Fostering Trust for Effective Information Sharing and Collaboration

Ilkka Tikanmäki[1, 2] and Harri Ruoslahti[1]
[1]Research, Design and Innovation, Laurea University of Applied Sciences, Espoo, Finland
[2]Department of Warfare, National Defence University, Helsinki, Finland

Ilkka.tikanmaki@laurea.fi
harri.ruoslahti}@laurea.fi

Abstract: Trust is crucial for effective information exchange that is needed to counter possible hybrid influence. This literature review outlines current views on strategies to build trust between stakeholders, such as creating strong partner relationships, transparent communication on how information is used, and adhering to clear standards and guidelines. Besides stakeholder cooperation, impacts of trust are also seen in, e.g. regulatory frameworks, data protection, information security, and information exchanges between IT systems. The results of this study emphasise understanding the importance of trust in building situational awareness, needed to identify hybrid influence. Confidence in all involved stakeholders and systems can enhance situational awareness, as, e.g. effective collaboration helps promote safety by enabling stakeholders to comprehend and effectively react to adverse events and information security failures. Trust becomes a fundamental prerequisite for the successful exchange of knowledge and information among stakeholders. Fostering trust can help stakeholders improve situational awareness, ensure effective decision-making, and achieve shared goals in various domains. Trusted information exchange may unlock opportunities for innovation, growth, and mutual prosperity. In today's information-driven world, trust can be seen as a cornerstone for effective communication and successful collaboration among stakeholders. Results suggest that trust-building among stakeholders can lead to a secure reliance on the integrity and reliability of others and thus promote comprehensive approaches, e.g. to manage emerging risks. This implies that sensitive information could be exchanged without fear of misuse or disclosure; trust between stakeholders seems to be more significant than mere cooperation. IT systems, regulatory frameworks, data protection, and security are all affected by trust in information exchange. To effectively increase their respective and collective situational awareness and safety, stakeholders need a foundation of trust to work efficiently.

Keywords: Trust, Situational awareness, Collaboration, Information sharing, Communication, Information exchange

1. Introduction

Trust can be, e.g., belief in the behaviour and goodwill of others, and these can grow or disappear due to interactions and experiences (Hakanen and Soudunsaari, 2012). Focus on trust can play a pivotal role in facilitating smooth flows of information between and among stakeholders (Gardberg, 2021; Lansing *et al.*, 2023). Stakeholders must be confident that their information will be protected and used only for its intended purpose (Pilerot, 2013). Without trust, the exchange of information can become hampered, which can bring unwanted risks and result in ineffectiveness. Building trust is based on many factors, including building relationships and partnerships across organisations, promoting transparency in how information is used, and adhering to clear guidelines and standards for sharing information. Maintaining stakeholder trust and reducing costs associated with potential information breaches requires investing in secure and reliable information systems (Pilerot, 2013; Rajamäki, 2020). Potential cyber threats increase complexity within the critical sectors and infrastructure of society; examples of these are energy, healthcare, and transport (DYNAMO project, 2024). Dynamic resilience is seen as a comprehensive approach for managing emerging risks; this framework encourages the growth of resilience management skills and capacity (World Energy Council, 2019). Thus, being aware of different risks and preparing for future developments becomes important when increasing resilience, be it to specific events, systemic changes or deliberate hybrid influence, which may be very hard to distinguish as such and difficult to trace back to a source. All sectors of society are needed to create holistic strategies to combat the potential widespread impacts of hybrid influence. Emergency services, e.g., should collaborate with other government agencies, private sector organisations, and even the public.

Trust impacts information exchange across various domains, including, e.g. trust between stakeholders and information technology (IT) systems, regulatory data protection, and information security frameworks. Establishing trust between stakeholders and information exchange systems becomes crucial to promoting efficiency, enhancing situational awareness, and increasing the safety of individuals and organisations (Staples and Webster, 2008; Rajamäki, 2020). The principles of Network Centric Warfare emphasise the significance of robust networking, shared situational awareness, and collaboration in enhancing the effectiveness of missions (Alberts, 2002).

The ability to understand information security failures and respond effectively to harmful events requires situational awareness, and trust is essential to the open sharing of information between different authorities

and facilitating decision-making processes (Tikanmäki, 2017). Collaboration is seen as a key aspect when developing the maturity and broadening knowledge bases needed to address common challenges and common goals (Alberts *et al.*, 2001). (Goldenberg *et al.*, 2019) argue that cooperation may encounter obstacles because of differences in culture, work styles, and perceived problems in commitment and dedication to work.

