


Connecting Critical Infrastructure Operators and Law Enforcement Agencies to Share Cyber Incident Information with Early Warning Systems

Harri Ruoslahti¹^a and Ilkka Tikanmäki^{1,2}^b

¹*ResLab, Laurea University of Applied Sciences, Vanha maantie 9, Espoo, Finland*

²*Department of Warfare, National Defence University, Helsinki, Finland*

Keywords: Early Warning System, Information Sharing, Law Enforcement, Critical Infrastructure.

Abstract: Cyber incidents and business interruptions rank as the foremost business risks. With Early Warning Systems (EWS), that work in parallel with other cyber mechanisms, organisations can independently manage cyber-sensitive intelligence-related data. This article provides a qualitative multi-case study analysis. The data consists of systematic reviews and cross-case conclusions of six (n = 6) case studies on information sharing. EWS is a valuable tool that can help critical infrastructure providers protect against cyberattacks. EWS can provide a platform for sharing information and resources. This can help improve situational awareness, enhance incident response, and facilitate collaboration. between critical infrastructure providers, as critical infrastructure operators and relevant Law Enforcement Agencies (LEA) can share information on cyber incidents and monitor cyber incident progress. EWS can be used to exchange cyber threat intelligence and information sharing can be facilitated with a common reference library where alerts can be shared as tickets. This would enable information exchange in both directions.

1 INTRODUCTION

Cyber Threat Intelligence (CTI) can be aided by an Early Warning System (EWS) to provide any type of organisation with an increased capability to share information needed to detect and respond to cyber incidents. An EWS is a security operation support tool that enables the coordination and sharing of cyber-incident information in near real-time. An EWS will help provide timely and accurate information to all involved parties.

The development of EWSs can be rooted in information sharing and trust models from within the cyber domain as well as models from other domains (Rajamäki & Katos, 2020).


This article provides a qualitative multi-case study analysis consisting of systematic reviews and cross-case conclusions of six (n = 6) case studies on information sharing among partners. This analysis provides a deeper understanding of how EWS can enable cyber incident information sharing across


organisational boundaries between critical infrastructure operators and Law Enforcement Agencies (LEA).

An EWS for cyber intelligence can serve as a security operations support tool in that it enables all network members to share information and coordinate their responses in near real-time (Rajamäki & Katos, 2020), e.g., connect critical infrastructure and service providers with law enforcement authorities (Almén et al., 2022).

With EWS stakeholders can retain their independent management of cyber-sensitive intelligence and related data management, while the EWS will work parallel with other cyber mechanisms (Rajamäki & Katos, 2020).

The ECHO project (European network of Cybersecurity centres and competence Hub for innovation and Operations) was one of four Pilot projects launched by the European Commission to establish and operate a Cybersecurity Competence Network focused on the ECHO Early Warning System (E-EWS) and ECHO Federated Cyber Range

^a <https://orcid.org/0000-0001-9726-7956>

^b <https://orcid.org/0000-0001-8950-5221>

(E-FCR) and related inter-sector prototypes (ECHO project, 2021).

The development of EWS can be traced to information sharing and trust models within the cyber domain (Rajamäki & Katos, 2020). Project ECHO conducted demonstration activities that highlighted e.g., the benefits of the features and capabilities of the E-EWS, and promoted the technology roadmaps for E-EWS, E-FCR, and inter-sector prototypes to show their value in multi-sector scenario requirements and demonstration cases (ECHO project, 2021).

This study's research question (RQ) is: How can an Early Warning System enable the sharing of cyber incident information between critical infrastructure operators and law enforcement agencies?

2 LITERATURE

According to the Allianz Risk Barometer 2023 cyber incidents and business interruptions rank as the foremost business risks (Allianz Global Corporate & Specialty SE, 2023). Today's critical infrastructure operators face critical incidents and cyber-attacks. Organisations need to reconsider their approaches to information-sharing-based resilience-building (Pöyhönen et al., 2020).

Organisations operating critical infrastructures or providing critical services for society are more and more dependent on complex and interlinked cyber systems and their interconnections (The International Chamber of Commerce, 2024).

2.1 Resilience

(Vos, 2017) defines resilience as the ability to adapt to a changing environment and mitigate emergency crises. Resilience can be demonstrated as flexibility, endurance, and an ability to recover from adverse events or to adapt to an after-crisis new normal (Cauffman, 2018). Crises are often caused by external risks, while the resilience of an organisation will also include many internal priorities, such as preventive behaviours, and preparing guidelines and procedures to when a response to a critical event may be needed (Linkov et al., 2014).

Four event management cycle phases (plan, absorb, recover, and learn/adapt) can be combined with the domains of physical, information, cognitive, and social can help understand resilience in the fields of Information Technology (IT) and systems sciences (Linkov et al., 2013).

