Trust Environment for Cyber-Physical Systems: The DYNAMO Approach

JYRI RAJAMÄKI
Unit W
Laurea University of Applied Sciences
Vanha maantie 9, 02650 Espoo
FINLAND

Abstract: - This paper explores the evolving landscape of cybersecurity within cyber-physical systems, emphasizing the critical need for resilience and trust-building mechanisms. Grounded in the foundational perspectives of Cybersecurity Science, the study addresses the challenges posed by the complex interdependencies among physical, information, cognitive, and social domains. It introduces the DYNAMO platform, a novel approach that integrates Cyber Threat Intelligence (CTI) with Business Continuity Management (BCM) to enhance situational awareness and recovery planning. The platform's comprehensive methodology spans existing tool incorporation, detailed assessments, identification of gaps, simulations, and knowledge generation. Furthermore, the paper delves into the intricacies of cybersecurity information sharing, advocating for a unified approach to combat hybrid threats. The establishment of a common operational picture and shared situational awareness emerges as pivotal, underlining the indispensable role of technology, social trust, and resilience in securing critical information-sharing mechanisms in cyber-physical systems.

Key-Words: - Cyber information sharing, cyber-physical system, cyber resilience, cybersecurity, cyber threat intelligence, DYNAMO Project, early warning system

Received: March 9, 2023. Revised: November 19, 2023. Accepted: December 21, 2023. Published: January 8, 2024.

1 Introduction

In today's dynamic and interconnected world, the realm of cybersecurity faces unprecedented challenges as cyber-physical systems become integral components of critical infrastructure. The convergence of cyber and physical domains has given rise to a complex landscape marked by diverse threats, including natural disasters, cyber-attacks, physical assaults, technical failures, and human errors. As a result, ensuring the resilience of these cyber-physical systems has become a paramount concern [1].

Cybersecurity science provides a foundation for understanding the complexity of cyber systems. This framework includes three key theoretical perspectives [2]:

1. the data or information perspective
2. the technology perspective
3. the human or social perspective.

Nowadays, we mostly focus on understanding the system through one perspective. However, the complexity of the threats would require a comprehensive approach, in which case the system should be reviewed across domain boundaries. For example, the European Union's General Data Protection Regulation (GDPR) illustrates the challenges of protecting personal data and highlights the need for a comprehensive understanding that encompasses human, physical, and data. When acting according to the GDPR, you need to know who processes the data, what this data is, and with what technology the data is processed, i.e., all three perspectives must be considered at the same time.

Critical infrastructures are cyber-physical systems. They face not only technical challenges but also due to their complex connections to other systems. According to the network-centric operational doctrine [3], these systems are divided into four domains:

1. physical
2. informational
3. cognitive,
4. social.

In this context, resilience means responding to challenges in these areas to increase trust and maintain operational stability.

Cybersecurity is central to promoting the digital world's trust, which includes key themes such as security management, situational awareness, security technology, and operational system resilience [4]. This foundation provides the background for the DYNAMO platform [5], designed to improve resilience assessment in critical sectors by combining Business Continuity Management (BCM) and Cyber Threat Intelligence (CTI).

The DYNAMO platform aims to respond to the multifaceted challenges caused by cyber threats with a holistic approach. By integrating CTI and BCM methods, the platform can improve situational awareness and recovery planning capabilities. Combining existing tools, comprehensive assessments, identifying gaps, simulations, and generating data form the pillars of the DYNAMO BCM approach [5].

For now, the DYNAMO platform focuses on identifying threats in the healthcare, energy, and maritime sectors. The Tool Portfolio related to the platform includes tools for incident detection, predictive analytics, visualization, information sharing, and cybersecurity information management, which contributes to a unified and functional Cyber Knowledge Graph [5].

Effective sharing of cyber security information becomes more important when threats evolve, including hybrid threats. A common early warning solution is imperative, extending beyond mere prevention to include the identification, tracing, and prosecution of cybercriminals. The integration of national Computer Emergency Response Teams (CERTs) and collaboration at regional and international levels underscores the necessity for shared cyber situational awareness.

As the article progresses, it delves into the intricate details of the DYNAMO information-sharing model, its trust-building mechanisms, and the establishment of a common operational picture for improving resilience. The exploration encompasses various domains - physical and technology, data, social, and cognitive decisions - shedding light on the comprehensive approach needed to build trust and resilience in the ever-evolving landscape of cyber-physical systems

2 Related Work

2.1 Cyber-Physical Resilience

In the ever-evolving landscape of cyber security and information systems, understanding the theoretical foundations of cyber systems is crucial. According to Edgar and Manz [2], Cyber Security Science encompasses three key theoretical perspectives within the realm of cyberspace:

1. Data or Information Perspective: Rooted in information theory, this perspective examines the flow of data and information within the cyber domain.
2. Technology Perspective: Encompassing hardware and software components, this perspective addresses the technical aspects that constitute the cyber environment.
3. Human Perspective: Recognizing the pivotal role of human actions and decisions in shaping cyber systems, this perspective highlights the significance of human factors alongside data and technology in understanding and managing cybersecurity.

