VARSTVOSLOVJE
Journal of Criminal Justice and Security
year 2024
volume 26
pp. 1–13

Relationship Between Threat Modelling, Cyber Threat Intelligence, and Cyber Resilience: a Systematic Literature Review

Luka Podlesnik, Anže Mihelič

Purpose:

This research aims to examine the relationship between threat modelling, cyber threat intelligence (CTI), and cyber resilience conceptualized in the recent literature. Current literature reviews focus mainly on each domain and do not examine their relationship.

Design/Methods/Approach:

We conducted a systematic literature review of academic journals and conference papers published after 2018. We queried three databases: IEEE Xplore, Scopus, and Web of Science, and used data synthesis to extrapolate key insights.

Findings:

Our research indicates that both threat modelling and cyber threat intelligence can contribute to enhancing cyber resilience. Some indications suggest that integrating cyber threat intelligence and threat modelling might have synergistic benefits for strengthening cyber resilience, but more research is needed to explore the potential synergies between them. We propose a conceptual model where threat modelling and cyber threat intelligence work together in a complementary manner to strengthen cyber resilience. Threat intelligence provides the latest threat context to inform threat modelling. In contrast, threat modelling provides a structured approach for prioritizing and addressing the most critical threats identified through cyber threat intelligence.

Research Limitations/Implications:

This article focuses only on threat modelling and cyber threat intelligence in relation to cyber resilience. The research was limited to academic journals and conference papers published after 2018.

Value:

The findings of the article offer insight into how recent research addresses the relations between threat modelling and cyber threat intelligence in the

context of cyber resilience, and the conceptual model is proposed where threat modelling and cyber threat intelligence work together in a complementary manner to strengthen cyber resilience.

Keywords: threat modelling, cyber threat intelligence, cyber resilience, cyber security

UDC: 004.056.53

Razmerje med modeliranjem groženj, obveščanjem o kibernetskih grožnjah in kibernetsko odpornostjo: sistematični pregled literature

Namen:

Namen članka je raziskati, kako literatura obravnava odnose med modeliranjem groženj, obveščanjem o kibernetskih grožnjah in kibernetsko odpornostjo. Trenutni pregledi literature se nanašajo predvsem na vsak koncept posebej in se ne osredotočajo na odnose med njimi.

Metode:

Opravili smo sistematični pregled literature, objavljene po letu 2018. Poizvedba je bila opravljena po treh podatkovnih bazah: IEEE Xplore, Scopus in Web of Science. Za izdelavo predloga rešitev je bila uporabljena metoda sinteze.

Ugotovitve:

Rezultati raziskave kažejo, da imata tako modeliranje groženj kot obveščanje o kibernetskih grožnjah pozitiven doprinos k izboljšanju kibernetske varnosti. Nekatere indikacije kažejo, da bi lahko integracija obveščanja o kibernetskih grožnjah in modeliranja groženj imela sinergijske koristi za krepitev kibernetske odpornosti.

Kot rešitev predlagamo idejni model, kjer se procesa modeliranja groženj in obveščanja o kibernetskih grožnjah medsebojno dopolnjujeta na osnovi povratnih informacij, ki nastanejo kot rezultat sprememb v modelu groženj, ali novih informacij o potencialnih kibernetskih grožnjah.

Omejitve:

Članek se osredotoča samo na odnose med modeliranjem groženj, obveščanjem o kibernetskih grožnjah in kibernetsko odpornostjo ter njihovo obravnavo v novejši literaturi, objavljeni po letu 2018.

Izvirnost/pomembnost prispevka:

Ugotovitve članka ponujajo vpogled v to, kako nedavne raziskave obravnavajo odnose med modeliranjem groženj in obveščanjem o kibernetskih grožnjah v kontekstu kibernetske odpornosti. Predlagan je konceptualni model, ki temelji na sinergiji modeliranja groženj in obveščanja o kibernetskih grožnjah z namenom izboljšanja kibernetske varnosti.