“Resilient organizations or networks show organizational stability, agility, and a culture that

promotes situational awareness to detect and identify clues that may indicate the realization of risks for appropriate mitigation and reaction” (Hytönen et al., 2023, p. 163).

Examples of threats against critical infrastructures and vital societal services include e.g., the attacks that impaired the functionality of the English National Health Service (NHS) in 2017 (Ghafur et al., 2019), halted a hospital network in the Czech Republic in 2021 (Muthuppalaniappan & Stevenson, 2020), and stopped the movement of goods by a South African port and rail operator in 2021 (Fitch Solutions, 2021). Similarly, an attacker stole the records of thousands of patients from the Finnish private psychotherapy service provider Vastaamo from 2018 to 2020 and tried to use the stolen files to blackmail individual patients threatening to expose documents that contained their personal identity codes and therapy session transcripts (Tuttle, 2021; Whitney, 2021).

Promoting resilience calls for leadership, resource allocation, planning, and awareness (O'Rourke & Briggs, 2007). Understanding how network members view a common problem can help enhance communication and understand interdependencies (Linkov et al., 2014). Systems that combine principles of business continuity with cyber threat warning systems can promote better preparedness and cyber resilience against cyber incidents (DYNAMO project, 2024).

Transparent dialogue on resilience management, and potential risks, supported by innovative leadership, effective planning, and long-term commitment to allocate needed resources help build and maintain acceptance of resilience (Linkov et al., 2014; O'Rourke & Briggs, 2007). Systems often show complex interactions between people, technologies, and processes (Vos, 2017), and the vulnerability of many of these socio-technical systems (combining human and technical aspects) have increased; understanding the mutual entanglement of material structures and human organisations help create practices to anticipate possible incidents and promote feedback and learning (Amir & Kant, 2018; Rajamäki & Ruoslahti, 2018).

(Vos, 2017) states that organisational resilience as a framework can create tools and conditions to help reduce risks, understand issues, and mitigate crises.

Resilience requires adaptive capacities and cooperation (Vos, 2017), where information on threats and vulnerabilities helps identify trends, understand risks, and determine preventive measures (Stanciugelu et al., 2013).

The resilience matrix integrates the phases of planning, absorbing, recovering, and learning/adapting combined with domains physical, information, cognitive, and social (Linkov et al., 2013). Domains can be based on business continuity management (BMC), adding elements: risks, critical functions, key personnel, guidelines/procedures, and open communication (Ruoslahti, 2020). These principles are combined in the project DYNAMO matrix (Hytönen & Ruoslahti, 2023).

2.2 Cybersecurity

The growing numbers and increasing sophistication of cybersecurity threats and attacks are a reality and one of the foremost risks to business continuity (Michel & King, 2019). Continuity management for critical infrastructure operators and their networks rely on the interconnectivity between other networks and systems of systems (Linkov et al., 2013).

Cybersecurity helps make the online secure and safe; cybersecurity uses technology and legislation to protect and manage information (Ruoslahti & Tikanmäki, 2022). Cybersecurity can be seen as processes and measures that protect cyberspace, its systems, physical aspects, devices, and software, which have no geographical boundaries leaving only digital traces (Mohammed, 2015) from foreseen threats (Craig et al., 2014). Cyber events can have very tangible effects though cyberspace in itself is intangible (Shoemaker & Conklin, 2011), and cybersecurity as well as security in general should be solidly embedded in all organisational processes (Kilani, 2020).

New cyber threats and vulnerabilities are constantly emerging, so cybersecurity needs to be a consistent and continuous process (Cavelty, 2010). Cybersecurity is needed to protect applications and cyberspace from various threats that could compromise their safety (Craig et al., 2014). Making cybersecurity part of comprehensive security and part of one's organisational security culture shared by all builds situational awareness, defined direction and guidelines (Linnell et al., 2014).

Cybercrime internationally is one recognised threat to cybersecurity (Mohammed, 2015), and costs caused by cybercrime have continuously increased (Cavelty, 2010). Cybercrime is seen as all illegal and criminal acts against computer data, systems, unauthorised access, modification or impairment of digital or computer systems (Mohammed, 2015; Payne, 2020).

ICT skills can be upgraded through proper ICT training (Conkova, 2013; Isidro-Filho et al., 2013).

Building skills and competencies aim at people to better navigate the cyber domain (Aaltola & Taitto, 2019). With appropriate knowledge of ICT, workers can capture, store and share organisational knowledge that makes their expertise better available within the organisation (Im et al., 2013), and that organisations can develop the skills needed to absorb state-of-the-art knowledge from external sources (Cupiał et al., 2018).

