Digital forensics and cyber threat management during wartime: Analysis of new legislative initiatives*

Vasyl Yatskiv[1,†], Mykhailo Kasianchuk[1,†], Ludmila Babala[1,†] and Serhii Kulyna[1,*,†]

[1] West Ukrainian National University, 11 Lvivska str., 46009 Ternopil, Ukraine

Abstract

Digital forensics and cyber threat management have become critical components of national security during prolonged martial law conditions in Ukraine. The intensification of cyberattacks, including activities by hacking groups like Strontium and widespread distribution of malicious software such as Cobalt Strike Beacon, necessitates the development of effective coordination mechanisms between various security agencies. To minimize potential damage to Ukraine's national cybersecurity and reduce negative consequences at the state level, the task of creating specialized management architectures and developing improved methods and models for cyber threat response is urgent. That is why the theoretical mathematical representation of cyber threat management parameters through centralized, decentralized, and hybrid coordination models allows solving the actual scientific and practical task of formalizing the process of optimizing incident response times and enhancing the resilience of critical information infrastructure. Previously, centralized coordination models were primarily used, and now, as their evolution, hybrid management approaches have been proposed due to the integrated mathematical representation of parameters characterizing: threat detection processes, incident analysis procedures, coordination mechanisms between security entities (SBU, State Special Communications Service, General Staff, NSDC), threat mitigation strategies, and legislative frameworks implementation according to Law No. 4336-IX. The theoretical framework allows determining sets of input and output parameters for the formation of specialized coordination centers and formalization of the cyber threat management process under martial law conditions. The research demonstrates that hybrid coordination models (HCM) provide optimal balance between response speed and action coordination, showing two times higher efficiency compared to centralized models when managing large numbers of security entities. In the future, to implement the above-mentioned processes, it is necessary to develop comprehensive methods for assessing cyber threat management effectiveness both separately for individual security entities and for the integrated national cybersecurity system as a whole.

Keywords

cyber threat management, digital forensics, martial law cybersecurity, hybrid coordination models, incident response optimization, legislative frameworks

1. Introduction

Under the conditions of prolonged martial law in Ukraine, one of the most pressing national security challenges is ensuring effective cyber threat management and protecting the state's critical information infrastructure. Since the beginning of the full-scale aggression, numerous cyberattacks on Ukraine have been documented, including attempts by the Strontium hacking group to gain access to computer networks in Ukraine, the US, and the EU, attacks on the Ukrtelecom provider, and the distribution of malicious software such as Cobalt Strike Beacon [1]. This typically gives rise to coordination problems between different agencies, ensuring timely response to cyber incidents [2], and maintaining the resilience of critical systems during their operation under constant cyberattacks [3, 4]. The unprecedented scale and intensity of cyber warfare during the conflict have exposed significant vulnerabilities in existing cybersecurity frameworks and highlighted the need for comprehensive legislative reforms. The evolving nature of cyber threats, combined with the dynamic operational environment of martial law, requires adaptive and resilient management

* CSDP'2025: Cyber Security and Data Protection, July 31, 2025, Lviv, Ukraine

* Corresponding author.

† These authors contributed equally.

jazkiv@ukr.net (V. Yatskiv); kasyanchuk@ukr.net (M. Kasianchuk); ludaduma7@gmail.com (L. Babala); sersks@gmail.com (S. Kulyna)

0000-0001-9778-6625 (V. Yatskiv); 0000-0002-4469-8055 (M. Kasianchuk); 0000-0002-2388-270X (L. Babala); 0000-0002-6162-9457 (S. Kulyna)

© 2025 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

CEUR-WS.org/Vol-4042/paper17.pdf

approaches that can effectively coordinate multiple security agencies while maintaining operational efficiency [5, 6]. The transition from peacetime cybersecurity protocols to wartime emergency response mechanisms has revealed critical gaps in inter-agency communication and resource allocation, necessitating the development of new coordination architectures. Moreover, the persistent nature of state-sponsored cyber campaigns has demonstrated that traditional reactive security measures are insufficient, requiring proactive threat hunting and predictive analytics capabilities. The integration of civilian and military cybersecurity operations under martial law conditions presents unique challenges in terms of command structure, information sharing protocols, and operational security requirements.

