The Social Domain: Resilience of Information-Sharing Networks

Harri Ruoslahti [1] and Ilkka Tikanmäki [1, 2]

[1] Security and Risk Management, Laurea University of Applied Sciences, Espoo, Finland

[2] Department of Warfare, National Defence University, Helsinki, Finland

https://orcid.org/ 0000-0001-9726-7956

https://orcid.org/0000- 0001-8950-5221

Harri.ruoslahti@laurea.fi
Ilkka.tikanmaki@laurea.fi

Abstract: The concept of networks in the social domain can be seen as a resilient complex social system, consisting of diverse and interdependent actors and organizations. These social networks are characterized by complicated interactions between people, technologies, and processes, making them cyber-physical or socio-technical in nature. However, these interactions and dependencies also bring vulnerabilities, encouraging member organizations to increase their resiliency. As organizations and digital structures become increasingly interconnected, there is a need for information sharing, and practices that anticipate future incidents and foster learning from them. Effective communication with stakeholders is essential to strengthening resilience, given the diverse interests and interdependencies between them. An integral system's perspective on an organisation in its environment emphasises relationships and interdependencies, enabling recognition of complexities to enhance resilience on various interrelated levels. Identifying trends and implementing preventive measures requires the sharing of information on threats and vulnerabilities. Open innovation, where outsiders contribute to co-creating innovations, can help organizations cope with unforeseen disruptive changes. Agility is essential for developing knowledge and adapting processes flexibly to changing contexts. Knowledge exchange between network stakeholders can reduce the complexity of communication and enable resilient collaboration. In this case study, the researchers offer a tool that is aimed at strengthening the resilience of collaborative networks by gaining a deeper understanding of each organisation's relevant processes and tools. They specifically focused on analysing and evaluating the effects of these processes on the safety of critical infrastructure. To enhance the sustainability of stakeholder collaborative networks, master's students in safety management conducted risk assessment workshops and compiled a list of characteristics. These attributes were then prioritised and incorporated into risk matrices. The results of the study revealed the key factors that contribute most significantly to the resilience of collaboration networks. These findings highlight the critical aspects that influence the resilience of collaborative networks. By incorporating these factors into their strategies and practices, organisations and stakeholders can enhance their ability to withstand disruptions and adapt effectively in the face of uncertainties.

Keywords: Networks, Collaboration, Resilience, Risk Assessment

1. Introduction

Networks in the social domain (Linkov et al., 2013) can be looked at through the lens of resilient complex social systems, as networks are organisational environments that consist of diverse interdependent actors, organisations can be understood as complex social systems (Mitleton-Kelly, 2003). This study is based on the action research-based case study continuum carried out in three EU-funded projects: European Network of Cybersecurity Centres and Competence Hub for Innovation and Operations (ECHO), Smart and Healthy Ageing through People Engaging in Supportive Systems (SHAPES), and Dynamic Resilience Assessment Method including a combined Business Continuity Management and Cyber Threat Intelligence solution for Critical Sectors (DYNAMO).

Project ECHO developed and delivered an organized coordinated, effective and efficient multi-sector collaboration-based approach to help strengthen the proactive cyber defences of the European Union (Pappalardo et al., 2020). The SHAPES project gathered stakeholders from across Europe to create, deploy and pilot at large-scale networked EU-wide harmonized open platforms to integrate broad ranges of technological, organizational, clinical, educational, and societal solutions. The aim is to enable ageing Europeans to remain healthy, active and productive while maintaining a high quality of life and sense of well-being for the longest time possible (Rajamäki and Ruoslahti, 2021). The project DYNAMO deals with increasing digitalisation and mounting potential of cyber threats, where networked experts work together with end-users to develop a single platform where artificial intelligence-based (AI) approaches combine business continuity management (BCM) and cyber threat intelligence (CTI) for resilience assessment and awareness to minimize the number of cyberattacks against the critical sectors of society (DYNAMO project, 2023).