2.3 Information Sharing

A secure barrier formed by cybersecurity can protect a most valuable organisational asset. Cybersecurity measures can enhance business continuity when well-organised and widely applied. According to literature, business continuity is the primary focus of every organisation, and Figure 1 shows how cyber security can be seen as a circle surrounding it (Frisk et al., 2022).

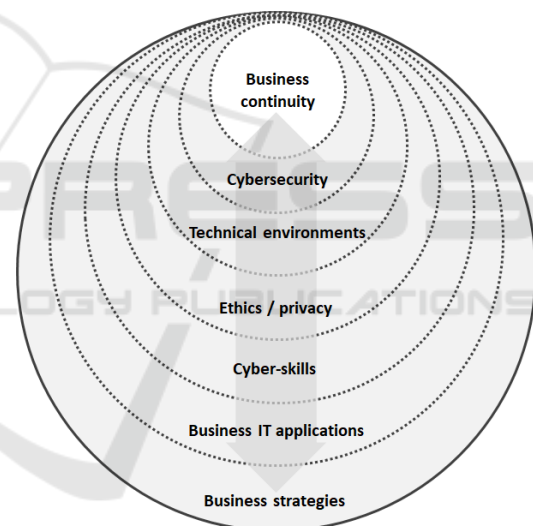


Figure 1: Model of the dimensions of cybersecurity (Frisk et al., 2022).

Cyber security is the key to achieving business continuity. The foundation for comprehensive cyber security combines appropriate levels of cyber skills and well-functioning trusted technical environments. Ethical configuration and use of technical environments are necessary to ensure privacy when using applications, as neither alone can guarantee security. Cyber security insight is provided by the company's IT applications, which have both digital and physical elements and are cyber-physical in nature. (Frisk et al., 2022).

The Maritime Integrated Surveillance Awareness (MARISA) project's user community's collaboration

was complicated due to its nature. The use cases of the MARISA project involved numerous actors from various sectors and countries. The complexity of the sector was further complicated by the presence of multiple authorities, such as police and gendarmerie, in some EU member states. (MARISA Project, 2017).

Collaboration is a key factor in the development of knowledge (Pirinen, 2015), and it is necessary to work intensely (Ruoslahti, 2018, p. 115), including interdependence and resource integration (Ruoslahti & Tikanmäki, 2017).

The consequence is the requirement to use resources belonging to others and generate exchange value: “Knowledge itself is an increasingly important source to competitive advantage and a key to the success of modern organisations and creative higher education, strengthening the collective expertise, industry-service clusters, employees and competitiveness in the global economy” (Pirinen, 2015, p. 315).

The dynamic interaction between several different actors with different interests must be highlighted in organisations' multi-stakeholder communication, including consortia of publicly funded innovation projects (Vos et al., 2014). Issues that hold the most significance to people are those that are central to them, as stated by (Luoma-aho & Vos, 2010). Problem-solving arenas for exchanging practical, legal, and ethical issues are provided by authority communities, where actors work together to define and refine creative use cases. These arenas are also places where people compete for problem-solving and influence, with their decisions being influenced by both common agendas and one's activities (Vos, 2018).

(Pirinen, 2017) states that sharing information and situational information is necessary to enhance resilience. Awareness and communication can help promote flexible networks (O'Rourke & Briggs, 2007). To be effective in addressing resilience training, it is necessary to include all stakeholders, such as industry, industry associations, and decision-makers (Ruoslahti et al., 2018).

The importance of communication with stakeholders in terms of resilience is highlighted by (Linkov et al., 2014). Networked organisations are striving to enhance their resilience due to the vulnerability inherent in interdependencies.

Building situational awareness and promoting collaboration requires the interaction between authorities and the sharing of information, which is important in increasing safety. Cooperation aims to enhance the situation by increasing recognition, exchanging best practices, enhancing interoperability, decreasing overlap, and promoting

cooperation across borders and sectors. (Tikanmäki & Ruoslahti, 2017).

Situational awareness is a crucial factor in resolving security incidents. Understanding the current situation and how their actions affect it is what it means to a person. Following an appropriate security policy can lead to a higher level of understanding and awareness. All employees are required to undergo training and continuous cyber security development as part of the security policy (Almén et al., 2022).

Network disruption data sharing between critical infrastructure administrators and law enforcement authorities can provide them with a shared situational awareness of new threats. A more proactive defensive position can be achieved through the identification of attack patterns, emerging vulnerabilities, and potential targets through this cooperation. Potential attackers can be deterred by a robust information sharing framework. Preventing adversaries from targeting critical infrastructure by quickly detecting, sharing, and responding to any cyber intrusion.

3 METHOD

This study is a qualitative multi-case research analysis consisting of systematic reviews and cross-case conclusions of six (n = 6) case studies on information sharing among partners.

Table 1: Six (n = 6) case studies on information sharing among partners.