Ključne besede: modeliranje groženj, obveščanje o kibernetskih grožnjah, kibernetska odpornost, kibernetska varnost

UDK: 004.056.53

1 INTRODUCTION

In today's cybersecurity landscape, organizations are increasingly confronted with sophisticated threats that pose a risk to their information systems. As cyber attacks grow more complex, traditional security measures often need to be revised to protect against these evolving threats (Appiah et al., 2022). This requires organizations to consider approaches like threat modelling and cyber threat intelligence (CTI) to improve their cybersecurity resilience (Ross et al., 2021).

Before delving deeper into the relationship between threat modelling, CTI, and cyber resilience, the meanings of those concepts, as defined in the literature, are presented in the following.

Threat modelling is a proactive approach to identifying and analyzing potential threats to a system and has been widely adopted across various domains (Shostack, 2014). It focuses on identifying and mitigating vulnerabilities before they can be exploited (Dhillon, 2011). Researchers define threat modelling as *"a systematic approach for characterizing potential threats to a system. It ensures completeness by including prioritizing threats and mitigation based on probabilities, business impacts, and cost of countermeasures"* (Nweke & Wolthusen, 2020). The existing literature has seen significant advancements in defining and developing viable threat modelling approaches based on their focus: asset-centric, attack-centric, software, and system-centric approaches (Bodeau et al., 2018; Nweke & Wolthusen, 2020). Using any of these threat modelling approaches, we can estimate risk by analyzing threats and accounting for the likelihood of occurrence and severity of impact (Bodeau et al., 2018).

CTI, on the other hand, provides information about potential threats and enables organizations to make informed cybersecurity decisions. It involves collecting, analyzing, and disseminating information about emerging cyber threats, allowing organizations to stay informed and responsive (Radoglou-Grammatikis et al., 2023). CTI leverages data for informed decision-making and refers to the collected information about potential and current cybersecurity threats and vulnerabilities. It is a proactive approach to cybersecurity that involves gathering data from various sources and consists of five main stages: planning and direction, collection, analysis, production and dissemination, and feedback (Radoglou-Grammatikis et al., 2023).

Cyber resilience is not solely about preventing or mitigating cyber attacks but also about maintaining critical functions and ensuring the ongoing operation of systems and services in the face of adversity. It refers to an organization's or system's ability to withstand, adapt to, and recover from disruptive cyber events (Ross et al., 2021). This requires shifting from a traditional approach, where systems are built to resist known threats, to a more adaptive and responsive model that can adapt to ever-changing threat landscapes (Kott & Linkov, 2019). It could

be defined as the system's ability to recover or regenerate its performance after a cyber attack degrades its performance (Kott & Linkov, 2019). Cyber resiliency aims to help organizations anticipate, withstand, and recover from cyber attacks (U.S. Department of Homeland Security, The Information Technology Sector Coordinating Council (IT SCC), The Information Technology Government Coordinating Council (IT GCC), 2017).

The three concepts of threat modelling, CTI, and cyber resilience may be intrinsically linked and can enhance the cyber security posture of organizations. Threat modelling helps organizations identify and mitigate vulnerabilities, while CTI provides the necessary information to understand and anticipate potential threats. Cyber resilience, in turn, enables organizations to anticipate, adapt, and respond to cyber incidents, ensuring the continuity of critical functions and services.

While there are existing literature reviews and surveys researching threat modelling (Bodeau et al., 2018; Erbas et al., 2024; Khalil et al., 2024; Nweke & Wolthusen, 2020), CTI (Bui et al., 2024; Chatziamanetoglou & Rantos, 2024; Radoglou-Grammatikis et al., 2023; Saeed et al., 2023; Sun et al., 2023), and cyber resilience (Araujo et al., 2024; Segovia-Ferreira et al., 2024; Sepúlveda Estay et al., 2020) individually or in a context of the applied domain, there is no literature review examining the interplay between threat modelling, CTI and cyber resilience. The complex and interrelated nature of these concepts requires a deeper understanding of their relationship and how they can be leveraged in a complementary manner to enhance an organization's overall cybersecurity posture.

This paper aims to review the existing literature to explore the relationship between threat modelling, CTI, and cyber resilience. By categorizing and synthesizing recent relevant research, we seek to answer the following research question:

RQ: How is the relationship between threat modelling, CTI, and cyber resilience conceptualized in the literature?