Networked SHAPES technologies and systems include many complex interactions between people, technologies and processes, and can be considered cyber-physical (Linkov et al., 2013; Rajamäki and Ruoslahti, 2018) or socio-technical (Amir and Kant, 2018). Interactions and interdependencies between complex social networks, such as the SHAPES-networks, come with vulnerabilities, come with vulnerabilities, so their member organisations work to increase their resilience. “Nowadays, there is a tight coupling of systems and processes, and there are many interdependencies between these systems and processes” (Vos, 2017, p. 23).

Due to the entanglement of human organisations, and digital and material structures, vulnerabilities within socio-technical systems that combine human and technical aspects have increased, resulting in a need to develop practices that anticipate possible future incidents and provide feedback to learn from (Amir and Kant, 2018; Linkov et al., 2014). Communication in the turbulent times of today is “co-constructed by multiple stakeholders characterised by different interests and various interdependencies” (Vos, 2017, p. 13), and communication with stakeholders is important in building resilience (Linkov et al., 2014). Agility can help develop the knowledge needed for resilient collaboration, and to flexibly adapt needed processes to changing contexts (Ruoslahti et al., 2018). Understanding an integral system’s view of an organisation in its environment emphasises relationships and interdependencies (Grunig et al., 1992), which enables the recognition of complexities to increase resilience on different interrelated levels, and across boundaries, as societal resilience is built together by the different actors (Vos, 2017).

Sharing information on threats and vulnerabilities “help identify trends, better understand the risk faced, and determine what preventive measures should be implemented” (Stanciugelu et al., 2013, p. 194). Open innovation, where outsiders are invited to co-create innovations can be one way of assisting to deal with unforeseen disruptive changes in volatile environments of the organisation and network (Pichyangkul et al., 2012). Agility is needed to develop the knowledge needed to flexibly adapt processes to changing contexts, and gaps and complexity in communicating existing knowledge can be reduced by exchanging knowledge among network actors for collaboration to function in a resilient way (do Nascimento Souto, 2013).

The research question of this paper is: How to measure the resilience of services networks?

This paper is organized as follows: Section 2 deals with literature on cybersecurity of eHealth platforms, security validation requirements for eHealth services, and ECHO efforts in the healthcare sector and cyber range (E-FCR). Section 3 outlines the used methods. Section 4 presents a tool for measurable attributes of resilience in collaboration networks. Section 5 concludes the paper and suggests possibilities for future work.

2. Literature Review

The framework of organizational resilience creates tools and conditions to help understand issues, reduce risks, and mitigate crises: “Resilience requires cooperation and adaptive capacities” (Vos, 2017, p. 20), which can be used to create tools or conditions to help organizations co-evolve with their constantly changing environments (Mitleton-Kelly, 2003). Innovation eco-systems where different types of actors build contexts for innovation build resilience with knowledge development that addresses vulnerabilities and risks that may spread within the system (Hautamäki, 2010; Oksanen and Hautamäki, 2014). Organizational resilience helps create tools and conditions for risk reduction, mitigation of crises, and understanding issues (Vos, 2017).

According to (Linkov et al., 2014) risks occur when threat, vulnerability and consequences for critical functionalities coincide. Organisations work to identify these elements in their risk assessments during when planning and preparing for possible disruptions. Organisations, and collaboration networks alike, require preparation and a process to update recovery plans (Savage, 2002). Robust business processes, keeping plans constantly updated and tested, and learning from actual experiences help prepare for possible disturbances (Draheim and Pirinen, 2011). Resilience management with transparent dialogue help network actors accept, promote, and maintain resilience concepts (Linkov et al., 2014). “Co-creation clearly requires alignment of vision and supporting processes, and the development of advanced inter-organisational collaboration skills” (Burdon et al., 2015, p. 296).To promote resilience calls for “awareness, leadership, resource allocation, and planning” (O’Rourke and Briggs, 2007, p. 26) and shared responsibility and situational intelligence (Pirinen, 2017).