Present efforts predominantly revolve around delineating systems within singular domains, whether it be the physical, information, or social domain, and the physical domain is usually the only domain explicitly modeled in most disaster-relief risk analysis models [6]. However, the prevailing landscape of security challenges is marked by an escalating complexity of threats that extend beyond these isolated domains. This intricate situation is further exacerbated by the growing interdependencies among these diverse domains. A noteworthy illustration of this challenge is meeting the criteria set by the EU’s General Data Protection Regulation 2016/679 (GDPR). Addressing questions such as the location of personal information, data ownership, secondary data usage by processors, data transfers to third parties, data retention policies, data protection measures, data processing entities, and the purpose of data processing cannot be adequately achieved by focusing solely on one domain.

As Figure 1 presents, cyber-physical systems can be seen as cyber systems that operate within human-designed environments and the natural world. They are confronting a myriad of challenges. They face a myriad of challenges that include natural disasters, cyber-attacks, physical attacks, technical failures, and human errors. What sets them apart as a characteristic of critical infrastructure is their complex interconnections with other systems, adding more complexity to their security environment [1].

A network-centric operations doctrine divides networked systems into four domains: 1) the physical domain, mainly the system infrastructure, and equipment; 2) the information domain, the information systems about the physical systems; 3) the cognitive domain, mainly decision-making processes informed by the information domain; and finally, 4) the social domain, the human resources supporting the entire system [3]. Linkov et al. [7] used this doctrine for designing the resilience matrix to explicitly capture the capacity of a system across the timeline of a disruptive event. Prochazkova and Prochazka [8] present a decision support system for determining the risk level of socio-cyber-physical systems, which shows the current level of risk and enables dangerous situations to be revealed and measures to be taken in time.

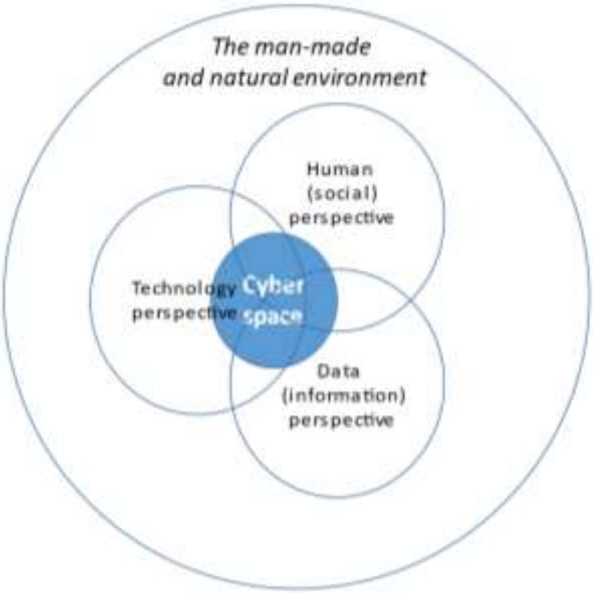

Fig. 1: Cyber-physical system as a cyber system operating in its environment.

Cybersecurity plays a pivotal role in fostering trust within the digital realm, aiming to achieve resilience across all operational systems and infrastructures. DIMECC [4] delineates four central themes in cybersecurity: security management, situational awareness, security technologies, and the resilience of operational systems. Figure 2 shows a resilient cyber-physical eHealth system. The figure has been adapted from DIMECC's model by substituting the 'boxes' representing situational awareness and resilience with the three perspectives of cyber systems.

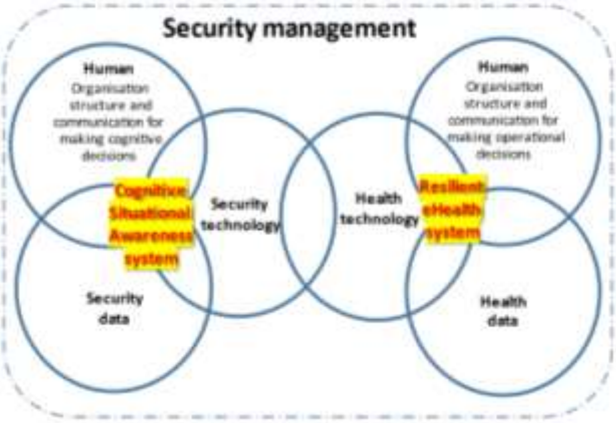
Security management
Human
Organisation structure and communication for making cognitive decisions
Cognitive Situational Awareness system
Security technology
Security data
Health technology
Human
Organisation structure and communication for making operational decisions
Resilient eHealth system
Health data

Fig. 2: Themes of a resilient cyber-physical eHealth system.