Data sources	Title
ECHO Deliverable D8.2	E-EWS and E-FCR demonstration surveys
Rajamäki & Katos, 2020	Information Sharing Models for Early Warning Systems of Cybersecurity Intelligence
Simola, J., & Lehto, M. 2020	National cyber threat prevention mechanism as a part of the E-EWS.
Rajamäki et al., 2024	View of E-EWS-based Governance Framework for Sharing Cyber Threat Intelligence in the Energy Sector
Hytönen, E., Rajamäki, J., & Ruoslahti, H., 2023	Managing Variable Cyber Environments with Organizational Foresight and Resilience Thinking.
Almén, C., Hagström, N., & Rajamäki, J., 2022	ECHO Early Warning System as a Preventive Tool against Cybercrime in the Energy Sector.

The final analysis provides a deeper understanding of how EWS can enable cyber incident information sharing across organisational boundaries between critical infrastructure operators and Law Enforcement Agencies (LEA).

4 ECHO EARLY WARNING SYSTEM

Early Warning Systems (EWS) can help critical infrastructure providers share information on cyber threats in near real-time, which allows them to be more proactive in protecting their systems from attacks (Simola & Lehto, 2020).

The ECHO Early Warning System (E-EWS) will allow the collection and preservation of evidence in a forensically sound manner through information sharing between CERTS/CSIRTS, Critical infrastructure and services providers, and LEA (Rajamäki & Katos, 2020).

Table 2: EWS network partners. Modified from (Rajamäki & Katos, 2020).

EWS User	Role
National/EU CERTS	Protect critical infrastructure
ISP CERTS	Protect Internet and its services
Organisational CERTS	Protect organisation
ICT Vendor CERTS	Protect products
Law enforcement Agencies	Ensure public safety and security of society
Critical infrastructure organisations	Provide products and services critical to society
Organisations, Individuals, Researchers	Secondary users that may be involved when handling incidents.

The E-EWS is a tool used to enhance proactive cyber defence through effective information sharing. It facilitates trusted cooperation among multiple parties in the cybersecurity domain, providing reliable incident handling and collaboration capabilities (Almén et al., 2022).

Sharing essential information quickly between stakeholders requires automated information sharing. E-EWS is designed to provide a security support tool that facilitates the coordination and sharing of information among ECHO network members in near real-time (Simola & Lehto, 2020). Proactive cyber defence is improved and strengthened through efficient and effective information sharing through the E-EWS tool. A reliable cooperation between multiple parties on the cyber security scene is created by the tool. (Almén et al., 2022).

Cyber-sensitive data management and related data management can be completely independent for ECHO partners in E-EWS. In the public safety environment, the early warning system functions as a supplementary component to other mechanisms. (Simola & Lehto, 2020). Collaboration and case handling are enhanced by its excellent and reliable features. These are suitable for use both at the start of attacks and during the duration of the attack (Almén et al., 2022).

Critical infrastructure operators use command and control networks and systems – Industrial Control Systems (ICS) / Supervisory Control and Data Acquisition (SCADA) systems – designed to support industrial processes. Today, ICS and SCADA systems are widely used in many critical infrastructure sectors to help for process control, automation, and safety (Almén et al., 2022).

The tool aims to aid and improve the performance of computer/cyber emergency response teams, including CIRTs and SOCs. Alerts are shared among partners and are the main source of information for E-EWS. An enriched data model that can be accessed by both humans and machines is produced by analysing and using alerts. Alerts give access to a vast array of attributes for records that can be utilised. (Almén et al., 2022). Table 3 provides three specific examples of how the EWS can help critical infrastructure providers.

Table 3: Examples of benefits of EWS to critical infrastructure. Modified from (Simola & Lehto, 2020).

Example	Possible actions
Provider receives alert from the EWS about a new malware that is targeting critical infrastructure.	Protect systems from malware, such as installing security patches or updating their antivirus software
Provider receives alert from the EWS about a denial-of-service attack that is targeting a specific critical infrastructure sector.	Protect systems from the attack, such as increasing their bandwidth or implementing security measures to prevent the attack from succeeding
Provider may participate in coordinated response to a cyber incident with other providers, government agencies, and other stakeholders.	Sharing information about the incident, coordinating security measures, or developing a plan for recovery

Firstly, as seen above (Table 3) a critical infrastructure provider receives an alert from the EWS about a new malware targeting critical infrastructure. The provider is prompted to take steps to protect their systems from the malware, e.g., by

installing security patches or updating their antivirus software. Secondly, a provider receives an alert from the EWS about a denial-of-service attack that is targeting a specific critical infrastructure sector. This would allow the provider to take steps to protect their systems from the attack by e.g., increasing their bandwidth or implementing security measures to prevent the attack from succeeding. Thirdly, a provider participates in a coordinated response to a cyber incident with LEA, government agencies, and other providers or stakeholders, involving e.g., sharing information about the incident, coordinating security measures, or developing a recovery plan. (Simola & Lehto, 2020).