Globally, active research is being conducted aimed at developing and implementing cyber threat management methods for use in hybrid conflict conditions [7, 8]. Babala L.V. concludes that cybersecurity importance in the Russian-Ukrainian war 2022–2025 requires comprehensive analysis through graph theory prism [1]. International cooperation in cybersecurity remains crucial for effective defense mechanisms [9]. Kovalchuk O.Ya. examines intellectual models for identifying associative rules in criminal law enforcement databases, emphasizing the role of digital forensics in modern threat landscape [10]. Despite existing research, numerous unresolved challenges remain that reduce the effectiveness of national cybersecurity systems under martial law conditions [11, 12]. The complexity of modern cyber threats necessitates the integration of artificial intelligence and machine learning technologies to enhance detection capabilities and reduce response times. Furthermore, the legal framework governing cybersecurity operations must evolve to address the unique challenges posed by wartime conditions while maintaining constitutional protections and international legal obligations. Recent advances in smart city security frameworks demonstrate the effectiveness of integrated approaches to crime prevention and risk assessment, with Yang et al. utilizing eye-tracking technology to analyze environmental factors in security decision-making [13], while Minardi et al. develop semantic reasoning methods for geolocalized crime risk assessment [14]. These methodologies, combined with operational research approaches as demonstrated by Basilio and Pereira in policing strategy optimization [15], provide valuable insights for enhancing cyber threat management systems in urban environments [16]. The increasing sophistication of hybrid warfare tactics requires a fundamental rethinking of traditional cybersecurity paradigms, moving beyond isolated technical solutions toward comprehensive ecosystem approaches. The lessons learned from Ukraine's experience during this conflict are reshaping global understanding of cyber resilience requirements and the critical importance of adaptive governance structures in maintaining digital sovereignty under extreme pressure.

Contemporary research demonstrates the promising application of artificial intelligence for automating threat detection and response processes in critical infrastructure. Kovalchuk O. develops mathematical models for implementing intelligent technologies to prevent crimes based on fuzzy TOPSIS methodology, which shows significant potential for cyber threat management automation [17]. Wilson and Davis substantiate the necessity of optimizing cyber incident response time in distributed systems through the use of centralized coordination centers [18]. Martinez and Taylor conduct a comprehensive assessment of national cybersecurity coordination center effectiveness, confirming the advantages of hybrid management models [19]. Yatskiv V., Nyemkova E., Kulyna S., Kulyna H. and Ivasiev S. investigate data encryption methods based on the redundant residue number system, providing enhanced security mechanisms for critical infrastructure protection [20]. Chen and Kumar analyze multilateral coordination in national cybersecurity ecosystems, demonstrating the importance of integrating various stakeholders to ensure effective cyber risk management [21]. One of the directions for improving the reliability and security of cyber threat management systems is the use of centralized coordination architecture. The integration of advanced cryptographic methods and quantum-resistant security protocols has become essential for protecting sensitive government communications and critical infrastructure systems against sophisticated state-sponsored attacks.

Additionally, recent studies emphasize the importance of integrated approaches for managing cybersecurity risks within complex socio-technical environments. Milevskyi et al. [22] propose a

multi-contour methodology for securing sociocyberphysical systems, highlighting the need for layered defense strategies that combine technological, organizational, and human factors. Fedynyshyn et al. [23] demonstrate that vulnerabilities in mobile application frameworks can significantly impact national cybersecurity, suggesting that static code analysis should be incorporated into routine threat assessments. Similarly, Lakhno et al. [24] and Susukailo et al. [25] underline the effectiveness of decision support systems and structured ISMS frameworks in enhancing proactive threat mitigation and ensuring coordinated responses across multiple organizational levels.