This will provide an understanding of the current state of the field and identify potential areas for future investigation.

The paper is structured as follows: it starts with Section 2, which presents the methods used; Section 3, which presents the results of the research; Section 4, which provides a discussion with theoretical and practical implications; and Section 5, which presents limitations and possible directions for future research.

2 METHODS

We conducted a systematic literature review to examine how the relationship between threat modelling, CTI, and cyber resilience is conceptualized in the literature. The review was conducted through a multi-stage process. Initially, we defined the field of interest and the research question, followed by the definition of the inclusion and exclusion criteria presented in Table 1. We reviewed academic journals and conference papers published after 2018. A visual representation of

the review process and the number of papers included at each step is presented in Figure 1.

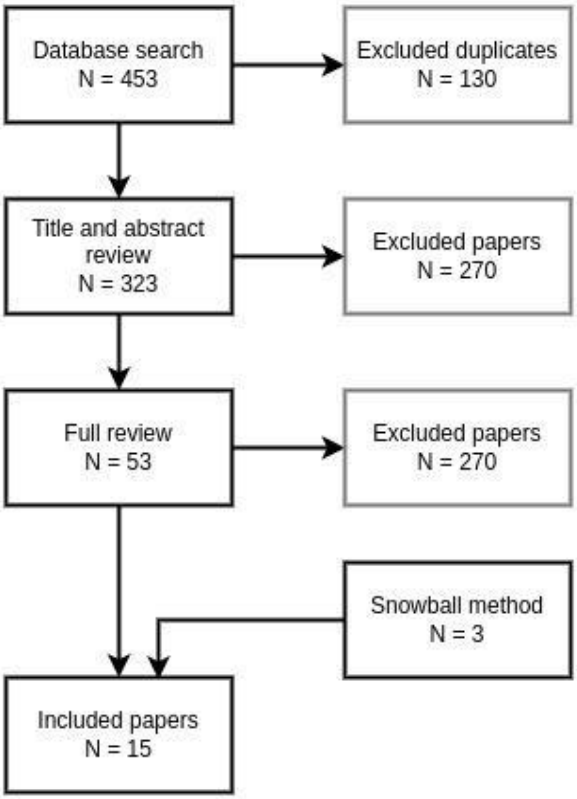

Figure 1: Systematic review process

Our literature survey was conducted on July 25, 2024. We queried three databases (IEEE Xplore, Scopus, and Web of Science) with the following query: *((“threat model*” **OR** “threat intelligence” **OR** “CTI”) **AND** cyber* **AND** resilien*)* and was adjusted to suit each database. The survey returned a total of $N = 453$ papers published after 2018. Distribution per database is displayed in Table 2. Afterward, we removed duplicates which resulted in a set of $N = 323$ unique papers. Next, we examined the titles and abstracts of the remaining papers, and the inclusion and exclusion criteria were applied, as presented in Table 1. All papers that meet the criteria and those where we could not determine if they meet the criteria were included in the full review resulting in $N = 53$. After the full paper review, $N = 13$ papers were included. By utilizing the snowball method + = 2 additional papers were included.

Table 1: Inclusion and exclusion criteria

Inclusion criteria	Exclusion criteria
The paper must be a journal article or conference proceeding	The paper is not in the English language
Published after 2018	The full paper is not available
It should focus on CTI or threat modelling in relation to cybersecurity resilience	The article focuses on CTI and/or threat modelling but not in relation to cyber resilience

Table 2: Data extraction per database

Database	*N*
IEEE Xplore	226
Scopus	103
Web of Science	124

3 RESULTS

The results of our literature review are presented in Table 3. Results are grouped based on whether they emphasize or utilize **CTI** or threat modelling (**TM**) methodology for improving cybersecurity resilience.