(Vos, 2017, p. 23) states that the concept of resilience is about “coping with change and managing the unexpected” when functioning in turbulent environments. (Ruoslahti, 2019) discusses resilience in complex social networks as important elements, which helps understand how these networks seek to reduce risks and mitigate crises on the level of social network collaboration, and how they adapt the process of joint knowledge creation in a changing environment. Today’s changing organisational environments are complex and filled with interrelated risks (Linkov et al., 2013; Mitleton-Kelly, 2003; Vos, 2017) which can also be said for collaboration networks. SHAPES-networks are organizational environments that consist of diverse interdependent actors, organizations they can be understood as complex social systems (Mitleton-Kelly, 2003).

Critical infrastructure provides citizens with essential services and supports our economies. It is therefore in everyone's interest to prevent disturbances from occurring. Critical energy infrastructure and supply chains' safety are vital for society's functioning; therefore, it is crucial to ensure their safety. Energy infrastructure is networked, so disturbances at one location can affect the rest of the region, and information on its location and routing is publicly accessible. To build resilience and be prepared to manage disruptions, organizations need to work together in a complementary and mutually reinforcing way (NATO-EU Task Force, 2023).

2.1 Collaboration Networks – Information Sharing in the Social Domain

(Tikanmäki et al., 2022) studied maritime surveillance and information sharing systems that help build better situational awareness on the European maritime domain. Digital transformation, such as are the SHAPES networks call for an added level of cyber security and increased resilience in modern societies. This study looked at different forms of collaboration networks, which can be decentralized, hybrid, and centralized.

Table 1: SWOT analysis of different network types (Tikanmäki et al., 2022).

Decentralized Networks		Hybrid Networks		Centralized Networks	
Strengths	Weaknesses	Strengths	Weaknesses	Strengths	Weaknesses
Cross sector actors Cross border actors Available information Area coverage	Access rights to the available information Network complexity Management Costs	Collaboration between large-scale, cross-sector, cross-border, and local operators	Trust, as to what will be done with information shared Ownership of information Potentially complex access rights	Security Easy access rights Existing co-operation Trust between partners Common interests ease information sharing Effective information	Shared information focused on limited geographical area Costly Political blocks Information from outside networks can not be shared
Opportunities	Threats	Opportunities	Threats	Opportunities	Threats
Potential of cross border collaboration Potential of cross sector collaboration Potential tools to mitigate risks	Cyber attacks Consortium collapse when not seen being beneficial Trust, as to what will be done with information shared	Geographical consortiums can utilize different solutions	Network security against cyber attacks Political obstacles	Connectivity to other networks	Political blocks

The advantages of different network designs depend on their use, as demonstrated in the SWOT table above. Authorities and actors from a geographically wider area can form the coalition in decentralized networks than in centralized networks (such as the European Union or the European Economic Area). The hybrid network is constructed based on the partners' interests, emphasizing a broader area than a specific geographical area. It enables the creation of a comprehensive Common Operational Picture (COP) between industries, cross-border players, and local players. Centralized networks, on the other hand, are a substitute for consortia formed by national authorities and actors that are restricted to specific geographical areas.

2.2 Attributes to Improve the Resilience of Collaboration Networks

Attributes to improve the resilience of collaboration networks (Rajamäki and Ruoslahti, 2018; Ruoslahti et al., 2018) can help toward greater resilience of multi-stakeholder collaboration networks, these attributes were then prioritized and placed in risk matrixes. The main characteristics are summarised in Table 2.

Table 2: Attributes that can improve resilience in collaboration networks.