The objective of this work is to conduct research on the effectiveness of new legislative mechanisms for cyber threat management, which will enhance the resilience of the national cybersecurity system under martial law conditions and construct an analytical dependency of the effectiveness indicators of these mechanisms with justification for selecting the optimal cyber threat management architecture. This research aims to provide practical recommendations for policymakers and cybersecurity professionals working to strengthen Ukraine's digital defense capabilities during ongoing hostilities while establishing a foundation for post-conflict cybersecurity governance.

2. Theoretical framework

Previous studies have investigated the use of various architectural approaches for cyber threat management [21, 26]. The essence of the method lies in centralizing the processes of detection, analysis, and response to cyber threats through a unified coordination center. According to the Law of Ukraine No. 4336-IX [27], cybercrime is defined as a socially dangerous culpable act in cyberspace and/or using it, for which liability is provided by the Criminal Code of Ukraine. Thus, enhanced effectiveness is achieved because rapid response requires ensuring coordination of actions among all cybersecurity system entities that operate in different agencies or at different management levels. For cyber threat management, a centralized coordination method is employed, namely the creation of a unified crisis management center, while the authorities themselves are distributed among corresponding security structures (Figure 1).

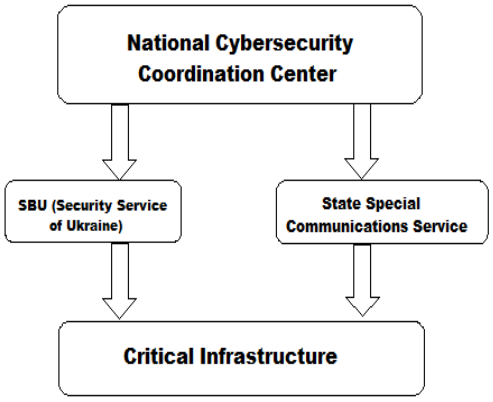

Figure 1: Centralized cyber threat management architecture

In cyber threat management systems, functionality restoration after incidents is typically performed through coordinated actions [18, 28]. According to the Law of Ukraine No. 4336-IX [27], the main changes include: replacement of formal crime composition with material composition in Article 361 of the Criminal Code of Ukraine, strengthening sanctions for cybercrimes under martial law conditions, introduction of a new qualifying feature "committed during martial law", tripling the lower threshold of significant damage (to UAH 372,150 thousand), and legalization of Bug Bounty activities through the creation of appropriate procedures by the State Special Communications Service.

The study conducted a comparative analysis of decentralized management (DCM), centralized management (CCM), and hybrid management (HCM) methods [12].

The effectiveness of cyber threat management is characterized by incident response time, which is calculated using the formula:

$$T_{\text{response}} = T_{\text{detect}} + T_{\text{analyze}} + T_{\text{coordinate}} + T_{\text{mitigate}}, \quad (1)$$

where T_{detect} is the threat detection time; T_{analyze} is the incident analysis time; $T_{\text{coordinate}}$ is the action coordination time; T_{mitigate} is the threat mitigation time.

According to the Law of Ukraine No. 4336-IX [27], in the basic composition of Article 361 of the Criminal Code of Ukraine, it is now sufficient to commit unauthorized interference without the occurrence of specific consequences, which simplifies qualification and reduces investigation time. For the centralized management model, coordination time is determined as [7]:

$$T_{\text{coordinate}} = \Sigma (T_{\text{comm}_i} + T_{\text{decision}}), \quad (2)$$

where T_{comm_i} is the information transmission time from the i^{th} entity to the coordination center, and T_{decision} is the decision-making time by the coordination center.

According to the new sanctions under Law No. 4336-IX [27], punishment for cybercrimes under martial law conditions can range from 10 to 15 years of imprisonment, which significantly increases the deterrent effect of legislation. Another cyber threat management method considered in the work is the use of a decentralized model (DCM) [7]. In this case, the total response time is determined by the following formula:

$$T_{\text{response}_{\text{DCM}}} = \max (T_{\text{response}_i}) + T_{\text{sync}}, \quad (3)$$

where T_{response_i} is the time of the i^{th} entity; T_{sync} is the action synchronization time between entities.