Answer to RQ: Findings indicate that the majority of the reviewed research 60% is utilizing a threat modelling approach to improve cyber resilience (Abdelgawad & Ray, 2024; Alhidaifi et al., 2024; Casola et al., 2024; Fowler & Sitnikova, 2019; Hacker et al., 2024; Larraz et al., 2023; Liu et al., 2024; Mulla et al., 2023; Strandberg et al., 2021). The second largest group, 27%, focuses on CTI (Fysarakis et al., 2023; Hytonen et al., 2023; van Haastrecht et al., 2021; Zighan, 2024). The last group is the smallest one, at 13%, using a hybrid approach by combining both methodologies (Gylling et al., 2021; Onwubiko, 2020).

Threat modelling can enhance cyber resilience, but not all threat modelling methodologies are suitable (Alhidaifi et al., 2024). In the threat modelling group, 33% of the reviewed papers utilize STRIDE threat modelling methodology (Casola et al., 2024; Hacker et al., 2024; Strandberg et al., 2021), while some of the others propose their custom threat modelling approaches catered towards more complex systems (Fowler & Sitnikova, 2019; Liu et al., 2024). Threat modelling can serve as a basis for assessing the cyber resilience of a system (Fowler & Sitnikova, 2019; Larraz et al., 2023) or can be used to develop domain-specific threat models that are further utilized to evaluate security risks and improve resilience (Liu et al., 2024; Mulla et al., 2023; Strandberg et al., 2021). Threat models can also be used to run attack simulations to help assess the cyber resilience of the system (Hacker et al., 2024).

Research suggests that sharing CTI among organizations can improve collective cybersecurity resilience (Fysarakis et al., 2023; van Haastrecht et al., 2021; Zighan, 2024), and resilience to cyber attacks can be increased by combining the principles of business continuity with cyber situational awareness created through CTI (Fysarakis et al., 2023; Hytonen et al., 2023).

Our literature review found two papers that combined threat modelling and CTI approaches. One presented a method that uses CTI data to build threat actor profiles and maps their properties to attack graphs generated by the SecuriCAD threat modelling tool to increase time to compromise (TTC), which was proposed as a resilience metric (Gylling et al., 2021). The other paper used threat modelling and CTI as part of a more comprehensive framework. They are both used to test if recovery controls are effective and that recovery capabilities are appropriate. Additional threat modelling is utilized for scenario-based cyber wargaming to assess and model recovery gaps and possible ways systems or services can be compromised (Onwubiko, 2020).

4 DISCUSSION

Our research suggests that threat modelling can be a powerful tool for identifying and assessing potential vulnerabilities, and it can enhance cyber resilience by enabling organizations to prioritize and address the most critical threats (Alhidaifi et al., 2024; Liu et al., 2024; Mulla et al., 2023; Strandberg et al., 2021), but it is the incorporation of CTI that elevates an organization's ability to anticipate current and emerging cyber threats (Fysarakis et al., 2023; Gylling et al., 2021; Zighan, 2024). CTI can provide the necessary context and insights to inform the threat modelling process, ensuring that the identified threats align with the organization's real-world challenges (Gylling et al., 2021). Furthermore, a comprehensive understanding of the threat landscape, facilitated by CTI, can inform the development of robust security controls and incident response plans, enhancing an organization's cyber resilience (Onwubiko, 2020; van Haastrecht et al., 2021).

Based on this data, we propose a conceptual model where threat modelling and CTI work together in a complementary manner to strengthen cyber resilience. Figure 2 - threat intelligence provides the latest threat context to inform threat modelling, while threat modelling provides a structured approach for prioritizing and addressing the most critical threats identified through CTI.

Systems are rarely static; they can change for various reasons, like changes in requirements, updates, changes in assets, and software development, so threat modelling should be done throughout the system lifecycle to reflect the changes. As the system changes, the threat models must be updated to reflect these changes and to model any new vulnerabilities and threats. These changes to the system can alter the attack surface, requiring updates to CTI collection and analysis, which is why the feedback loop from threat modelling to CTI is needed.

Additionally, CTI evolves as new threat actors emerge, new attacker tools and techniques are developed, and the overall threat landscape changes. Threat models must be updated to account for new information provided by CTI. This continuous feedback loop between threat modelling and CTI ensures that organizations can proactively adapt their cybersecurity posture to address the evolving threat landscape, ultimately enhancing their cyber resilience.