2.2 DYNAMO Platform

The DYNAMO platform aims to enhance resilience assessment in critical sectors by combining Business Continuity Management (BCM) and Cyber Threat Intelligence (CTI) [5].

CTI is information based on knowledge, skills, and experience to mitigate potential cyber threats. It involves identifying cyber-attacks, understanding threat actors' motives and approaches, and processing results to evaluate risks. DYNAMO integrates CTI processing with BCM approaches to improve situational awareness and recovery planning capabilities for businesses and critical infrastructures [9].

BCM is a discipline focused on the advanced planning, preparation, and implementation of procedures within an organization. The goal is to maintain business functions within acceptable time frames and predefined capacities during disruptions, such as cyber-attacks. The BCM process involves business impact analysis to identify potential events that could interrupt business operations. Procedures are then defined to either avoid or mitigate the impact of these events. Regular testing, review, and employee training are crucial elements of BCM to ensure effectiveness and resilience. With the increasing threat of cyber-attacks in today's technologically driven business landscape, it is essential to integrate BCM processes to safeguard critical sectors [10].

The DYNAMO BCM approach includes:

1. Incorporation of Existing Tools: DYNAMO plans to build on existing tools and approaches to create an advanced situational awareness toolset, knowledge repository, training tools, and a forensic intelligence toolset.
2. Comprehensive Assessment: The platform aims to provide a detailed assessment of critical business processes, interactions within sectors, potential vulnerabilities, and existing processes to maintain business operations during disruptions.
3. Identifying Gaps: Through academic research, review of ISO standards, and discussions with industry professionals, DYNAMO aims to highlight gaps related to the integration of BCM, CTI, and resilience. It proposes definitions for these key terms, emphasizing essential crossovers in a resilience cycle and framework.
4. Simulation and Measurement: Agent-based simulations are expected to measure business/process resilience for various threats, evaluating mitigation and recovery strategies using state-of-the-art AI-based solutions.

5. Knowledge Generation: The results will generate knowledge about sector susceptibility, vulnerabilities, existing mitigation measures, and possibly define new measures to safeguard critical aspects of businesses.

The DYNAMO CTI approach involves identifying threats in the health, energy, and maritime sectors. It aims to provide timely, relevant, and actionable information on emerging threats, combined with the BCM approach. The platform collects, extracts, analyzes, and shares actionable CTI from both internal and external sources, contributing to an integrated Cyber Knowledge Graph for enhanced situational awareness.

The DYNAMO CTI suite includes tools for incident detection, predictive analytics, visualization, information sharing, and cyber security intelligence management. These tools contribute to a seamless flow from incident detection to response, improving organizations' ability to proactively address cyber threats and enhance their security posture.

2.3 Cybersecurity Information Sharing

The term ‘cybersecurity information sharing’ lacks a pervasive and widely agreed-upon definition, leading to sector-specific structures for information-sharing models in different environments [11]. A pressing need exists for a common early warning solution, particularly in the context of combating hybrid threats. This goes beyond merely preventing cyber-attacks; it involves the identification, tracing, and prosecution of criminals or criminal groups [12]. Consequently, there is a growing imperative for deeper integration of government systems, considering that the term "warning" encompasses preventive functions.

In the event of a major hybrid incident, pertinent information should be promptly shared with national Computer Emergency Response Teams (CERTs), followed by a coordinated response. The importance of combining information to ensure correct and reliable sharing cannot be overestimate in building cyber capacity. Shared information must be presented in an unambiguous and accessible format for all involved parties. Future cyber defense operations are anticipated to be more integrated and automated, aligning with local capabilities, authorities, and mission needs [13]. A shared common operational picture necessitates real-time communication links from the local level to the national and EU levels. This common cyber situational awareness is crucial for operating Cyber-Physical Systems (CPS) and emergency and crisis management [14]. Establishing a connection between cyber situational awareness and emergency management is imperative [15].

Furthermore, considerations should extend to how national Cyber Security Centers collaborate with other organizations within critical infrastructure at the national level. In the United States, various departments closely collaborate in combating cyber security threats. Within the European Union, public administration organizations cooperate on a formal basis as outlined in the Network and Information Security (NIS) directive and the Cyber Security Act.