This study builds on prior studies to look at the role of trust in promoting transparent communications, secure systems, and compliance with standards and how trust can help stakeholders improve their situational awareness, ensure effective decision-making, and work towards achieving common goals in various domains. The research question of this study is: How can building trust among stakeholders promote dynamic resilience?

2. Method

This study is an effort to provide in-depth, detailed information on trust as a human factor in building dynamic resilience, using an empirical research approach to examine the culture of the researched area (Benbasat, Goldstein and Mead, 1987; Dubé and Pare, 2003; Yin, 2009). The aim was to investigate the process of building and maintaining trust, which was done by reading and analysing the results of systematic data collection.

Literature review can help display the present state of research and knowledge, identify new research, shortcomings, and future developments to propose opportunities or solutions, while enhancing theoretical understanding (Lim, Kumar and Ali, 2022). Knowledge of general theories or methods is necessary in conducting qualitative research (Alasuutari, 1996, 2004). Using multiple lines of evidence is suggested (Yin, 2009) when examining comprehensive and extensive phenomena that may require extensive research (Dubé and Pare, 2003) and valuable information can be gathered from various sources, such as journal articles, official or unofficial reports, regulations, brochures, and memos (Patton, 2002)

This study addresses trust by focusing on the human aspects of collaboration and cooperation between organisations to identify confidential aspects of information sharing. The sample material in this research consists of document-based written material that includes published studies, academic dissertations, scientific articles, and literature in the field (Figure 1).

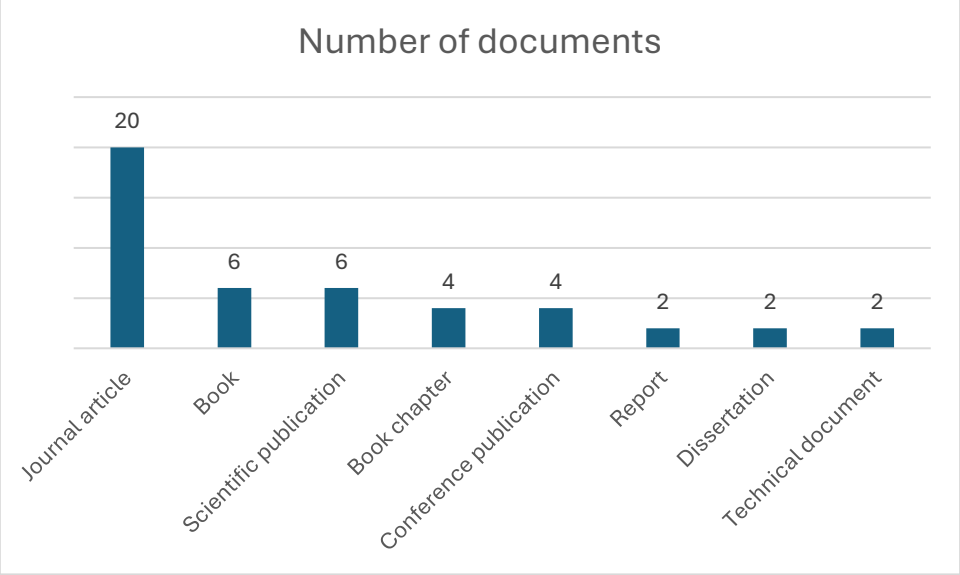

Figure 1: Types and number of documents

The research method used for this study was descriptive and conducted as a qualitative study using a literature review of 46 source documents. Most material was from journals and scientific or conference publications (n = 30). This material was examined to gain a more comprehensive understanding of the research problem based on four theoretical approaches; documents that addressed themes related to trust, situational awareness, collaboration, or information sharing within or between organisations were included. Documents that lacked an empirical or theoretical basis or that did not fall within the scope of the research topic were excluded.

According to (Kitchenham, 2004) a literature review is a comprehensive procedure that helps present evidence of the effects of specific events. The purpose of this study was to conduct an academic search to obtain answers

to the research question. This study involved a search, selection criteria, and analysis with a Data Extraction Table (DET) that mirrored the research question to guide reporting of findings and conclusions.

3. Results

Results show that trust is crucial to sharing information, as stakeholders need confidence that any information they share will be protected and used solely for intended purposes (Johnson *et al.*, 2016; Sedenberg and Dempsey, 2018). Trust can impact information exchange on many levels, e.g. trust between stakeholders, IT systems, regulations, standards, data protection and information security. Stakeholders must have confidence in each other and the systems used to process and share information. Establishing trust leads to improved efficiency, reduced risks, and better outcomes in the sharing of information among various entities, while roles between stakeholders are in constant fluid change (Ruoslahti, 2018).