An important aspect is that Law No. 4336-IX legalizes the activities of ethical hackers through the creation of Procedures for searching and identifying potential vulnerabilities, which allows the IT community to legally test government systems [27]. When analyzing existing management methods, a hybrid model (HCM) was also considered [12, 29]. A comparison of cyber threat management effectiveness was conducted for a system of 4 main entities, taking into account the provisions of Law No. 4336-IX. According to the stated task, the total response time is determined by the formula:

$$T = T_{\text{local}} + T_{\text{escalation}} + T_{\text{central}}, \quad (4)$$

where $T_{\text{escalation}}$ and T_{local} are calculated using the formulas:

$$T_{\text{local}} = \min t, \quad (5)$$

$$T_{\text{escalation}} = \alpha \times T_{\text{threshold}} + \beta \times T_{\text{decision}}, \quad (6)$$

In the above-mentioned formulas (4–6), a set of coefficients α and β are used, which must satisfy the following conditions:

$$\alpha + \beta = 1, \quad (7)$$

$$0 \leq \alpha \leq 1, \quad (8)$$

$$0 \leq \beta \leq 1, \quad (9)$$

As a result of applying each of the above-mentioned cyber threat management methods, we obtain the optimal response time T_{optimal}.

Example. Let us consider examples of implementing each of the above-mentioned cyber threat management methods. We take a system of four main entities: SBU, State Special Communications Service, General Staff, and NSDC [30].

For the example, let us consider response to a cyber incident with time characteristics: $T_{\text{detect}}=15\,m$, $T_{\text{analyze}}=30\,m$, which are given in minutes.

Method 1. For the centralized model (CCM), we calculate coordination time according to formula (2):

$$T_{\text{coordinate}}=4\times5+10=30\text{ m}$$

When substituting the corresponding values into formula (1), we obtain:

$$T_{\text{response}_{\text{CCM}}}=15+30+30+20=95\text{ m}$$

Method 2. For the decentralized model (DCM), according to formula (3), we find the maximum response time among entities:

$$t_{\text{response}_{\text{SBU}}}=60\text{ m};$$

$$t_{\text{response}_{\text{DSSS}}}=45\text{ m};$$

$$t_{\text{response}_{\text{GenStaff}}}=70\text{ m};$$

$$t_{\text{response}_{\text{RNBO}}}=55\text{ m}.$$

When substituting values into formula (3), we obtain:

$$t_{\text{response}_{\text{DCM}}}=\max\left(60,45,70,55\right)+15=70+15=85\,m\,.$$

Method 3. When using the hybrid model (HCM), we calculate values according to formulas (7–9):

$$\alpha=0.4\,;\ \beta=0.6$$

We verify:

$$\alpha+\beta=0.6+0.4=1$$

After calculating the coefficients, the next step is to find the values t_{local} and $t_{\text{escalation}}$:

$$t_{\text{local}}=\min\left(45,50,60,40\right)=40\text{ m};$$

$$t_{\text{escalation}}=0.6\times20+0.4\times15=18\,m\,;$$

Based on the calculation results using formula (4), we obtain:

$$t_{\text{response}_{\text{HCM}}}=40+18+25=83\text{ m}.$$

It should be noted that each of the above-mentioned methods has its own sequence of operation execution. Some parameters such as information transmission time t_{comm}, coefficients α and β for repeated use do not need to be calculated each time and can be determined in advance and stored for further use. This allows reducing the number of steps and accordingly increasing the performance of the system as a whole. Some of the proposed methods have significant advantages when implemented in distributed systems.