While it might be argued that collaboration beyond EU borders could face challenges due to fundamental differences in administrative functions, there are indications to the contrary. Ilves et al. [16] suggest that there are no insurmountable barriers to increasing collaboration between the US, NATO, and the EU, especially concerning early warning solutions. Both the US Cybersecurity Sharing Act and Europe's NIS Directive share similar goals. Moreover, in 2016, the EU and NATO signed a technical arrangement to enhance information sharing between the NATO Computer Incident Response Capability and the EU Computer Emergency Response Team [17]. Public safety actors, such as European law enforcement agencies, require a shared situational picture for cross-border tasks, emphasizing the need for operational cooperation on a reliable platform [18].

3 Trust Building

The DYNAMO information-sharing model will be built on assumptions, including a clear governance model for intelligence data items (IDIs) [19], a process for onboarding and offboarding organizations, and the formation of clusters for information sharing based on sectoral or goal-related similarities. Trust is expected to be established through technical, organizational, and human means. The scope of data items is suggested to extend to Cyber-Physical Systems, acknowledging the interdependencies between physical and cyber domains. Translation and normalization services are proposed for standardizing IDIs, and existing standards for information processing and sharing are recommended for adoption.

Next, the creation of a trusted environment for cyber threat intelligence sharing is discussed from the perspective of four resilience domains:

1. physical and technology (HW&SW)
2. data/information/intelligence
3. human/social/organizational, and
4. cognitive decisions/situational awareness.

3.1 Physical and Technology Domain

The DYNAMO CTI platform is based on the modified hybrid model architecture for the ECHO Early Warning System (E-EWS) [19], which is based on case-by-case analysis and produces a balance between hierarchy and peering. This hybrid approach aims to facilitate information sharing among different hubs, representing sectors, interest groups, or national points. It emphasizes the importance of trust realms, creating a two-tier cross-organizational boundary structure. The governance model defines the policies, information security certification requirements, and the processes according to which organizations and individuals can join the EWS ecosystem. Trust realms control both how information is shared within their borders and how the more complex data management of external borders between different realms is implemented [11].

The management model of E-EWS is modular, the core of which includes a ticketing system for distributed workflow among partners. It emphasizes the need to enrich and contextualize information through a standard description and an extensible taxonomy of information. Table 1 presents the most important features of the governance of E-EWS.

The integration of trust-boosting security technologies, data redaction capabilities, and attribution features further underscores the commitment to security, privacy, and traceability. The allowance for anonymous information sharing, though marked and acknowledged for its potential impact on reliability, adds a layer of flexibility to accommodate various sources. The customizable exchange of intelligence data and predefined criteria for data dissemination ensure that the system can adapt to both internal and external requirements, providing a tailored and efficient experience for users [11].

Overall, the proposed features collectively contribute to the creation of a robust and adaptable Early Warning System, capable of fostering a collaborative and trusted environment for intelligence sharing among diverse stakeholders.

Table 1. E-EWS governance features

Feature	**Explanation**
Confidentiality Model:	Traffic Light Protocol (TLP) is applicable when defining intelligence targets so that sensitive information is shared appropriately. This model works alongside standard access control mechanisms.
Access Control Scheme:	A fine-grained access control system performs its tasks based on classifiers such as organizations, groups, and roles.
Support for Multiple Taxonomies:	The system supports different taxonomies and standards for intelligence sharing, allowing organizations from different fields to participate.
Structured Intelligence Data Sharing:	Possibility of structured sharing using standards such as Structured Threat Information eXpression (STIX).
Interoperability with Law Enforcement Agencies (LEAs):	The system facilitates the exchange of intelligence between computer emergency response teams (CERTs)/computer security incident response teams (CSIRTs) and LEAs using common terminology.
Common Data and Document Formats:	E-EWS supports widely used formats such as Word, PDF, and CSV, making it easy to share data.
Reliability Assessment:	E-EWS assesses the reliability of data sources based on technical capabilities or historical data of human intelligence sources.
Credibility Assessment:	E-EWS assesses the credibility of intelligence based on the verification levels of other sources, which include anti-fake news mechanisms.
Workflow Management System:	A shared case management system is one of the most important core functions of EWS to monitor efficiency and effectiveness.
Information Security Technologies that Increase Trust:	E-EWS supports closed communities and encrypted peer-to-peer communication to increase trust.
Data Redaction Capabilities:	Capability to redact personal information for privacy compliance, both automatically for structured data and semi-automatically for unstructured data.
Attribution Capabilities:	Identification of the origins of information sources for traceability.
Anonymous Information Sharing:	Despite attribution requirements, the system should allow for anonymous information, clearly marked as such, with an acknowledgment of the potential impact on reliability.
Customizable Exchange of Intelligence Data:	Allow customization based on internal or external requirements.
Predefined Criteria for Data Dissemination:	Criteria set for both the originator and consumer of information, considering factors like audience, trust realms, data versions, revisions, and severity.