Attributes of resilience in collaboration networks
Co-create a clear purpose and common aims for the network
Agree on organization and roles within the network
Create a common culture and common ways of working among network stakeholders
Develop leadership within the network
Facilitate collaboration and co-creation in the network
Develop systems to back up or exchange network stakeholder representatives
Build trust among the stakeholders of the network
Have open communication, sharing information with every network stakeholder

As Table 2 demonstrates, these are clear attributes that a network can manage to bring resilience to its social domain. A clear goal is the starting point for agreement on roles and establishing common methods of operating. Leadership and facilitation are necessary, and these roles must also be accepted by those involved in the networks. It is important to develop a backup system for representatives both regarding open communication and enhancing trust among stakeholders.

A social network's resilience depends on the network having a clear purpose and common objectives. The preparatory stage on the work of strategy depends on resulting in common aims and ways of working. Stakeholders must work on the development of guidance plans and standards, agree on clear roles and responsibilities, and identify and reconcile individual and general user requirements. Where the need recognizes the effects of potential adverse events, the level of acceptance of the roles and responsibilities of each stakeholder group emerges.

A common operational culture also has the flexibility to succeed in changing circumstances. A recovery towards jointly agreed objectives is necessary to enable full standardisation of services and operations. The adjustment phase should include an open analysis of the actions undertaken and the utility of the instructions and actions provided. Educated decision-making requires information and a situational picture of the operating environment. In addition, a resilient social network also demonstrates leadership and facilitation.

The planning phase should have a comprehensive risk management process, with input from the views of each stakeholder. In the aftermath of the event, crisis management is pivotal. A clear picture of the situation makes it possible to envisage possible environmental modifications. Leadership should concentrate on the most critical element required to recover from the incident and prioritize the activities of the network. Monitoring and reporting help to gather the necessary information for learning from the experiences of both your own organization and other organizations in the network. It was concluded that the leadership and coordination of the network should not be too undefined or over-controlling.

Security for information sharing both cyber and physical is also necessary. The aspects of this are the related documentation and stand-in procedures in the event of a representative is not present and deal with staff changes. A clear system needs to be put in place to mitigate the impact of possible absences and changes in stakeholder representation. Timely and efficient communication and exchange of information contributes to increased trust among stakeholders. The conclusion was that trust should exist between the representatives of the stakeholders and the organizations.

In addition, the participants stated that major changes in the operational environment, such as rapid technological development and scheduling and cost challenges may call into question the sustainability and cooperation processes of the network at risk. Open communication during the preparatory phase is linked to the management of communication before the crisis (Vos et al., 2014), whereas after the event the interaction is transformed into crisis communication (Palttala and Vos, 2012). In the recovery phase, emphasis is placed on communication issues.

2.3 Competence Management – Basis for Information Sharing

Competence management is how organizations deal with the competence of enterprises, groups, and individuals. The purpose of which is to define and permanently maintain competence in line with the objectives of the enterprise (Berio and Harzallah, 2005). EU define competence as "a combination of knowledge, skills and attitudes appropriate to the context" (European Parliament and the Council, 2006, p. 16). Competence is part of human capital, which includes e.g., the level of education of the personnel and the measured competencies, job satisfaction and state of health (Lepak and Snell, 1999).

To meet an organization's perceived needs for expertise, individuals should acquire the knowledge and skills necessary, which help successful integration of expert community members to research and development processes. To be transformed into organizational know-how information must be acquired, understood, internalized, and shared within the community (Eisenberger et al., 2016). The competences of an organisation's personnel, consisting of practices, processes or systems that store and accumulate new know-how, forms a common knowledge base for an entire company (Fagerberg et al., 2012).

Meetings, training sessions, group work, etc. can be used to share information. When the information becomes understood at the organizational level, the suitability of the information for practice can be tested for organizational learning. It can become reflected in the structures and practices of the organization and its written instructions (Levitt and March, 1988). On the report of (Otala et al., 2004) strategic competences can be determined by identifying strategic starting points, required competencies and capabilities, future competence needs and drawing up competence profiles, so that the work community and organization form a network that supports learning.