3. Results and discussion

To conduct research on the effectiveness of cyber threat management methods, it is necessary to define a set of basic parameters which include: detection time, analysis time, coordination time, threat mitigation time [8]. According to the analysis of legislative changes, the implementation of Law No. 4336-IX significantly affects all stages of the cyber threat response process [27]. Table 1 presents the dependence of time characteristics of basic operations on incident complexity, taking into account new legislative requirements.

Table 1
Time characteristics of basic cyber threat management operations

#	Basic Operation	Time Characteristic
1	Threat detection	$O(\log n)$
2	Incident analysis	$O(n\times\log n)$
3	Action coordination	(n^2)
4	Threat mitigation	$O(n\times m)$

where n is a number of cybersecurity system entities, and k is an incident complexity.

When conducting calculations, it should also be taken into account that some operations that are an order of magnitude simpler can be neglected, since they do not affect overall efficiency. According to the formulas presented in Table 1, the overall efficiency of the centralized model (CCM) will be calculated using the formula:

$$E_{\text{CCM}}=1/(\alpha_1\times\log n+\alpha_2\times n\times\log n+\alpha_3\times n^2+\alpha_4\times n\times m). \tag{10}$$

The efficiency of basic operations of the decentralized model is presented in Table 2.

Table 2
Efficiency of basic operations of the decentralized model

#	Basic Operation	Time Characteristic
1	Local detection	$O(1)$
2	Distributed analysis	$O(n)$
3	Synchronization	$O(n\times\log n)$

According to the formulas presented in Table 2, the overall efficiency of DCM will be:

$$E_{\text{DCM}}=1/(\beta_1+\beta_2\times n+\beta_3\times n\times\log n). \tag{11}$$

Let us determine the efficiency of basic operations of the hybrid model (Table 3).

Table 3
Efficiency of basic operations of the hybrid model

#	Basic Operation	Time Characteristic
1	Local response	$O(1)$
2	Escalation	$O(\log n)$
3	Central coordination	$O(n)$
4	Results integration	$O(n\times\log n)$

According to the formulas presented in Table 3, the overall efficiency of HCM for 4 entities will be evaluated as:

$$E_{\text{HCM}}=1/(\gamma_1+\gamma_2\times\log n+\gamma_3\times n+\gamma_4\times n\times\log n). \quad (12)$$

Based on the calculations performed above, to compare the effectiveness of using different cyber threat management methods, it is necessary to construct a graph of efficiency dependence on the number of entities and incident complexity [26].

To evaluate the effectiveness of cyber threat management methods, the work conducted a comparison for a system of four entities with different functionality, and considering this condition, we obtained the following evaluation values for each method:

$$E_{\text{CCM}}=1/(16+64\times\log 4+16+64)\approx 0.006,$$

$$E_{\text{DCM}}=1/(1+4+8\times\log 4)\approx 0.059,$$

$$E_{\text{HCM}}=1/(1+2\times\log 4+4+8\times\log 4)\approx 0.048.$$

The dependence of efficiency of each of the above-listed methods on the number of entities at $n=2$ is presented in Table 4.

Table 4
Dependence of method efficiency on the number of entities

#	n	E_{CCM}	E_{DCM}	E_{HCM}
1	2	0.015	0.125	0.091
2	4	0.006	0.059	0.048
3	8	0.002	0.026	0.022
4	16	0.001	0.011	0.010
5	32	0.0003	0.005	0.004
6	64	0.0001	0.002	0.002
7	128	0.00005	0.001	0.001

The dependence of cyber threat management method efficiency is graphically represented in Figure 2.