3.2 Data Domain

Rajamäki and Katos [19] discuss the importance of intelligence data items (IDIs) in information sharing, especially in the context of cybersecurity. The DYNAMO platform will utilize this framework to manage the data lifecycle from data creation to its destruction. Chalkias et al. [11] highlight the handling of personal information in IDIs, emphasizing anonymization and redaction layers before leaving a tenant's area. Access control and information classification schemes are enforced at organizational boundaries. As participation and connectivity increase, the network's value is expected to follow Metcalfe's Law, but the potential increase in data volume necessitates effective filtering. The suggestion is to use contextual features, such as asset information, for efficient noise reduction, enhancing the overall effectiveness of information sharing [11].

The characteristics of IDIs are outlined, distinguishing between structured, semi-structured, and unstructured data, as well as reference and operational information [19]. Metadata accompanying IDIs is deemed essential for contextualization and implementing authorization and access control mechanisms. Table 2 provides a list of information categories and their expressions as IDIs, covering technical threat indicators, security alerts, vulnerability information, incident reports, and more.

3.3 Social Domain

The sharing of information is profoundly shaped by regulatory frameworks and cultural norms within specific sectors and organizations. In academia, for instance, the culture of academic freedom lowers barriers to sharing, driven by academic expression, peer review, and research dissemination. Conversely, critical sectors such as Energy and Banking experience stricter regulation, which is reflected in their organizational cultures. This dynamic creates a mosaic of regulatory frameworks and cultural influences at various levels [11]:

Table 1. Intelligence data items

Information category	**IDI**	**structured (S) / semi-structured (Semi) / unstructured (U)**	**reference/ operational**	**Personal Information**
Technical threat indicator	IOC (email, IP address, file hash, mutex, domain)	S	R	
Intrusion attempt	Threat Actor	S	O	X
	IOC (atomic, composite, behavioural)	S	O	
Security alert	Ticket	Semi	O	
	Readiness level	S	R/O	
Vulnerability information	CVE CVSS	S	R/O R/O O	
	Threat identification	S	R	
	Geopolitical	Semi	R	
	Exploitability	U		
		S		
Vulnerability report	Vulnerability scanning report	S	R	
Incident report	Report	U	O	?
TTP	ATT&CK	S	R/O	
	STIX object	S	R/O	
Remediation actions	Operating procedure	U	O	
	Playbook	U	O	
Asset	CPE to describe system platforms	S	R/O	
	CCE (common configuration enumeration)	S	R/O	
Discussion	Discussion item	U	R/O	?
Blog post	Reference	U	R/O	
Poll	Poll item	U	R/O	
Raw data	Log-file	S	O	
	Netflow	S	O	X
	Packet capture	Semi	O	X
	RAM image dump	Semi	O	X
	Malware sample	Semi	O	?
	VM Image	U	O	X
	File	U	R/O	X
	Email	U	R/O	

- Intra-Organizational Level: Influenced by internal policies and procedures.
- Intra-Sector Level: Dictated by sector-specific regulations.
- National-Governmental Level: Governed by strategic decisions at the national level.
- Transnational Level: Influenced by international agreements, treaties, and EU legislation, particularly for organizations within the EU, including frameworks for sharing information with Law Enforcement entities.

These levels are complemented by overarching legislation such as GDPR, applicable across all sectors. Considering the context of the EU initiative for a network of competency centers and the EWS supporting cross-sector information sharing, a hybrid model architecture is recommended. This model maintains a basic hierarchical structure while facilitating peer-to-peer connections between different hubs, aligning with CERTs' operational approach.

Figure 3 presents the hybrid model that permits some centralization, enabling centralized decision-making and the emergence of Coordination Centres [19]. Each hub can represent specific communities, such as sectors or interest groups, simplifying management and governance. This aligns with the EWS architecture, supporting seamless integration through sharing API capability.

From a governance perspective, this leads to trust realms that represent clusters of organizations (e.g., academic CERTs, national cyber security competency centers, maritime industry). Each realm can have multiple EWS instances for scalability and resilience, governed by policies and security certification requirements [19].

To join the EWS ecosystem, organizations go through a process where they are allocated a tenant that hosts all the data they provide. Trust realms facilitate information sharing within boundaries, defined by inner boundary data governance. Inter-realm sharing is governed by outer boundary data governance, a more complex and diverse process with a longer maturity period. Not all trust realms may connect, implying differing levels of authority and trustworthiness [11].