Defining a vision, strategy, core competencies, and competence development needs can locate the differences between the current situation and the competence needs, and a development plan helps target, implement, and monitor the measures; monitoring and evaluating development measures can support management guide the organizational operations and make a follow-up plan for competence development (Bergenhenegouwen, 1996). Creating student-expert alliances can connect science, culture, and experts with work life activities to create learning environments together (Westermann, 2011). The collective individual competences of the personnel accumulate organizational competence, which can form permanent and secure organizational knowledge capital, not just the competence of individuals (Hakanen and Soudunsaari, 2012).

The emergence of innovations is influenced by strong links between actors, as well as by the essential new knowledge brought by beginners, which develops and deepens community activities (Ojasalo, 2012). Knowledge and information are shared in an open atmosphere, symmetrically through and between both old professionals and newcomers provides support to competence management in changing the way an organization operates, and the emergence of know-how because of work life cooperation to be key (Wan et al., 2020). Management practices should support and enable radical, collective learning (Kallio and Lappalainen, 2015).

3. Methodology

The purpose of the case study is to provide detailed case study information in support of development activities. The more the research questions aim to explain some current situation, e.g., how, or why, the more relevant the case study method in question is. The method is especially relevant as questions require a wide and thorough description of certain social phenomena. Case studies are used in a variety of situations to increase information on individual, collective, organisational, socio-political, and affiliated issues (Benbasat et al., 1987; Dubé and Pare, 2003; Yin, 2009). A case study is a suitable approach when producing a solution to a specific problem or making suggestions for research development (Yin, 2009).

This study is a multiple case study based on the action research-based case study continuum carried out in the projects 1) ECHO, 2) SHAPES, and 3) DYNAMO using the attributes to improve the resilience of collaboration networks, and collaborative information sharing systems for situational awareness.

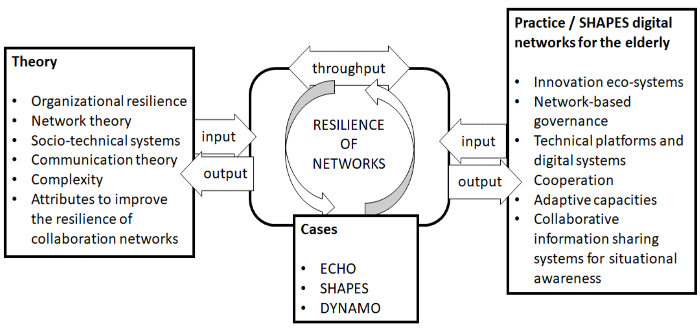

Figure 1: The structure of this case study research.

The theoretical inputs are organizational resilience, network theory, socio-technical systems, communication, complexity, and theoretical attributes to improve the resilience of collaboration networks. Practical inputs are innovation eco-systems, governance of networks, platforms, cooperation, adaptive capacities, and collaborative information sharing systems for situational awareness. The throughput is a continuum of action research involving three different case projects (ECHO, SHAPES, DYNAMO) to create a piloted practical tool to measure relevant attributes of the resilience of networked activities.

4. Results: Attributes of Collaboration Network Resilience

Understanding how resilience becomes built in SHAPES collaboration networks can guide SHAPES governance and direct their strategy work resulting in common aims and common ways of working and a common operational culture which can ensure needed flexibility to successfully face changing situations. This can be achieved with the attributes of resilience (Rajamäki and Ruoslahti, 2018; Ruoslahti et al., 2018).

By applying a Likert-scale a template (Table 3) can be formed that can be used to assess the state of collaboration network resilience within any specific SHAPES network, and even the entire network of SHAPES networks. Each attribute can be assessed as frequency answering the question 'How often does this attribute occur in our SHAPES network; never, rarely, sometimes, often, or always?'

Table 3: Attributes of collaboration network resilience assessed as frequency (Never = 1, Rarely = 2, Sometimes = 3, Often = 4, Always = 5).