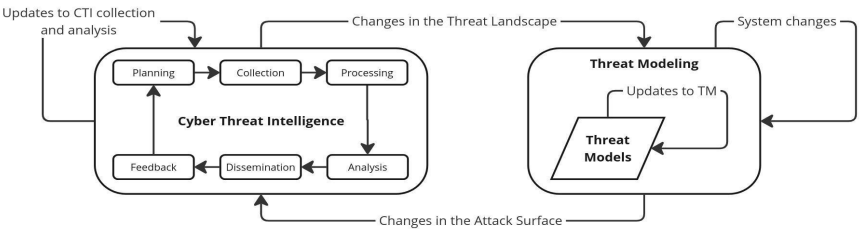

Figure 2: The proposed conceptual model

The relationship between CTI and threat modelling processes is depicted as a feedback loop consisting of changes in the attack surface and changes in the threat landscape. CTI informs the threat modelling process about evolving threats, while the threat modelling process provides information to the CTI process about changes in the attack surface. Both processes leverage the insights from this feedback loop to make necessary internal adjustments.

Organizations can develop a dynamic cybersecurity strategy by applying the proposed conceptual model. For instance, consider a financial institution that handles sensitive customer data and is frequently targeted by cybercriminals attempting to exploit system vulnerabilities. The CTI team continuously monitors the threat landscape, identifying emerging threats such as new phishing tactics or malware variants aimed at financial systems. This intelligence is then integrated into the threat modelling process, which updates the attack surface to reflect these evolving threats. As the attack surface changes, the threat modelling process identifies potential vulnerabilities within the organization's systems and prioritizes them based on the latest threat intelligence. This prioritized list of threats guides security measures, such as reinforcing authentication protocols or deploying advanced anti-phishing technologies. Meanwhile, the threat modelling process provides feedback to the CTI team about changes in the institution's attack surface, enabling them to refine their intelligence-gathering and analysis efforts. Through this continuous feedback loop, organizations can proactively address vulnerabilities, anticipate potential attacks, and enhance their overall cyber resilience, thereby reducing the likelihood of successful breaches and minimizing the impact of any incidents that do occur.

In summary, the intersection between threat modelling and CTI can present a powerful synergistic approach to enhancing cyber resilience. Threat modelling provides the framework for identifying and prioritizing threats, while CTI provides the context and insights needed to anticipate and address emerging threats. The integration of these two disciplines, in turn, strengthens an organization's cyber resilience, enabling it to withstand, adapt, and recover from cyber incidents more effectively.

5 LIMITATIONS AND FUTURE WORK

This research was limited to papers published after 2018. In future research, the time frame should be expanded to include a broader range of publications to gain a more thorough and longitudinal understanding of the evolution and application of CTI and threat modelling in the context of cyber resilience. The search strategy

could include more scientific databases, ensuring a more comprehensive coverage of the available literature. The review focused on the general principles and theoretical frameworks of CTI, threat modelling, and cyber resilience, but it didn't explore the specific methodologies, tools, and techniques used in these approaches in depth.

Future research could examine these practical aspects more thoroughly to provide guidance and recommendations to help organizations implement these approaches in their systems to enhance their cyber resilience. Additionally, future research could further explore integrating these approaches with other emerging technologies and methodologies, such as machine learning, artificial intelligence, and blockchain, to enhance the cyber resilience of complex cyber-physical systems.