Projects ECHO and DYNAMO connect information sharing with the concept of situation awareness – understanding the current situation of a security incident and how one’s actions impact the situation – is an important element in solving critical infrastructure security incidents (Almén et al., 2022, pp. 17). Cyber situational awareness to support decision-making can be improved by combining systematic Cyber Threat Intelligence (CTI) and Business Continuity Management (BCM) (Hytönen et al., 2023).

Early warning systems can be highly beneficial for users in countering potential threats and attacks (Simola, 2019). However, it's crucial to note that the effectiveness of these systems may be compromised if the users operating them are unsure of how to act in difficult circumstances (Matveeva, 2006).

Cybercriminals and state-sponsored actors can exploit vulnerabilities in industrial control systems and SCADA systems (Alanazi et al., 2023). The E-EWS, further developed at DYNAMO, offers the energy sector valuable resources to secure infrastructure availability and performance in the event of a cyber threat and prevent this type of attack (Rajamäki et al., 2024).

The complexity of interdependencies and their impact on operational continuity is often forgotten during traditional risk assessments and information security management processes (Hytönen et al., 2023). All company or organisation staff should have an understanding of cybersecurity-related issues and countermeasures (National Cyber Security Centre, 2016).

EWSs assist in orchestrating responses to cyber incidents, potentially reducing the impact of attacks and preventing their spread to other service providers (Simola, 2019).

Fighting cybercrime requires a powerful combination of situation awareness and Early Warning Systems (Almén et al., 2022). Improving

cyber security awareness, coordination, and response capabilities can be achieved through EWS, which can be an important instrument for safeguarding critical infrastructure against cyber threats (Ramaki & Atani, 2016).

5 CONCLUSIONS

Providing a common platform for cybersecurity information sharing can help improve communication and collaboration between providers, government agencies, and other stakeholders. Early warning systems (EWS) can help raise awareness about cybersecurity threats and best practices among critical infrastructure providers (Almén et al., 2022; Rajamäki & Katos, 2020; Simola & Lehto, 2020).

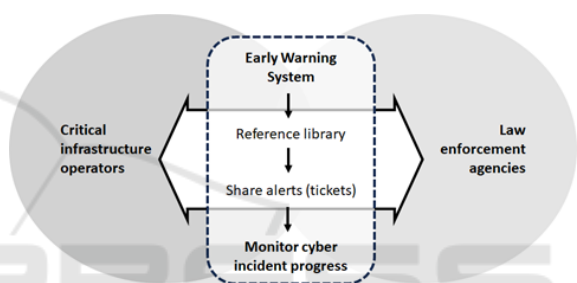


Figure 2: The concept to connect critical infrastructure operators and law enforcement agencies with Early Warning Systems to share cyber incident information (by author).

Critical infrastructure operators and law enforcement agencies (LEA) can share information on cyber incidents and monitor cyber incident progress (Figure 2). The two entities would use an EWS to exchange cyber threat intelligence. Information sharing can be facilitated with a common reference library where alerts can be shared as tickets. This would enable information exchange in both directions.

The security of critical infrastructure like power grids, water supplies, transportation systems, and communication networks has become crucial in an interconnected world. The breakdown of these systems is a significant risk to economic, social, and national security, as they are the backbone of modern society. Fostering strong collaboration between critical infrastructure operators and law enforcement agencies is a highly effective strategy for securing these vital assets. Our collective ability to detect, prevent, and respond to cyber threats is enhanced by this partnership, which enables us to share cyber incident information through EWS.

Cybercriminals and nation-state actors are attracted to critical infrastructure due to its central role in societal functioning. A cyber-attack that succeeds in attacking these systems can cause widespread outages, economic losses, and even death. The power grid may be disrupted by a cyber-attack, which can have an impact on hospitals, emergency services, and everyday operations. The protection of these systems is a national responsibility, not just a technical challenge.

The investigation of cybercrimes, gathering intelligence on potential threats, and coordinating responses to cyber incidents are all carried out by LEA. The early detection of anomalies and potential cyber intrusions by critical infrastructure operators can be strengthened by timely and accurate information exchange with their efforts.

Cyber threats are detected by early warning systems before they can cause significant damage. To identify and report suspicious activity, these systems utilise continuous monitoring, data analytics, and threat intelligence. Early warning systems can gain a broader perspective on the threat landscape by integrating inputs from multiple sources, such as critical infrastructure operators and LEAs.

By sharing information, coordinating response can be achieved and all relevant parties can be informed to take appropriate action to mitigate impacts. The significance of this is amplified for critical infrastructure, as a delay in response can lead to significant consequences.