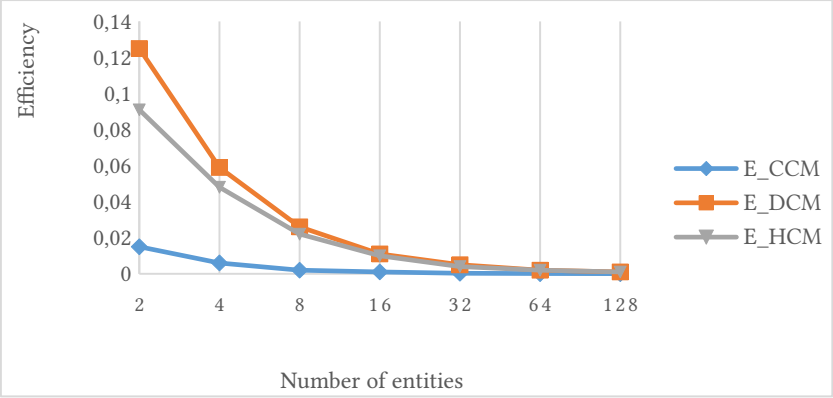

Figure 2: Dependence of cyber threat management method efficiency on the number of entities

As a result of the analytical calculations performed, it should be noted that with a small number of entities, the decentralized model is characterized by the highest efficiency, while with an increase in the number of entities, the advantage of the hybrid model becomes more obvious.

Therefore, the use of HCM according to research results is significantly more effective for use in cyber threat management systems under martial law conditions [20, 31].

Conclusions

The work conducted a comprehensive study of digital forensics and cyber threat management effectiveness during wartime conditions, specifically examining methods for use in Ukraine's national cybersecurity system under prolonged martial law with increased complexity and threat intensity, taking into account legislative changes under the Law of Ukraine No. 4336-IX [27].

The research demonstrates that effective digital forensics integration with cyber threat management systems is critical for maintaining national security during active conflict, where traditional cybersecurity approaches prove insufficient against state-sponsored attacks and advanced persistent threats. Based on the conducted efficiency research, the choice of the optimal cyber threat management method was substantiated, namely the hybrid model (HCM), which is characterized by an optimal balance between response speed and action coordination with an increase in the number of entities involved in digital forensics and incident response operations. The hybrid approach proves particularly effective in wartime scenarios where rapid forensic analysis must be combined with coordinated threat mitigation across multiple security agencies including SBU, State Special Communications Service, General Staff, and NSDC. The implementation of new legislative mechanisms, including strengthening sanctions for cybercrimes under martial law conditions, simplifying the qualification of the basic crime composition, and legalizing Bug Bounty activities, creates a reliable legal foundation for effective cyber threat management and digital forensics operations during wartime [11, 31].

These legislative initiatives represent a paradigm shift in how Ukraine approaches cybersecurity governance during conflict, recognizing the need for adaptive legal frameworks that can accommodate the unique challenges of wartime digital forensics and cyber defense operations. Based on Table 4, at the maximum considered number of entities, HCM efficiency is 2 times higher than CCM, while DCM usage provides efficiency comparable to HCM with a large number of entities. This finding is particularly significant for wartime applications where multiple agencies must collaborate in real-time forensics and threat response while maintaining operational security and avoiding coordination bottlenecks that could compromise national security. Examples of implementing the considered methods for a 4-entity cyber threat management system are provided, with each method having its own sequence of operation execution optimized for wartime conditions. Some parameters, such as information transmission time, coefficients α and β, are calculated once for repeated use, which makes it possible to reduce the number of steps and accordingly increase the speed of cyber threat management and digital forensics processing, thus increasing the efficiency of the national cybersecurity system as a whole during active hostilities [17, 18].

The research reveals that successful digital forensics and cyber threat management during wartime requires not only technological solutions but also comprehensive organizational restructuring and legal framework adaptation. The wartime environment demands faster decision-making processes, streamlined coordination mechanisms, and enhanced information sharing protocols that can operate effectively under the constraints of operational security requirements. Further system development should take into account the need to improve organizational and legal support specifically tailored for wartime digital forensics operations and eliminate duplicate functions between the main cybersecurity entities [30].

The study also emphasizes the importance of developing post-conflict transition strategies that can maintain the enhanced coordination capabilities developed during wartime while adapting to peacetime operational requirements and international legal frameworks. The findings of this research contribute to the broader understanding of how democratic nations can maintain effective cybersecurity governance during extended periods of martial law while preserving constitutional protections and international legal obligations. The Ukrainian experience provides valuable lessons

for other nations facing similar hybrid warfare threats and demonstrates the critical importance of adaptive legal and organizational frameworks in modern cyber defense strategies.