Table 3: Literature review

Source	Approach	Short description
(Strandberg et al., 2021)	**TM**	The paper presents the Resilient Shield framework, which defines essential security and resilience mechanisms for modern vehicles. The framework employs STRIDE threat modelling methodology.
(Abdelgawad & Ray, 2024)	**TM**	This paper introduces a methodology for conducting mission resiliency analysis for mission-critical systems. The methodology consists of seven steps one of which is the construction of threat models is one of them.
(Mulla et al., 2023)	**TM**	The paper emphasizes the importance of UAV threat modelling for identifying, assessing, and prioritizing the risks and vulnerabilities specific to UAV systems.
(Fowler & Sitnikova, 2019)	**TM**	The paper presents a framework that leverages threat modelling as the basis for assessing the cyber-worthiness of complex cyber-physical systems.
(Liu et al., 2024)	**TM**	This paper provides a survey of the cyber resilience enhancement process in DER-based smart grids, focusing on threat modelling, risk assessment, and defense strategies.
(Larraz et al., 2023)	**TM**	The paper introduces Cyber-Resiliency Verifier (CRV), an automated tool for analyzing the resiliency of a system design against one or more threat models.
(Hacker et al., 2024)	**TM**	The research paper presents an advanced co-simulation environment developed to assess the cyber resilience of active distribution grids. The approach utilizes threat modelling as a tool for conducting threat analysis.
(Casola et al., 2024)	**TM**	The paper introduces a model-based methodology to enhance CPS security and resilience through threat modelling, security control identification, and MTD strategy integration.
(Alhidaifi et al., 2024)	**TM**	The paper provides a review of various domains of cyber resilience. It evaluates the threat modelling methodology and assesses the suitability of different threat modelling frameworks for cyber resilience

(Zighan, 2024)	**CTI**	The paper suggests a "sense, resist, and react" paradigm for a digital resilience framework, with cyber threat intelligence as part of the "sense" component.
(van Haastrecht et al., 2021)	**CTI**	The paper proposes a solution for SMEs that utilizes data from shared CTI platforms to automatically prioritize threats and provide actionable recommendations for addressing them.
(Hytonen et al., 2023)	**CTI**	This case study explores how combining CTI and Business Continuity Management can enhance an organization's foresight and resilience against cyber attacks.
(Fysarakis et al., 2023)	**CTI**	The paper presents the PHOENI2X project and underlying Cyber Resilience Framework (CRF) that aims to provide AI-assisted orchestration, automation & response capabilities for business continuity and recovery, incident response, and information exchange, tailored to the needs of OES and of the EU Member State (MS) National Authorities entrusted with cyber-security.
(Gylling et al., 2021)	**TM, CTI**	The paper presents a method to map CTI data to attack graphs generated by the securiCAD threat modelling tool.
(Onwubiko, 2020)	**TM, CTI**	The paper presents an adaptive cyber recovery operational framework comprising eight core components, with CTI and threat modelling as part of the testing component. Threat modelling is also used within the playbook component.

TM = threat modelling CTI = cyber threat intelligence

REFERENCES

Abdelgawad, M., & Ray, I. (2024). Methodology for resiliency analysis of mission-critical systems. In *Proceedings of the 39th ACM/SIGAPP Symposium on Applied Computing* (pp. 1292–1300). https://doi.org/10.1145/3605098.3636066

Alhidaifi, S. M., Asghar, M. R., & Ansari, I. S. (2024). A survey on cyber resilience: Key strategies, research challenges, and future directions. *ACM Computing Sureys*, *56*(8), 196. https://doi.org/10.1145/3649218

Appiah, G., Amankwah-Amoah, J., & Liu, Y.-L. (2022). Organizational architecture, resilience, and cyberattacks. *IEEE Transactions on Engineering Management, 69*(5), 2218–2233. https://doi.org/10.1109/TEM.2020.3004610

Araujo, M. S. de, Machado, B. A. S., & Passos, F. U. (2024). Resilience in the context of cyber security: A review of the fundamental concepts and relevance. *Applied Sciences*, *14*(5), 2116. https://doi.org/10.3390/app14052116

Bodeau, D., McCollum, C., & Fox, D. (2018). *Cyber threat modeling: Survey, assessment, and representative framework.* Homeland Security Systems Engineering and Development Institute. https://www.mitre.org/sites/default/files/2021-11/prs-18-1174-ngci-cyber-threat-modeling.pdf

Bui, H. T., Aboutorab, H., Mahboubi, A., Gao, Y., Sultan, N. H., Chauhan, A., Parvez, M. Z., Bewong, M., Islam, R., Islam, Z., Camtepe, S. A., Gauravaram,

P., Singh, D., Ali Babar, M., & Yan, S. (2024). Agriculture 4.0 and beyond: Evaluating cyber threat intelligence sources and techniques in smart farming ecosystems. *Computers & Security, 140,* 103754. https://doi.org/10.1016/j.cose.2024.103754