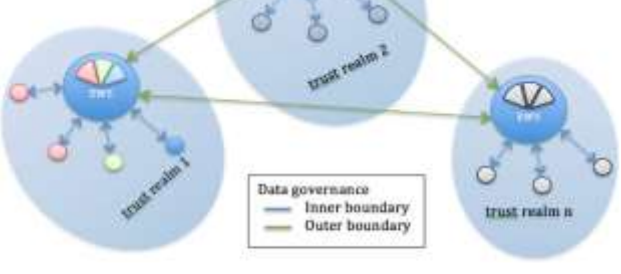

Fig. 3: Hybrid model information sharing (modified from [19]).

Personal information in IDIs undergoes anonymization and redaction before leaving a tenant's area. Information classification schemes, including access control, are enforced at both organizational and internal boundaries [19].

As participation and connectivity between hubs increase, the network's value is expected to follow Metcalfe's Law. However, to manage the potential influx of data, information sharing should incorporate not only access control criteria but also additional contextual features for effective filtering. When asset information is standardized using the Common Platform Enumeration (CPE) convention, irrelevant information can be filtered out and noise reduced [11].

3.4 Common Operational Picture and Shared Situational Awareness

The Observe – Orient – Decide – Act (OODA) loop emphasizes continuous improvement in iterative cycles that enable learning from past experiences. The OODA loop focuses on human aspects in crises and is commonly used in decision-making and cyber defense actions [20]. Zager and Zager [21] emphasize that the faster the OODA loop is completed, the better decisions can be made. They also propose models that can speed up decision-making processes and improve the quality of information synthesis. OODA loop plays an important role when building a common operational picture (COP) and shared situational awareness (SSA). Tikanmäki and Ruoslahti [21] emphasize the need for organizations to collect information about their environment so that they can understand environmental events and their effects on operations. The OODA loop, which is utilized as shown in Figure 4 in the ECHO project [22], provides a framework for cooperation to improve CSA.

The OODA loop in cyber defense involves gathering sensor information in the observation phase, analyzing it during orientation, choosing countermeasures and response activities in the decision phase, and implementing chosen actions in the action phase. The loop then begins a new cycle with a fresh observation phase. Tactical, operational, and strategic agility are essential for the OODA loop's decision cycle, as illustrated in Figure 4. Without OODA loops, organizations lack the ability

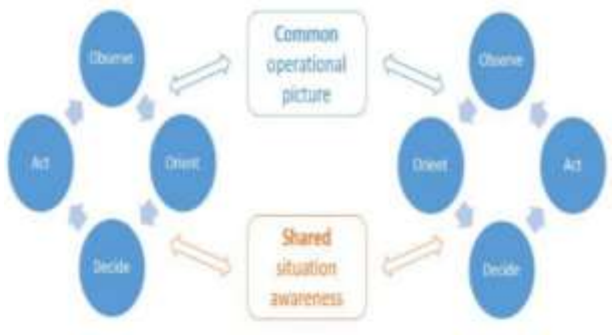

Fig. 4: Decision-making in complex environments.

to sense, observe, decide, and implement actions effectively in dynamic and uncertain environments [23].

4 Conclusion

Figure 5 summarizes the conclusions of this paper using the healthcare system as an example. The trust environment for cyber threat intelligence sharing consists of four levels. First of all, the data must be reliable and both technically and semantically compatible. Achieving this necessitates placing trust in the technology, encompassing both hardware and software components. The physical domain is usually the only domain explicitly modeled in most disaster-relief risk analysis models.

While the main focus of most cybersecurity risk analysis models is on explicitly modeling the technical domain, our research reveals an additional layer placed on social trust. Although knowledge and technology are unwaveringly trusted, facilitating the exchange of information is linked to the formation and maintenance of social trust. The central question that emerges is the means by which social trust can be implemented effectively. The answer, as elucidated through our exploration, lies in the cultivation of resilience. Resilience, the absolute prerequisite for overcoming the challenges posed in data exchange, is intricately tied to situational awareness. Within the framework of a cyber-physical system network, achieving resilience necessitates an overarching situational awareness that spans the entirety of the network. This, in turn, demands the existence of a Common Operational Picture and shared situational awareness.

The critical role played by a Common Situational Picture and Shared Situational Awareness in building resilience cannot be overstated. It forms the linchpin for seamless information exchange, relying on a set of indispensable conditions. Foremost among these conditions is the reliability of the technology employed, followed closely by the quality and semantic coherence of the shared information.