EWS can help critical infrastructure providers improve their situational awareness with a more comprehensive picture of the cyber threat landscape, which can help them identify and prioritise risks. EWS facilitate collaboration by helping critical infrastructure providers to collaborate with each other and with LEA to share information and resources. EWS enhance incident response by providing them with access to information and resources.

Our contribution to theory is the understanding that EWS can greatly facilitate cyber incident information sharing between critical infrastructure operators and LEAs, and the contribution to practice is, despite only providing a preliminary take on the subject, opening a practical discussion on how critical infrastructure operators and LEAs can better collaborate in cyber incident management. Further study is recommended to gain a more in-depth discussion of the practical ramifications and real-world uses of EWS. These future studies should look to understand how different critical infrastructure operators and LEAs can use EWS as a common information-sharing environment in various practical

settings and national structures that may differ between EU member states.

Sharing cyber incident information through early warning systems with critical infrastructure operators and law enforcement is a crucial step in improving cybersecurity. Overcoming challenges associated with trust, standardisation, legal frameworks, and technical integration can result in more effective threat detection, better incident response, and a more resilient society through collaboration. As cyber threats progress, so do our methods to safeguard the vital systems that support our way of life. The overall security and stability of an interconnected world are strengthened through this collaborative approach, which not only secures critical infrastructure but also enhances its overall security and stability.

ACKNOWLEDGEMENTS

This study has received funding from the European Union projects DYNAMO, under grant agreement no. 101069601 and CONNECTOR, under grant agreement no. 101121271. The views expressed are those of the authors only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

REFERENCES

- Aaltola, K., & Taitto, P. (2019). Utilising Experiential and Organizational Learning Theories to Improve Human Performance in Cyber Training. *Information & Security: An International Journal*, 43(2), 123–133. <https://doi.org/10.11610/isij.4311>
- Alanazi, M., Mahmood, A., & Chowdhury, M. J. M. (2023). SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues. *Computers & Security*, 125, 103028. <https://doi.org/10.1016/j.cose.2022.103028>
- Allianz Global Corporate & Specialty SE. (2023). *Allianz Risk Barometer: Identifying the major business risks for 2023* (p. 40) [Survey].
- Almén, C., Hagström, N., & Rajamäki, J. (2022). ECHO Early Warning System as a Preventive Tool against Cybercrime in the Energy Sector. *Information & Security: An International Journal*, 53(1), 11–20. <https://doi.org/10.11610/isij.5301>
- Amir, S., & Kant, V. (2018). Sociotechnical Resilience: A Preliminary Concept. *Risk Analysis*, 38(1), 8–16. <https://doi.org/10.1111/risa.12816>
- Cauffman, S. A. (2018). *Community resilience planning guide for buildings and infrastructure systems: Observations on initial implementations* (Guide

