the legal order requires the international community to create technological means of protection, to form an effective legal framework capable of facing new challenges.

Ensuring privacy and protection of users' personal data contributes to the development of web resource technologies for the implementation of reliable information protection mechanisms.

Recommendations and necessary measures should include a number of strategic initiatives to strengthen the monitoring of the web space and create a reliable response system. International cooperation needs to be strengthened through the development of common cybersecurity standards and the exchange of information on threats and best practices for protection. The global community should focus on the development of national strategies for the formation of information networks, which include comprehensive action plans for the protection of critical infrastructure and raising the awareness of citizens on issues of cyber hygiene. It is important to stimulate innovation in the field of protection of information systems, through investments in research and development of advanced cyber protection technologies. The issue of training personnel potential and specialists in the field of data security, ensuring their competences for effective resistance to modern and future threats is becoming critical. Implementation of the recommendations requires coordinated efforts at the national and international levels, active participation of the private sector and civil society to ensure a safe digital environment for all.

Ethical considerations

Not applicable.

Conflict of Interest

The authors declare no conflicts of interest.

Funding

This research did not receive any financial support.

References

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics, 12*(6), 1333. https://doi.org/10.3390/electronics12061333

Botta, A., Rotbei, S., Zinno, S., & Ventre, G. (2023). Cyber security of robots: A comprehensive survey. *Intelligent Systems with Applications, 18*. https://doi.org/10.1016/j.iswa.2023.200237

Cains, M., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2022). Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation. *Risk Analysis, 42*(8), 1643–1669. https://doi.org/10.1111/risa.13687

Cartwright, A., Cartwright, E., & Edun, E. S. (2023). Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies. *Computers and Security, 131*. https://doi.org/10.1016/j.cose.2023.103288

Catal, C., Ozcan, A., Donmez, E., & Kasif, A. (2023). Analysis of cyber security knowledge gaps based on cyber security body of knowledge. *Education and Information Technologies, 28*(2), 1809–1831. https://doi.org/10.1007/s10639-022-11261-8

De Azambuja, A. J. G., Plesker, C., Schützer, K., Anderl, R., Schleich, B., & Almeida, VR (2023). Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0 - A Survey. *Electronics, 12*(8), 1920. https://doi.org/10.3390/electronics12081920

Eze, V. H. U., Ugwu, C. N., & Ugwuanyi, I. C. (2023). A Study of Cyber Security Threats, Challenges in Different Fields and its Prospective Solutions. A Review. *INOSR Journal of Scientific Research, 9*(1), 13–24. https://www.researchgate.net/publication/367742804. Accessed: March 28, 2024.

Fan, Z., Zhao, P., Jin, B., Tang, Q., Zheng, C., & Li, X. (2023). Research on Key Method of Cyber Security Situation Awareness Based on ResMLP and LSTM Network. *IETE Journal of Research*. https://doi.org/10.1080/03772063.2023.2176365

Galinec, D. (2023). Cyber Security and Cyber Defense: Challenges and Building of Cyber Resilience Conceptual Model. *International Journal of Applied Sciences & Development, 1*, 83–88. https://doi.org/10.37394/232029.2022.1.10

Garcia-Perez, A., Cegarra-Navarro, J., Sallos, M., Martinez-Caro, E., & Chinnaswamy, A. (2023). Resilience in healthcare systems: Cyber security and digital transformation. *Technovation, 121*. https://doi.org/10.1016/j.technovation.2022.102583

Gupta Bhol, S., Mohanty, J.R., & Kumar Pattnaik, P. (2023). Taxonomy of cyber security metrics to measure strength of cyber security. *Materials Today: Proceedings, 80*, 2274–2279. https://doi.org/10.1016/j.matpr.2021.06.228

Hasan, M. K., Habib, A. A., Shukur, Z., Ibrahim, F., Islam, S., & Razzaque, M. A. (2023). Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. *Journal of Network and Computer Applications, 209*. https://doi.org/10.1016/j.jnca.2022.103540

Jamil, A. S., Azeez, R. A., & Hassan, N. F. (2023). An Image Feature Extraction to Generate a Key for Encryption in Cyber Security Medical Environments. *International Journal of Online and Biomedical Engineering, 19*(1), 93–106. https://doi.org/10.3991/ijoe.v19i01.36901