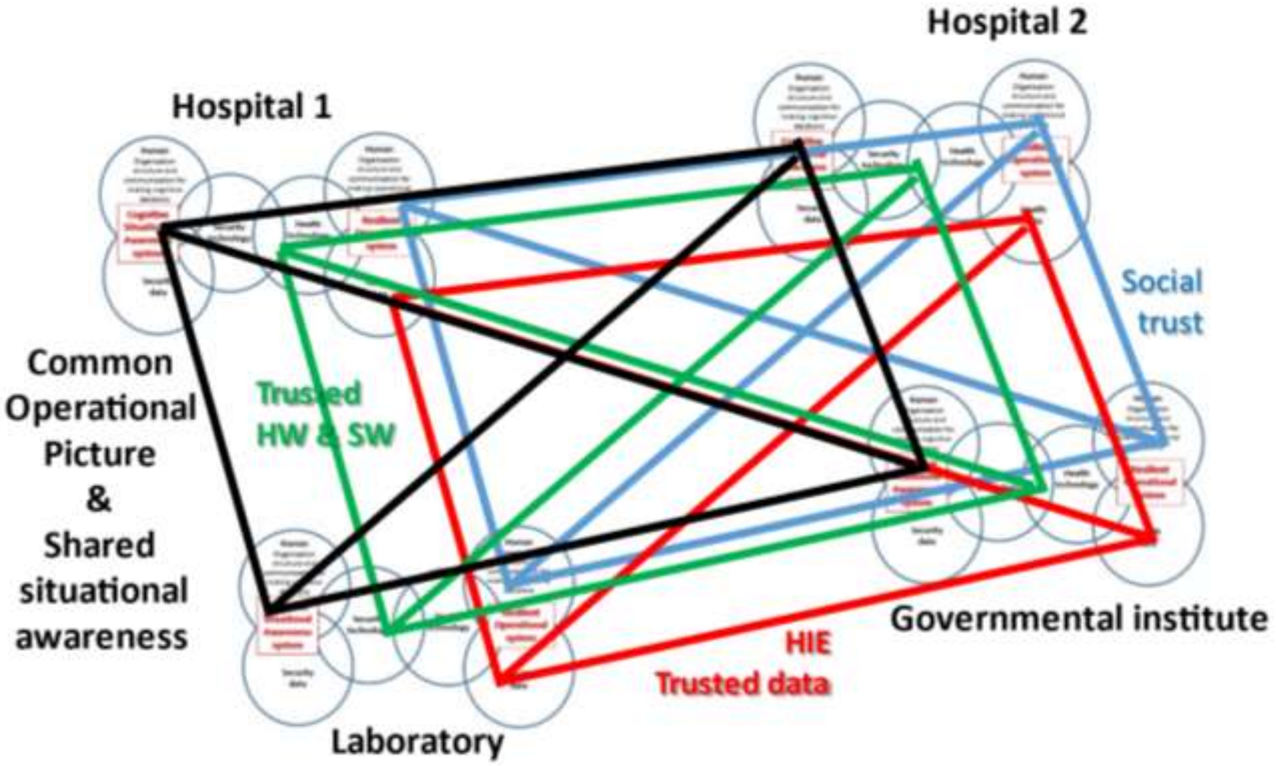

Fig. 5: Trust dimensions of critical eHealth infrastructure.

Equally crucial is the establishment of social trust, a pivotal factor operating at both organizational and individual levels.

In the complex interplay of various cyber-physical systems dependent on one another, the establishment of a Common Situational Picture and Shared Situational Awareness necessitates the integration of artificial intelligence and machine learning. This, in turn, requires further research of the kind that is being done, among others, in the DYNAMO project, which integrates artificial intelligence-based solutions to accelerate recovery behavior (recovery) for the health, marine, and energy sectors. These technologies emerge as indispensable tools, orchestrating the orchestration of a resilient network that effectively navigates the challenges inherent in information exchange within disaster-relief risk analysis models. As we venture into an era of heightened interconnectivity, these conclusions underscore the multifaceted nature of trust, resilience, and technological innovation in ensuring the efficacy of data exchange mechanisms in critical domains.

Acknowledgement:
This work was supported by the DYNAMO project, which has received funding from the European Union’s Horizon Europe research and innovation funding programme under the grant agreement no. 101069601.

References:

[1] J. Rajamäki, "Towards a Design Theory for Resilient (Sociotechnical, Cyber-Physical, Software-intensive and Systems of) Systems," *WSEAS Transactions on Computers*, vol. 20, pp. 97-102, 2022.

[2] T. Edgar and D. Manz, *Research Methods for Cyber Security*, Cambridge, MA: Elsevier, 2017.

[3] D. Alberts and R. E. Hayes, "Power to the Edge: Command Control in the Information Age," Command and Control Research Program, Washington, DC, 2003.

[4] DIMECC, "The Finnish Cyber Trust Program 2015–2017," DIMECC, Tampere, 2017.

[5] DYNAMO, "DYNAMO homepage," 2023. [Online]. Available: https://horizon-dynamo.eu/. [Accessed 11 10 2023].