- NISTIR 8229; p. 39). US Department of Commerce, National Institute of Standards and Technology. <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8229.pdf>
- Cavelty, M. D. (2010). Cyber-Security. In *The Routledge Handbook of New Security Studies* (1st ed., p. 328). Routledge.
- Conkova, M. (2013). Analysis of Perceptions of Conventional and E-Learning Education in Corporate Training. *Journal of Competitiveness*, 5(4), 73–97. <https://doi.org/10.7441/joc.2013.04.05>
- Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, 4(10), 13–21.
- Cupiał, M., Szeląg-Sikora, A., Sikora, J., Rorat, J., & Niemiec, M. (2018). Information technology tools in corporate knowledge management. *Ekonomia i Prawo. Economics and Law*, 17(1), 5–15.
- DYNAMO project. (2024, May 9). *Dynamic Resilience Assessment Method including combined Business Continuity Management and Cyber Threat Intelligence solution for Critical Sectors*. https://horizon-dynamo.eu/wp-content/uploads/2023/01/DYNAMO_Leaflet_web.pdf
- ECHO project. (2021). *E-EWS and E-FCR demonstration surveys* (Deliverable D8.2; p. 25). European Commission. https://echonetwork.eu/wp-content/uploads/2022/03/ECHO-D8.2-E-EWS-and-E-FCR-demonstration-surveys_v1.0.pdf
- Fitch Solutions. (2021). *South Africa Autos Report* (Country Industry Reports Q4; p. 1). Fitch Solutions. <https://store.fitchsolutions.com/autos/south-africa-autos-report>
- Frisk, I., Tikanmäki, I., & Ruoslahti, H. (2022). Piloting the ECHO E-skills and Training Toolkit. *Information & Security: An International Journal*, 53(2), 163–175. <https://doi.org/10.11610/isij.5311>
- Ghafur, S., Graß, E., Jennings, N., & Darzi, A. (2019). The challenges of cybersecurity in health care: The UK National Health Service as a case study. *The Lancet Digital Health*, 1(1), e10–e12. [https://doi.org/10.1016/S2589-7500\(19\)30005-6](https://doi.org/10.1016/S2589-7500(19)30005-6)
- Hytönen, E., Rajamäki, J., & Ruoslahti, H. (2023). Managing Variable Cyber Environments with Organizational Foresight and Resilience Thinking. *International Conference on Cyber Warfare and Security*, 18, 162–170. <https://doi.org/10.34190/iccws.18.1.979>
- Hytönen, E., & Ruoslahti, H. (2023). A Lens to Examine Communication Through Business Continuity Management. In D. Verčič, A. T. Verčič, & K. Sriramesh (Eds.), *Public Relations and Sustainability* (pp. 205–216). University of Ljubljana: Faculty of Social Sciences. <https://www.bledcom.com/>
- Im, T., Porumbescu, G., & Lee, H. (2013). ICT as a Buffer to Change. *Public Performance & Management Review*, 36(3), 436–455. <https://doi.org/10.2753/PMR1530-9576360303>
- Isidro-Filho, A., Guimarães, T. de A., Perin, M. G., & Leung, R. C. (2013). Workplace learning strategies and professional competencies in innovation contexts in Brazilian hospitals. *BAR - Brazilian Administration Review*, 10(2), 121–134. <https://doi.org/10.1590/S1807-76922013000200002>
- Kilani, Y. (2020). Cyber-security effect on organizational internal process: Mediating role of technological infrastructure. *Problems and Perspectives in Management*, 18, 449–460. [https://doi.org/10.21511/ppm.18\(1\).2020.39](https://doi.org/10.21511/ppm.18(1).2020.39)
- Limnell, J., Majewski, K., & Salminen, M. (2014). *Kyberturvallisuus*. Docendo.
- Linkov, I., Bridges, T., Creutzig, F., Decker, J., Fox-Lent, C., Kröger, W., Lambert, J. H., Levermann, A., Montreuil, B., & Nathwani, J. (2014). Changing the resilience paradigm. *Nature Climate Change*, 4(6), 407–409.
- Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions*, 33, 471–476.
- Luoma-aho, V., & Vos, M. (2010). Towards a more dynamic stakeholder model: Acknowledging multiple issue arenas. *Corporate Communications: An International Journal*, 15(3), 315–331. <https://doi.org/10.1108/13563281011068159>
- MARISA Project. (2017). *MARISA Grant Agreement number 740698*. European Commission.
- Matveeva, A. (2006). *Early Warning and Early Response: Conceptual and Empirical Dilemmas* (Issue Paper 1; p. 66). European Centre for Conflict Prevention /International Secretariat of the Global Partnership for the Prevention of Armed Conflict. <https://gppac.net/files/2018-12/Early%20Warning%20and%20Early%20Response.pdf>
- Michel, M. C. K., & King, M. C. (2019). Cyber Influence of Human Behavior: Personal and National Security, Privacy, and Fraud Awareness to Prevent Harm. *2019 IEEE International Symposium on Technology and Society (ISTAS)*, 1–7. <https://doi.org/10.1109/ISTAS48451.2019.8938009>
- Mohammed, S. (2015). An Introduction to Digital Crimes. *International Journal in Foundations of Computer Science & Technology*, 5(3), 13–24. <https://doi.org/10.5121/ijfctst.2015.5302>
- Muthuppalaniappan, M., & Stevenson, K. (2020). Healthcare Cyber-Attacks and the COVID-19 Pandemic: An Urgent Threat to Global Health. *International Journal for Quality in Health Care*, 33(1), 1–4. <https://doi.org/10.1093/intqhc/mzaa117>
- National Cyber Security Centre. (2016). *Common Cyber Attacks: Reducing the Impact*. Crown Copyright. <https://www.ncsc.gov.uk/guidance/white-papers/common-cyber-attacks-reducing-impact>
- O'Rourke, T. D., & Briggs, T. R. (2007). Critical Infrastructure, Interdependencies, and Resilience. *The Bridge*, 22–29.
- Payne, B. K. (2020). Defining Cybercrime. In T. J. Holt & A. M. Bossler (Eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 3–