Casola, V., De Benedictis, A., Mazzocca, C., & Montanari, R. (2024). Designing secure and resilient cyber-physical systems: A model-based moving target defense approach. *IEEE Transactions on Emerging Topics in Computing, 12*(2), 631–642. https://doi.org/10.1109/TETC.2022.3197464

Chatziamanetoglou, D., & Rantos, K. (2024). Cyber threat intelligence on blockchain: A systematic literature review. *Computers, 13*(3), 60. https://doi.org/10.3390/computers13030060

Dhillon, D. (2011). Developer-driven threat modeling: Lessons learned in the trenches. *IEEE Security & Privacy, 9*(4), 41–47. https://doi.org/10.1109/MSP.2011.47

Erbas, M., Khalil, S. M., & Tsiopoulos, L. (2024). Systematic literature review of threat modeling and risk assessment in ship cybersecurity. *Ocean Engineering, 306,* 118059. https://doi.org/10.1016/j.oceaneng.2024.118059

Fowler, S., & Sitnikova, E. (2019). Toward a framework for assessing the cyber-worthiness of complex mission critical systems. In *2019 Military Communications and Information Systems Conference (MilCIS).* Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/MilCIS.2019.8930800

Fysarakis, K., Lekidis, A., Mavroeidis, V., Lampropoulos, K., Lyberopoulos, G., Vidal, I. G.-M., Terés i Casals, J. C., Luna, E. R., Moreno Sancho, A. A., Mavrelos, A., Tsantekidis, M., Pape, S., Chatzopoulou, A., Nanou, C., Drivas, G., Photiou, V., Spanoudakis, G., & Koufopavlou, O. (2023). PHOENI2X – A European cyber resilience framework with artificial-intelligence-assisted orchestration, automation & response capabilities for business continuity and recovery, incident response, and information exchange. In *2023 IEEE International Conference on Cyber Security and Resilience (CSR)* (pp. 538–545). https://doi.org/10.1109/CSR57506.2023.10224995

Gylling, A., Ekstedt, M., Afzal, Z., & Eliasson, P. (2021). Mapping cyber threat intelligence to probabilistic attack graphs. In *2021 IEEE International Conference on Cyber Security and Resilience (CSR)* (pp. 304–311). https://doi.org/10.1109/CSR51186.2021.9527970

Hacker, I., Lenzen, J., Schmidtke, F., van der Velde, D., & Ulbig, A. (2024). A co-simulation environment to evaluate cyber resilience in active distribution grids utilising behind-the-meter assets. *Electric Power Systems Research, 230,* 110254. https://doi.org/10.1016/j.epsr.2024.110254

Hytonen, E., Rajamaki, J., & Ruoslahti, H. (2023). Managing variable cyber environments with organizational foresight and resilience thinking. In R. L. Wilson, & M. B. Curran (Eds.), *Proceedings of the 18th International Conference on Cyber Warfare and Security ICCWS* (pp. 162–170). Acad Conferences. https://www-webofscience-com.ezproxy.lib.ukm.si/wos/woscc/full-record/WOS:001047434700020

Khalil, S. M., Bahsi, H., & Korõtko, T. (2024). Threat modeling of industrial control systems: A systematic literature review. *Computers & Security, 136,* 103543.

https://doi.org/10.1016/j.cose.2023.103543

Kott, A., & Linkov, I. (Eds.). (2019). *Cyber resilience of systems and networks*. Springer. https://doi.org/10.1007/978-3-319-77492-3

Larraz, D., Lorch, R., Yahyazadeh, M., Arif, M. F., Chowdhury, O., & Tinelli, C. (2023). CRV: Automated Cyber-Resiliency Reasoning for System Design Models. In A. Nadel, & K. Y. Rozier (Eds.), *Proceedings of the 23rd Conference on Formal Methods in Computer-Aided Design - FMCAD 2023* (pp. 209–220). TU Wien Academic Press. https://doi.org/10.34727/2023/isbn.978-3-85448-060-0_29