Attribute	1	2	3	4	5
Does our network co-create a clear purpose for the network					
Does our network co-create common aims for the network					
Agree on organisation within the network					
Agree on roles within the network					
Create a common culture of working among network stakeholders					
Create common ways of working among network stakeholders					
Develop leadership within the network					
Facilitate the collaboration in the network					
Facilitate co-creation in the network					
Develop systems to back-up network stakeholder representatives					
Develop systems to exchange network stakeholder representatives					
Build trust among the stakeholders of the network					
Have open communication with every network stakeholder					
Have sharing information with every network stakeholder					

Understanding these attributes can provide understanding of how resilience can be built within each SHAPES Data Value Network. This understanding can help guide the design of governance for each SHAPES network, and for the system of SHAPES network systems. Intensive interaction among the many diverse actors of the network enhances relationships and trust so that common problems can be defined collaboratively so that all network partners are motivated to solve them together. To ensure continuity in the collaboration and co-creation of a network, both vulnerabilities and interdependencies are considered by agile communication. This helps in addressing any potential disruptions to network interactions.

Carefully considering these attributes can be done as a group, which can promote open communication and sharing of information. This in turn can build purpose and common aims, as well as trust among the stakeholders of for the network. These facilitate collaboration and agreement on organization and roles within SHAPES data value networks, and to develop leadership, common culture, and ways of working in them.

5. Conclusions

Resilience can be strengthened through a deeper understanding of the relevant processes and tools that each organization uses and by analysing and evaluating the effects on the safety of critical infrastructure. Master's students in safety management conducted risk assessment workshops and compiled a list of characteristics to enhance the sustainability of stakeholder collaborative networks. In this case study, the students aimed to enhance the resilience of collaborative networks by gaining a more thorough understanding of the processes and tools employed by each organization. Their primary focus was to analyse and evaluate the effects of these processes on the safety of critical infrastructure. These attributes were then prioritized and embedded in the risk matrix.

The results show the resilience of collaboration networks as the most important factors are presented in the following Table 4.

Table 4: Cybersecurity themes and their key features

Attribute	Definition
Clear purpose and common objectives	Having a well-defined purpose and shared objectives among network participants.
Roles and responsibilities of stakeholders	Clearly defining the roles and responsibilities of each stakeholder within the network.
Common operational culture	Fostering a cohesive and unified operational culture across the network.
Leadership and coordination defined	Establishing effective leadership and coordination mechanisms within the collaborative network.
Collaboration and co-creation facilitated	Encouraging and enabling collaboration and co-creation among the stakeholders.
Systems back-up Development	Implementing systems back-up measures to ensure continuity in case of disruptions.
Trust building between stakeholders	Building and maintaining trust among all network stakeholders.
Open communication in information sharing	Promoting open and transparent communication for efficient information sharing.

The findings of the study highlighted the main contributes to the resilience of collaborative networks. Organizations and stakeholders can enhance their ability to withstand disruptions and adapt effectively in the face of uncertainties by incorporating these factors into their strategies and practices.

The practical contribution of this study is a tool to measure relevant attributes of the resilience of networked activities. This tool will be tested and further developed in project DYNAMO where networked experts collaborate with end-users to develop the DYNAMO-platform that will combine business continuity management (BCM) and cyber threat intelligence (CTI). The contribution to theory is a deeper understanding of how the attributes of resilience in networks can help increase the continuity of their collaboration. The economic impacts of such networks as a basis to focus on resilience is an interesting direction for further studies, which could include a review of literature on collaborative networks from a business context.

Acknowledgements

This study has received funding by the European Union projects ECHO, which has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement no. 830943, and DYNAMO, under grant agreement no. 101069601. The views expressed are those of the author(s) 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

Amir, S., Kant, V., 2018. Sociotechnical Resilience: A Preliminary Concept. Risk Analysis 38, 8–16. https://doi.org/10.1111/risa.12816

Benbasat, I., Goldstein, D.K., Mead, M., 1987. The Case Research Strategy in Studies of Information Systems. MIS Quarterly 11, 369–386. https://doi.org/10.2307/248684

Bergenhenegouwen, G.J., 1996. Competence development - a challenge for HRM professionals: core competences of organizations as guidelines for the development of employees. Journal of European Industrial Training 20, 29–35. https://doi.org/10.1108/03090599610150282

Berio, G., Harzallah, M., 2005. Knowledge Management for Competence Management. J.UKM 0, 21–28.