- 25). Springer International Publishing. https://doi.org/10.1007/978-3-319-78440-3_1
- Pirinen, R. (2015). Studies of Externally Funded Research and Development Projects in Higher Education: Knowledge Sources and Transfers. *Creative Education*, 6(3), 315–330. <https://doi.org/10.4236/ce.2015.63030>
- Pirinen, R. (2017). Towards Common Information Systems Maturity Validation: Resilience Readiness Levels (ResRL). In *Proceedings of the 9th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management*, 3, 259–266. <https://doi.org/10.5220/0006450802590266>
- Pöyhönen, J., Rajamäki, J., Ruoslahti, H., & Lehto, M. (2020). Cyber Situational Awareness in Critical Infrastructure Protection. *Annals of Disaster Risk Sciences : ADRS*, 3(1), 0–0. <https://doi.org/10.51381/adrs.v3i1.36>
- Rajamäki, J., Feyesa, A., & Nepal, A. (2024). View of E-EWS-based Governance Framework for Sharing Cyber Threat Intelligence in the Energy Sector. *Proceedings of the 23rd European Conference on Cyber Warfare and Security, ECCWS 2024*, 23, 398–406. <https://doi.org/10.34190/eccws.23.1.2073>
- Rajamäki, J., & Katos, V. (2020). Information Sharing Models for Early Warning Systems of Cybersecurity Intelligence. *31679, 46(2)*, 198–214.
- Rajamäki, J., & Ruoslahti, H. (2018). Educational Competences with Regard to Critical Infrastructure Protection. *Journal of Information Warfare*, 17(3), 415–423.
- Ramaki, A. A., & Atani, R. E. (2016). A survey of IT early warning systems: Architectures, challenges, and solutions. *Security and Communication Networks*, 9(17), 4751–4776. <https://doi.org/10.1002/sec.1647>
- Ruoslahti, H. (2018). Co-creation of knowledge for innovation requires multi-stakeholder public relations. In *Public Relations and the Power of Creativity* (Vol. 3, pp. 115–133). Emerald Publishing Limited.
- Ruoslahti, H. (2020). Business continuity for critical infrastructure operators. *Annals of Disaster Risk Sciences: ADRS*, 3(1), 0–0.
- Ruoslahti, H., Rajamäki, J., & Koski, E. (2018). Educational Competences with regard to Resilience of Critical Infrastructure. *Journal of Information Warfare*, 17(3), 1–16.
- Ruoslahti, H., & Tikanmäki, I. (2017). End-users Co-create Shared Information for a More Complete Real-time Maritime Picture: *Proceedings of the 9th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management*, 267–274. <https://doi.org/10.5220/0006559702670274>
- Ruoslahti, H., & Tikanmäki, I. (2022). Cybersecurity in Skills Development and Leadership. *Future-Proof Business - System Leadership Competences*. 3UAS: Future-proof Business - System Leadership Competences, Virtual conference.
- Schoemaker, D., & Conklin, W. A. (2011). *Cybersecurity: The Essential Body of Knowledge*. Cengage Learning.
- Simola, J. (2019). Comparative Research of Cybersecurity Information Sharing Models. *Information & Security: An International Journal*, 43(2), 175–195. <https://doi.org/10.11610/isij.4315>
- Simola, J., & Lehto, M. (2020). National Cyber Threat Prevention Mechanism as a part of the E-EWS. *The Proceedings of the International Conference on Cyber Warfare and Security*, 539–548. <https://jyx.jyu.fi/handle/123456789/69054>
- Stanciugelu, I., Alpas, H., Florin, S. D., & Bozoglu, F. (2013). Perception and communication of terrorism risk on food supply chain: A case study (Romania and Turkey). In *Applied Social Sciences: Communication Studies* (pp. 189–196). Cambridge Scholars Publishing.
- The International Chamber of Commerce. (2024, July). *Protecting the cybersecurity of critical infrastructures and their supply chains*. ICC. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_2021/ICC-2024_Protecting-the-cybersecurity-of-critical-infrastructures-and-their-supply-chains.pdf
- Tikanmäki, I., & Ruoslahti, H. (2017). Increasing Cooperation between the European Maritime Domain Authorities. *International Journal of Environmental Science*, 02. <https://www.iaras.org/iaras/home/caijes/increasing-cooperation-between-the-european-maritime-domain-authorities>
- Tuttle, H. (2021, March). Ransomware Attackers Turn to Double Extortion. *Risk Management*, 68(2), 8–9.
- Vos, M. (2017). *Communication in turbulent times: Exploring issue arenas and crisis communication to enhance organisational resilience* (Vol. 40). Vos & Schoemaker.
- Vos, M. (2018). Issue Arenas. In R. L. Heath & W. Johansen, *The International Encyclopedia of Strategic Communication* (1st ed., pp. 1–10). John Wiley & Sons. <https://doi.org/10.1002/9781119010722.iesc0093>
- Vos, M., Schoemaker, H., & Luoma-aho, V. (2014). Setting the agenda for research on issue arenas. *Corporate Communications: An International Journal*, 19(2), 200–215. <https://doi.org/10.1108/CCIJ-08-2012-0055>
- Whitney, L. (2021, June 4). *Ransomware: A Cheat Sheet for Professionals*. TechRepublic. <https://www.techrepublic.com/article/ransomware-cheat-sheet-everything-you-need-to-know/>