Technical, organisational, and human means may establish trust (Rajamäki, 2024). Building trust is crucial for facilitating information sharing (Staples and Webster, 2008). "Trust is, after all, the single most important precondition for knowledge exchange" (Rolland and Chauvel, 2012, p. 239) and it creates positive impacts on information sharing; trust and information sharing have a strong positive relationship (Staples and Webster, 2008). "Nowadays, there is a tight coupling of systems and processes, and there are many interdependencies between these systems and processes" (Vos, 2017, p. 23). Building trust can be achieved by establishing partnerships between organisations and transparent communication on how information is utilised (Liu and Chetal, 2005; Ahmad and Huvila, 2019; Mirkovski, Davison and Martinsons, 2019; Rajamäki, Tikanmäki and Räsänen, 2019).

3.1 Trust Between Stakeholders

Sharing information on threats and vulnerabilities can "help identify trends, better understand the risk faced, and determine what preventive measures should be implemented" (Stanciugelu *et al.*, 2013, p. 6) and defining common problems and goals are in themself collaborative processes (Ruoslahti, 2018). Identifying important themes can help identify risks, critical activities, key personnel, guidelines, procedures, and open communication to manage continuity and enhance resilience (Hytönen and Ruoslahti, 2024).

Business continuity management principles can be used to dynamically build resilience, important for all organisations (Hytönen and Ruoslahti, 2024). Coalitions and cross-cultural collaboration present challenges, which, when better understood, can engage different stakeholders in long-term cooperation in co-creation that helps affect change, build alignment, and best practices (Alberts *et al.*, 2001; Ruoslahti and Hyttinen, 2017). Multiple stakeholders may have very different interests and various interdependencies (Vos, 2017, p. 13). Lack of mutual understanding of roles, abilities, cultures, and perspectives of others can greatly hinder cooperation (Goldenberg *et al.*, 2019).

Cultural differences between actors present challenges of varying perspectives, values, and communication styles. To ensure everyone is moving in the same direction, cultural divides need to be bridged (Goldenberg *et al.*, 2019). "There must be trust between stakeholder representatives and organisations" (Ruoslahti, Rajamäki and Koski, 2018, p. 10). Perceived incompatibilities of work styles, work ethics, commitment or dedication to work can be common collaboration problems, while work rotation bridges loss of knowledge, effectiveness, and business continuity (Goldenberg *et al.*, 2019). "A clear situational picture enables consideration of possible further changes in the environment"(Ruoslahti, Rajamäki and Koski, 2018, p. 9).

3.2 Trust in Communication

Solving common issues motivates stakeholders to collaborate and build trust in open innovation environments that facilitate communication and interaction (Ruoslahti, 2018). Determining targets involves identifying how to work together, gaining knowledge of stakeholder traits, tasks and situations (Alberts *et al.*, 2001). Situational awareness is based on open, trust-based information sharing of simultaneous relationships of knowledge creation and knowledge transfer (Sankowska, 2013; Ruoslahti, Rajamäki and Koski, 2018; Ruoslahti and Tikanmäki, 2019).

Knowledge building processes are "increasingly complex, multidisciplinary, trust-based, co-created, path-depended, and globalized" (Pirinen, 2015, p. 323). Inter-organisational learning highlights networks that exchange information and resources, collaboratively solve problems across organisational boundaries, and actively build trust (Engeström, Kerosuo and Kajamaa, 2007). Collaboration in networks calls for active

coordination and facilitation that motivates its members and other stakeholders to participate actively (Ruoslahti and Tikanmäki, 2019).

One of eight attributes of resilience in collaboration networks is trust building, the other seven being: clear co-created purpose and common aims, agreed organisation and roles, a common culture and common ways of working, leadership within the network, facilitation of collaboration and co-creation, system to back-up or exchange of network stakeholder representatives, and open communication and information sharing between all network stakeholders (Ruoslahti, Rajamäki and Koski, 2018). Building trust enhances open flows of communication among stakeholders (Rajamäki and Ruoslahti, 2018), while the effective functioning of businesses, governments, and societies requires information exchange, which also has risks, such as misuse or disclosure of shared sensitive data (Goldenberg *et al.*, 2019).