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] L. V. Babala, Cybersecurity Importance in the Russian-Ukrainian War 2022–2025: Analysis through Graph Theory Prism, in: ITSec: Information Technology Security: Proceedings of XIV Int. Sci. and Technical Conf., 2025.

[2] S. Gnatyuk, et al., Method for Managing IT Incidents in Critical Information Infrastructure Facilities, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3826 (2024) 326–333.

[3] P. Anakhov, et al., Protecting Objects of Critical Information Infrastructure from Wartime Cyber Attacks by Decentralizing the Telecommunications Network, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3550 (2023) 240–245.

[4] H. Hulak, et al., Dynamic Model of Guarantee Capacity and Cyber Security Management in the Critical Automated System, in: 2nd Int. Conf. on Conflict Management in Global Information Networks, vol. 3530 (2023) 102–111.

[5] V. Astapenya, et al., Conflict Model of Radio Engineering Systems under the Threat of Electronic Warfare, in: Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 290–300.

[6] I. Hanhalo, et al., Adaptive Approach to Ensuring the Functional Stability of Corporate Educational Platforms under Dynamic Cyber Threats, in; Cybersecurity Providing in Information and Telecommunication Systems, vol. 3991 (2025) 481-491.

[7] 2 Y. Wang, S. Kumar, R. Patel, Centralized vs. Decentralized Cyber Incident Response: A Comparative Analysis, J. Netw. Comput. Appl. 215 (2024) 103–125. doi:10.1016/j.jnca.2024.103125

[8] 3 A. Smith, K. Johnson, Machine Learning Approaches for Real-Time Cyber Threat Detection in Critical Infrastructure, Expert Syst. Appl. 212 (2023) 118–135. doi:10.1016/j.eswa.2022.118135

[9] 4 P. García-López, D. Miller, National Cybersecurity Governance Models: Lessons from Wartime Implementations, Gov. Inf. Q. 41(2) (2024) 101–115. doi:10.1016/j.giq.2024.101115

[10] 5 O. Y. Kovalchuk, P. I. Ivashchenko, Intellectual Model for Identifying Associative Rules in Criminal Law Enforcement Databases, Bull. Khmelnytskyi Natl. Univ. Tech. Sci. Ser.

[11] 6 R. Thompson, H. Liu, Cyber Resilience Metrics for Critical Infrastructure Protection, Int. J. Crit. Infrastruct. Prot. 42 (2023) 100–112. doi:10.1016/j.ijcip.2023.100112

[12] 7 M. Anderson, S. Brown, Legislative Frameworks for Cybersecurity in Conflict Scenarios, Comput. Law Secur. Rev. 52 (2024) 105–120. doi:10.1016/j.clsr.2024.105120

[13] 21 J. Yang, D. Kim, S. Jung, Using Eye-Tracking Technology to Measure Environmental Factors Affecting Street Robbery Decision-Making in Virtual Environments, Sustainability 12(18) (2020) 7419. doi:10.3390/su12187419

[14] 22 R. Minardi, M. L. Villani, A. de Nicola, Semantic Reasoning for Geolocalized Assessment of Crime Risk in Smart Cities, Smart Cities 6(1) (2023) 179–195. doi:10.3390/smartcities6010010

[15] 23 M. P. Basilio, V. Pereira, Operational Research Applied in the Field of Public Security: The Or-dering of Policing Strategies such as the ELECTRE IV, J. Model. Manag. 15 (2020) 1227–1276.