Burdon, S., Mooney, G.R., Al-Kilidar, H., 2015. Navigating service sector innovation using co-creation partnerships. Journal of Service Theory and Practice 25, 285–303.

do Nascimento Souto, P.C., 2013. Beyond knowledge, towards knowing: the practice-based approach to support knowledge creation, communication, and use for innovation. RAI Revista de Administração e Inovação 10, 51–79.

Draheim, D., Pirinen, R., 2011. Towards exploiting social software for business continuity management, in: 22nd International Workshop on Database and Expert Systems Applications. IEEE, pp. 279–283.

Dubé, L., Pare, G., 2003. Rigor In Information Systems Positivist Case Research: Current Practices, Trends, and Recommendations. MIS Quarterly 27, 597–635. https://doi.org/10.2307/30036550

DYNAMO project, 2023. Dynamic Resilience Assessment Method [WWW Document]. URL https://horizon-dynamo.eu/wp-content/uploads/2023/01/DYNAMO_Leaflet_web.pdf (accessed 1.24.24).

Eisenberger, R., Malone, G.P., Presson, W.D., 2016. Optimizing Perceived Organizational Support to Enhance Employee Engagement.

European Parliament and the Council, 2006. Recommendation of the European Parliament and of the Council of 18 December 2006 on key competences for lifelong learning. Official Journal of the European Union L394/310, 19.

Fagerberg, J., Fosaas, M., Sapprasert, K., 2012. Innovation: Exploring the knowledge base. Research Policy, Exploring the Emerging Knowledge Base of "The Knowledge Society" 41, 1132–1153. https://doi.org/10.1016/j.respol.2012.03.008

Grunig, L.A., Grunig, J.E., Ehling, W.P., 1992. What is an effective organization?, in: Excellence in Public Relations and Communication Management. Routledge, New York, p. 26.

Hakanen, M., Soudunsaari, A., 2012. Building Trust in High-Performing Teams. Technology Innovation Management Review 2, 38–41. https://doi.org/10.22215/timreview/567

Hautamäki, A., 2010. Sustainable innovation: a new age of innovation and Finland's innovation policy. Sitra.

Kallio, K., Lappalainen, I., 2015. Organizational learning in an innovation network: Enhancing the agency of public service organizations. Journal of Service Theory and Practice 25, 140–161. https://doi.org/10.1108/JSTP-09-2013-0198

Lepak, D.P., Snell, S.A., 1999. The Human Resource Architecture: Toward a Theory of Human Capital Allocation and Development. AMR 24, 31–48. https://doi.org/10.5465/amr.1999.1580439

Levitt, B., March, J.G., 1988. Organizational Learning. Annual Review of Sociology 14, 319–340.

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, 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.

Mitleton-Kelly, E., 2003. Ten principles of complexity and enabling infrastructures, in: Complex Systems and Evolutionary Perspectives on Organisations: The Application of Complexity Theory to Organisations. Pergamon, An Imprint of Elsevier Science, London UK, pp. 23–50.

NATO-EU Task Force, 2023. EU-NATO Task Force on the Resilience of Critical Infrastructure (Final Assessment Report). NATO-EU Task Force.

Ojasalo, J., 2012. Challenges of Innovation Networks: Empirical Findings. International Journal of Management Cases 14, 6–17.

Oksanen, K., Hautamäki, A., 2014. Transforming regions into innovation ecosystems: A model for renewing local industrial structures. The Innovation Journal 19, 16.

O'Rourke, T.D., Briggs, T.R., 2007. Critical Infrastructure, Interdependencies, and Resilience. The Bridge 22–29.