Khan, N.F., Ikram, N., Saleem, S., & Zafar, S. (2023). Cyber-security and risky behaviors in a developing country context: a Pakistani perspective. *Security Journal, 36*(2), 373–405. https://doi.org/10.1057/s41284-022-00343-4

Marican, M. N. Y., Razak, S. A., Selamat, A., & Othman, S.H. (2023). Cyber Security Maturity Assessment Framework for Technology Startups: A Systematic Literature Review. *IEEE Access, 11*, 5442–5452. https://doi.org/10.1109/ACCESS.2022.3229766

Mishra, S. (2023). Exploring the Impact of AI-Based Cyber Security Financial Sector Management. *Applied Sciences, 13*(10). https://doi.org/10.3390/app13105875

Muthuswamy, V. V. (2023). Cyber Security Challenges Faced by Employees in the Digital Workplace of Saudi Arabia's Digital Nature Organization. *International Journal of Cyber Criminology, 17*(1), 40–53. https://doi.org/10.5281/zenodo.4766603

Nguyen, T. T., & Reddy, V.J. (2023). Deep Reinforcement Learning for Cyber Security. *IEEE Transactions on Neural Networks and Learning Systems, 34*(8), 3779–3795.https://doi.org/10.1109/TNNLS.2021.3121870

NSCI (2023). *National cyber security index in Europe*. https://ncsi.ega.ee/ncsi-index/?order=rank&archive=1. Accessed on March 28, 2024.

Patterson, C. M., Nurse, J. R. C., & Franqueira, V. N. L. (2023). Learning from cyber security incidents: A systematic review and future research agenda. *Computers and Security, 132*. https://doi.org/10.1016/j.cose.2023.103309

Pöyhönen, J., Simola, J., & Lehto, M. (2023). Basic Elements of Cyber Security for a Smart Terminal Process. International Conference on Cyber Warfare and *Security, 18*(1), 300–308. https://doi.org/10.34190/iccws.18.1.966

Raju, R., Rahman, N. H. A., & Ahmad, A. (2022). Cyber Security Awareness in Using Digital Platforms Among Students in A Higher Learning Institution. *Asian Journal of University Education, 18*(3), 756–766. https://doi.org/10.24191/ajue.v18i3.18967

Safaei Pour, M., Nader, C., Friday, K., & Bou-Harb, E. (2023, May 1). A Comprehensive Survey of Recent Internet Measurement Techniques for Cyber Security. *Computers and Security, 128.* https://doi.org/10.1016/j.cose.2023.103123

Seki, T., Çimen, F., & Dilmaç, B. (2023). The Effect of Emotional Intelligence on Cyber Security: The Mediator Role of Mindfulness. *Bartın Üniversitesi Eğitim Fakültesi Dergisi, 12*(1), 190–199. https://doi.org/10.14686/buefad.1040614

Shreeve, B., Gralha, C., Rashid, A., Araújo, J., & Goulão, M. (2023). Making Sense of the Unknown: How Managers Make Cyber Security Decisions. *ACM Transactions on Software Engineering and Methodology, 32*(4). https://doi.org/10.1145/3548682

Statista. (2023). Average cost of all cyber attacks to European and North American firms from 2018 to 2023, by size. *https://www.statista.com/statistics/1008112/european-north-american-firms-cyberattack-cost.* Accessed on March 28, 2024.

Vesić, S., & Bjelajac, M. (2023). Cyber security of a critical infrastructure. *Law - Theory and Practice, 40*(2), 77–88. https://doi.org/10.5937/ptp2302077v

Wazid, M., Das, A. K., Chamola, V., & Park, Y. (2022). Uniting cyber security and machine learning: Advantages, challenges and future research. *ICT Express, 8*, 313–321. https://doi.org/10.1016/j.icte.2022.04.007

Zouqiong H. (2023). Cyber Security Evolution and Conceptualization. *Social Science Journal for Advanced Research, 3(1),* 1–5. *https://ssjar.singhpublication.com.* Accessed on March 28, 2024.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems, 62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269