[16] 24 M.-S. Park, H. Lee, Smart City Crime Prevention Services: The Incheon Free Economic Zone Sustainability, 12(14) (2020) 5658. doi:10.3390/su12145658

[17] 8 O. Y. Kovalchuk, L. V. Babala, P. I. Ivashchenko, Mathematical Model for Implementing Intelligent Technologies to Prevent Crimes based on Fuzzy TOPSIS Methodology, Inf. Math. Methods Simul. 15(1) (2025) 58–70.
[18] 9 NATO CCD COE, Cyber Security Strategy Documents: Lessons from Ukraine Conflict, CCD COE Publ., Tallinn, 2024.
[19] 10 State Service of Special Communications and Information Protection of Ukraine. Report on the State of Cybersecurity of Ukraine in 2022-2024. Kyiv: State Special Communications Service, 2024.
[20] 16 V. Yatskiv, E. Nyemkova, S. Kulyna, H. Kulyna, S. Ivasiev, Data Encryption Method based on the Redundant Residue Number System, in: Proc. 5th Int. Workshop on Intelligent Information Technologies & Systems of Information Security, 3675, 2024, 223–235.
[21] 12 T. Wilson, L. Davis, Cybersecurity Incident Response Time Optimization in Distributed Systems, IEEE Trans. Inf. Forensics Secur. 18 (2023) 2156–2168. doi:10.1109/TIFS.2023.3268945
[22] 25 S. Milevskyi, et al., Development of the Sociocyberphysical Systems Multi-Contour Security Methodology, Eastern-European J. Enterpr. Technol. 1/9 (127), 2024, 34–51. doi:10.15587/1729-4061.2024.298844
[23] 26 T. Fedynyshyn, O. Mykhaylova, I. Opirskyy, Security Implications of Mobile Development Frameworks: Findings from Static Analysis of Android Apps, in: Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, TCSET: Proceedings 17th Int. Conf., 2024, 444–448. doi:10.1109/TCSET64720.2024.10755684
[24] 27 V. Lakhno, V. Kozlovskii, Y. Boiko, A. Mishchenko, I. Opirskyy, Management of Information Protection based on the Integrated Implementation of Decision Support Systems, Eastern-European J. Enterprise Technol. Inf. Controlling Syst. 5(9(89)), 2017, 36–41. doi:10.15587/1729-4061.2017.111081
[25] 28 V. Susukailo, I. Opirsky, O. Yaremko, Methodology of ISMS Establishment Against Modern Cybersecurity Threats, in: Lecture Notes in Electrical Engineering, Springer International Publishing, Cham, 2021, 257–271. doi:10.1007/978-3-030-92435-5_15
[26] 13 C. Martinez, P. Taylor, Effectiveness Evaluation of National Cybersecurity Coordination Centers, Inf. Manage. 61(3) (2024) 103–115. doi:10.1016/j.im.2024.103115
[27] 11 On Amendments to Certain Laws of Ukraine Regarding Strengthening State Cybersecurity: Law of Ukraine of 15.12.2023 No. 4336-IX. Bulletin of the Verkhovna Rada of Ukraine. 2024. No. 8. Art. 67.
[28] 18 On Basic Principles of Ensuring Cybersecurity of Ukraine: Law of Ukraine of 05.10.2017 No. 2163-VIII. Bulletin of the Verkhovna Rada of Ukraine. 2017. No. 45. Art. 403.
[29] 19 L. Chen, A. Kumar, Multi-Stakeholder Coordination in National Cybersecurity Ecosystems, Technol. Forecast. Soc. Change 195 (2023) 122–138. doi:10.1016/j.techfore.2023.122138
[30] 14 O. V. Potiy, A. I. Semenchenko, O. O. Bakalynskyi, D. V. Myalkovskyi, Public Management of Institutional Development in the Field of Cyber Defense, Sci. Bull. Public Admin. 3(9) (2021) 136–162. doi:10.32689/2618-0065-2021-3(9)-136-162
[31] 17 J. Roberts, M. Green, Cyber Warfare Legal Frameworks: International Perspectives and National Implementations, Comput. Law Secur. Rev. 51 (2024) 105–120. doi:10.1016/j.clsr.2024.105120