3.3 Trust in Systems

To avoid trust issues, it is also important to trust all information exchange systems, e.g. confidence in system security and reliability, and accuracy and timeliness of shared information (Pilerot, 2013; Sedenberg and Dempsey, 2018). "Investing in systems that improve confidence and trust can significantly reduce costs and improve the speed of interaction" (Rajamäki, 2020, p. 99). Setting clear guidelines and expectations for sharing information with common rules and standards fosters transparency and builds dynamic resilience, with e.g. business continuity management principles, which are essential for all organisations (Mizrak, 2024). Compliance with regulations and standards can ensure that information is shared consistently and reliably, and this fosters trust among stakeholders (Soderlind, 2009).

Common continuity management analysis of risks, critical activities, key personnel, guidelines and procedures, and open communication can help establish trust needed to enhance resilience (Mizrak, 2024). Stakeholders should have confidence in the security of their data and that adequate data protection and security measures have been taken for information exchange (Boehm, 2012).

Situational awareness is the ability to perceive and comprehend what is happening in one's surroundings, evaluate this information, and predict future developments (Endsley and Garland, 2000). Situational awareness is necessary to comprehend information security failures and other crucial factors that may impact security (Pöyhönen *et al.*, 2020). Human aspects need to be managed by security management to allow resilient systems and infrastructure to prepare, plan, absorb, recover, and adapt more efficiently to adverse events (Rajamäki, 2020).

Building trust allows stakeholders to work efficiently to enhance situational awareness, effectiveness, and safety of both individuals and organisations (Lansing *et al.*, 2023). SA enables the systematic prevention, identification, and protection of systems against unwanted disturbances and enables system protection against various threats (Pöyhönen *et al.*, 2020).

Decision-making requires collecting information about the environment from various sources, such as networks, risk trends and operational parameters, and exchanging this information between different stakeholders is necessary (Tikanmäki, 2017). Situational awareness is needed to develop and use countermeasures. Observations, analysis, visualisation, and national and international cooperation are some of the most important elements of situational awareness (Tikanmäki and Ruoslahti, 2019). (Pöyhönen *et al.*, 2020) e.g., offer the Observe – Orient – Decide – Act (OODA) loop to promote collaboration towards a shared situational picture, awareness and understanding and improving resilience. Shared information can increase situational awareness during operational activities and support decision-making as long as the shared information is reliable (Zaerens, 2022). Trust is an especially important element when exchanging information among authorities (Tikanmäki, 2017).

Shared situational awareness can significantly increase the effectiveness and availability of information on all levels to help redefine relationships between participants (Alberts, 2002) to help complete project tasks (Howah and Chugh, 2019). Understanding how human organisations and material structures are mutually entangled helps develop practices that anticipate possible future incidents and gain the feedback required for learning from the experiences gained from these incidents (Amir and Kant, 2018).

3.4 Information Sharing

Trust enables the smooth flow of information between stakeholders. However, they must be confident that the information they share is safeguarded and solely used for intended purposes (Pilerot, 2013). According to (Ruoslahti, 2018) for collaboration to become jointly constructed and coordinated, stakeholders must feel they

will benefit from the process and its outcomes. Mutual collaboration within or between organisations requires sharing knowledge. With the help of trust management, the correctness of the shared information can be assessed, and the reliability of the recipients of the information can be defined (Zaerens, 2022).

Lack of trust in information exchange may lead to ineffectiveness and risks (Pilerot, 2013). Exchanging information in many fields, such as business, government, and society, depends on trust, and it is important that organisations, both companies and authorities, trust that all partners act in good faith so that confidential information is protected (Hakanen and Soudunsaari, 2012; Gardberg, 2021). Human relationships are the key when building trust, as stakeholders can gain a better understanding of each other's needs and concerns by taking the time to get to know each other (Goldenberg *et al.*, 2019). Organisations and individuals can establish trust by building relationships, promoting transparency, adhering to standards, and investing in security (Soderlind, 2009).

Trust in IT systems, regulations, standards, data protection, and information security promotes smooth flows of information (Pilerot, 2013). Information is more likely to be shared freely and openly when stakeholders have trust in the systems and processes used for information exchange (Zaerens, 2022). Situational awareness of what is happening and how it might affect you (Tikanmäki and Ruoslahti, 2019) requires trust, which is crucial to promote efficiency, increase situational awareness, improve safety, and foster successful collaboration (Pilerot, 2013; Sedenberg and Dempsey, 2018). Network Centric Warfare principles, for example, highlight the importance of trust in building a strong network, sharing situational awareness, and collaborative efforts, which contribute to the enhancement of the quality and availability of information and increase mission effectiveness and help promote the maturity, development, and expansion of knowledge to collectively address challenges (Alberts, 2002).