Otala, L., Jaskari, J., Vartiainen, M. (Eds.), 2004. Oppivien organisaatioiden tunnuspiirteet. Helsinki University of Technology, Department of Industrial Engineering and Management, Espoo.

Palttala, P., Vos, M., 2012. Quality Indicators for Crisis Communication to Support Emergency Management by Public Authorities. Journal of Contingencies and Crisis Management 20, 39–51. https://doi.org/10.1111/j.1468-5973.2011.00654.x

Pappalardo, S.M., Niemiec, M., Bozhilova, M., Stoianov, N., Dziech, A., Stiller, B., 2020. Multi-sector Assessment Framework – a New Approach to Analyse Cybersecurity Challenges and Opportunities, in: Dziech, A., Mees, W., Czyżewski, A. (Eds.), Multimedia Communications, Services and Security, Communications in Computer and Information Science. Springer International Publishing, Cham, pp. 1–15. https://doi.org/10.1007/978-3-030-59000-0_1

Pichyangkul, C., Nuttavuthisit, K., Israsena, P., 2012. Co-creation at the front-end: a systematic process for radical innovation. International Journal of Innovation, Management and Technology 3, 121–127.

Pirinen, R., 2017. Towards Common Information Systems Maturity Validation : Resilience Readiness Levels (ResRL), in: In Proceedings of the 9th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management. Science and Technology Publications, pp. 259–266. https://doi.org/10.5220/0006450802590266

Rajamäki, J., Ruoslahti, H., 2021. ECHO Federated Cyber Range as a Tool for Validating SHAPES Services, in: Proceeding of the 20th European Conference on Cyber Warfare and Security ECCWS 2021. Academic Conferences International, Reading, UK, pp. 623–627. https://doi.org/10.34190/EWS.21.076

Rajamäki, J., Ruoslahti, H., 2018. Educational competences with regard to critical infrastructure protection, in: ECCWS 2018: Proceedings of the 17th'European Conference on Cyber Warfare and Security. pp. 415–423.

Ruoslahti, H., 2019. Co-creation of Knowledge for Innovation in Multi-stakeholder Projects (Doctoral dissertation). University of Jyväskylä, Jyväskylä.

Ruoslahti, H., Rajamäki, J., Koski, E., 2018. Educational Competences with regard to Resilience of Critical Infrastructure. Journal of Information Warfare 17, 1–16.

Savage, M., 2002. Business continuity planning. Work study 51, 254–261.

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. Cambridge Scholars Publishing, Newcastle upon Tyne, UK, pp. 189–196.

Tikanmäki, I., Räsänen, J., Ruoslahti, H., 2022. Information Sharing Networks for European Land and Maritime Border Authorities. Presented at the 26th International Conference on Circuits, Systems, Communications and Computers (CSCC), IEEE, Crete, Greece, pp. 149–160. https://doi.org/10.1109/CSCC55931.2022.00035

Vos, M., 2017. Communication in turbulent times: Exploring issue arenas and crisis communication to enhance organisational resilience. Vos & Schoemaker, Jyväskylä.

Vos, M., Schoemaker, H., Luoma-aho, V., 2014. Setting the agenda for research on issue arenas. Corporate Communications: An International Journal 19, 200–215. https://doi.org/10.1108/CCIJ-08-2012-0055

Wan, T., Geraets, A.A., Doty, C.M., Saitta, E.K.H., Chini, J.J., 2020. Characterizing science graduate teaching assistants' instructional practices in reformed laboratories and tutorials. IJ STEM Ed 7, 30. https://doi.org/10.1186/s40594-020-00229-0

Westermann, K.D., 2011. Learning the "Craft of Auditing": Applications of the Cognitive Apprenticeship Framework (Ph.D.). ProQuest Dissertations and Theses. Bentley University, United States -- Massachusetts.

Yin, R.K., 2009. Case study research: Design and methods, 4th ed. Thousand Oaks, CA: Sage Publications.