[6] C. Ehlschlaeger, J. Burkhalter, I. Chiu, I. Linkov, J. Cegan, O. David, Y. Ouyang, J. Parker, F. Serafin, D. Morrison, J. Westervelt, L. Lu, J. Palacio, D. Patterson, T. Perkins, A. Petit and Y. Liu, "Resilience Modeling for Civil Military Operations with the Framework Incorporating Complex Uncertainty Systems," The US Army Engineer Research and Development Center (ERDC), Washington, DC, 2023.

[7] I. Linkov, D. Eisenberg, K. Plourde, T. Seager, J. Allen and J. Kott, "Resilience metrics for cyber systems," *Environ Syst Decis*, 2013.

[8] D. Prochazkova and J. Prochazka, "Tool for Determination of Risk for Risk-Based Operation of Socio-Cyber-Physical Systems. Applications in Engineering Education," *WSEAS Transactions on Advances in Engineering Education*, vol. 18, no. 8, pp. 58-79, 2021.

[9] J. Rajamäki, N. Chaulagain, M. Kukkonen, P. Nurmi, M. Honkonen, S. Saarinen and T. Kinnunen, "Improving the Cybersecurity Awareness of Finnish Podiatry SMEs," *WSEAS Transactions on Computers*, vol. 22, pp. 198-205, 2023.

[10] E. Hytönen, J. Rajamäki and H. Ruoslahti, "Managing Variable Cyber Environments with Organizational Foresight and Resilience Thinking," *International Conference on Cyber Warfare and Security*, vol. 18, no. 1, pp. 162-170, 2023.

[11] I. Chalkias, C. Yucel, D. Mallis, J. Rajamaki, F. De Vecchis, P. Hagstrom and V. Katos, "An Empirical Evaluation of Cyber Threat Intelligence Sharing in the ECHO Early Warning System," in *T. Tagarev and N. Stoianov (Eds.) Digital Transformation, Cyber Security and Resilience, DIGILIENCE 2020*, Cham, Springer Nature Switzerland, 2023, p. 23–40.

[12] K. Wang, M. Du, Y. Sun, A. Vinel and Y. Zhang, "Attack detection and distributed forensics in machine-to-machine networks," *IEEE Network*, vol. 30, no. 6, p. 49–55, 2016.

[13] V. Li, M. Dunn, P. Pearce, D. McCoy, G. Voelker and S. Savage, "Reading the tea leaves: a comparative analysis of threat intelligence," *28th USENIX security symposium*, pp. 851-868, 2019.

[14] E. Burger, M. Goodman, P. Kampanakis and K. Zhu, "Taxonomy model for cyber threat intelligence information exchange technologies," *2014 ACM Workshop on Information Sharing and Collaborative Security*, pp. 51-60, 2014.

[15] H. Kaufmann, R. Hutter, F. Skopik and M. Mantere, "A structural design for a pan-European early warning system for critical infrastructures," *Elektrotechnik und Informationstechnik,* vol. 132, no. 2, p. 117–121, 2015.

[16] L. Ilves, T. Evans, F. Cilluffo and A. Nadeau, "European Union and NATO global cybersecurity challenges: a way forward," *PRISM*, vol. 6, no. 2, pp. 126-141, 2016.

[17] European Council, "EU Cyber Defence Policy Framework," Council of the European Union, Brussels, 2018.

[18] ENISA, Europol/EC3, "Common Taxonomy for Law Enforcement and The National Network of CSIRTs," Europol, 2017.

[19] J. Rajamäki and V. Katos, "Information Sharing Models for Early Warning Systems of Cybersecurity Intelligence," *Information & Security: An International Journal*, vol. 46, no. 2, pp. 198-214, 2020.

[20] T. Pahi, M. Leitner and F. Skopik, "Analysis and Assessment of Situational Awareness Models for National Cyber Security Centers," *ICISSP*, pp. 334-345, 2017.

[21] I. Tikanmäki and H. Ruoslahti, "How Are Situation Picture, Situation Awareness, and Situation Understanding Discussed in Recent Scholarly Literature?" *11th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management,* pp. 419-426, 2019.

[22] ECHO, "ECHO - Home," 2022. [Online]. Available: https://echonetwork.eu/. [Accessed 13 Nov. 2023].

[23] J. R. Boyd, "The essence of winning and losing," *Unpublished lecture notes*, vol. 12, no. 23, pp. 123-125, 1996.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

This work was supported by the DYNAMO project, which has received funding from European Union's Horizon Europe research and innovation funding programme under the grant agreement no. 101069601.

Conflict of Interest

The authors have no conflicts of interest to declare that are relevant to the content of this article.

Creative Commons Attribution License 4.0 (Attribution 4.0 International, CC BY 4.0)