Liu, M., Teng, F., Zhang, Z., Ge, P., Sun, M., Deng, R., Cheng, P., & Chen, J. (2024). Enhancing cyber-resiliency of DER-based smart grid: A survey. *IEEE Transactions on Smart Grid, 15*(5), 4998-5030. https://doi.org/10.1109/TSG.2024.3373008

Mulla, Y. U., Chavekar, A., Mane, S., & Kazi, F. (2023). Threat modeling of cube orange based unmanned aerial vehicle system. In *2023 International Carnahan Conference on Security Technology (ICCST)*. https://doi.org/10.1109/ICCST59048.2023.10474259

Nweke, L. O., & Wolthusen, S. D. (2020). A review of asset-centric threat modelling approaches. *International Journal of Advanced Computer Science and Applications (IJACSA), 11*(2). https://doi.org/10.14569/IJACSA.2020.0110201

Onwubiko, C. (2020). Focusing on the recovery aspects of cyber resilience. In *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*. https://doi.org/10.1109/CyberSA49311.2020.9139685

Radoglou-Grammatikis, P., Kioseoglou, E., Asimopoulos, D., Siavvas, M., Nanos, I., Lagkas, T., Argyriou, V., Psannis, K. E., Goudos, S., & Sarigiannidis, P. (2023). Surveying cyber threat intelligence and collaboration: A concise analysis of current landscape and trends. In *2023 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)* (pp. 309–314). https://doi.org/10.1109/CloudCom59040.2023.00057

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021). *Developing cyber-resilient systems: A systems security engineering approach*. National Institute of Standards and Technology, U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-160v2r1

Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. *Sensors, 23*(16), 7273. https://doi.org/10.3390/s23167273

Segovia-Ferreira, M., Rubio-Hernan, J., Cavalli, A., & Garcia-Alfaro, J. (2024). A survey on cyber-resilience approaches for cyber-physical systems. *ACM Computing Surveys, 56*(8), 202. https://doi.org/10.1145/3652953

Sepúlveda Estay, D. A., Sahay, R., Barfod, M. B., & Jensen, C. D. (2020). A systematic review of cyber-resilience assessment frameworks. *Computers & Security, 97*, 101996. https://doi.org/10.1016/j.cose.2020.101996

Shostack, A. (2014). *Threat modeling: Designing for security*. Wiley.

Strandberg, K., Rosenstatter, T., Jolak, R., Nowdehi, N., & Olovsson, T. (2021). Resilient shield: Reinforcing the resilience of vehicles against security threats.

In *2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)*. https://doi.org/10.1109/VTC2021-Spring51267.2021.9449029

Sun, N., Ding, M., Jiang, J., Xu, W., Mo, X., Tai, Y., & Zhang, J. (2023). Cyber threat intelligence mining for proactive cybersecurity defense: A survey and new perspectives. *IEEE Communications Surveys & Tutorials, 25*(3), 1748–1774. https://doi.org/10.1109/COMST.2023.3273282

U.S. Department of Homeland Security, The Information Technology Sector Coordinating Council (IT SCC), The Information Technology Government Coordinating Council (IT GCC). (2017). *Cyber resilience white paper: An information technology sector perspective*. https://www.it-scc.org/uploads/4/7/2/3/47232717/it_sector_cyber_resilience_white_paper.pdf

van Haastrecht, M., Golpur, G., Tzismadia, G., Kab, R., Priboi, C., David, D., Răcătăian, A., Baumgartner, L., Fricker, S., Ruiz, J. F., Armas, E., Brinkhuis, M., & Spruit, M. (2021). A shared cyber threat intelligence solution for SMEs. *Electronics, 10*(23), 2913. https://doi.org/10.3390/electronics10232913

Zighan, S. (2024). Navigating the cyber landscape: A framework for transitioning from business continuity to digital resilience. In *2024 2nd International Conference on Cyber Resilience (ICCR)*. https://doi.org/10.1109/ICCR61006.2024.10532999

About the Authors

Anže Mihelič, Ph.D., Assistant Professor, Faculty of Criminal Justice and Security, University of Maribor, Slovenia. E-mail: anze.mihelic@um.si

Luka Podlesnik, B.Sc. E-mail: luka.podlesnik@gmail.com