4. Conclusions

The results of this study indicate that building trust among stakeholders can promote dynamic resilience, which is needed to counter possible hybrid threats and influence. In today's information-driven world, trust is a cornerstone for effective communication and successful collaboration among stakeholders. The significance of trust lies in its ability to foster assured reliance on the integrity and reliability of others. This means exchanging sensitive information without fear of its misuse or disclosure.

Organisational stakeholders must mainly rely on trust to share critical data. If this becomes compromised, it can greatly impact business operations and reputation. Stakeholders should ensure that their information will be protected and used only for its intended purpose. Without trust, flows of information may waver, causing inefficiencies and potential risks, resulting in loss of effectiveness and productivity.

Results show how cooperation benefits from new and diverse perspectives. Different backgrounds, cultures, skills, or work experiences can be beneficial to help make effective decisions, develop a broad understanding, and improve leadership. Additional work-related knowledge and skills can be based on competent individuals having valuable individual skills, and organisational stability, continuity, and collective corporate memory become beneficial assets to supplement areas of discontinuity.

The depth and abundance of experience and knowledge gained from others, learning the general operational experiences of others, and specialised knowledge and culture are the advantages of a cooperative culture. Creating a positive work culture fosters a sense of unity and supports the organisation positively.

One of the most significant factors in creating and maintaining cooperation is to respect all organisations involved. The importance of comprehending the perspectives of others, their roles, and their tasks, while also understanding and being familiar with each other and each other's organisations, are seen in the results. Knowing their backgrounds, skills, and working methods helps build trust. The importance of communication in general and the exchange of information, perspectives, and initiatives in a timely and efficient manner is highlighted in relevant literature. Strengthening cooperation and integration requires opportunities to interact and work on common tasks to achieve a common objective.

Building trust involves creating strong partnerships and relationships among organisations, promoting transparency in the use of information, and adhering to clear guidelines and standards. Maintaining stakeholder trust to safeguard against potential information breaches depends on investing in secure and reliable information systems. Based on the results, trust has a more profound impact than just cooperation between stakeholders. Trust also affects the influence of information exchange between information technology systems,

regulatory frameworks, data protection and security. A foundation of trust helps, and is even necessary, for stakeholders to work efficiently to increase their respective and collective situational awareness and safety.

Situational awareness is crucial in comprehending and responding effectively to information security failures and adverse events, and trust is key to sharing critical information across different authorities, facilitating decision-making processes, and creating a collaborative environment. However, collaboration may face barriers due to cultural differences, divergent work styles, and perceived issues of commitment and dedication. EU-funded projects, for example, aim to bring experts from different backgrounds to work with end-users with selected tools and platforms.

To conclude, trust seems to be one of the most important preconditions for successful knowledge exchange and information sharing. By fostering trust through transparent communications, secure systems, and adherence to standards, stakeholders can improve cyber situational awareness, ensure effective decision-making, and achieve shared objectives in a variety of domains.

Trust can help speed recovery processes and contribute to self-healing. As stakeholders adopt confidence as a guiding principle, information sharing will catalyse innovation, growth, and mutual prosperity. Building trust among stakeholders can promote information sharing, which in turn should indeed enhance dynamic resilience that helps combat hybrid threats.

In promoting the integration of both human and technological aspects of trust, this study advances sociotechnical systems theory and highlights the significance of trust in network-centric and collaborative governance. A practical contribution is that dynamic resilience can be supported by trust as a multidimensional concept. Moreover, this study supports knowledge management and open innovation theories by demonstrating how trust can facilitate effective knowledge exchange and organisational learning.

This research offers very practical advice for organisations to invest in secure, transparent, and standards-compliant information systems to foster trust and reduce risks. Business continuity professionals can improve preparedness and recovery by incorporating trust principles into continuity planning. Investing in trust-building activities, such as training and transparent communication, can help improve collaboration and resilience in a multi-stakeholder environment.

A limitation of this study is that trust, the concept that it examines, is a very comprehensive and extensive phenomenon. More research is recommended to further verify the connection between trust-based information sharing and the improvement of sustainable development, cybersecurity, and business continuity management and to strengthen the dynamic cyber resilience of critical services, especially against hybrid threats.

Acknowledgements

Acknowledgements are paid to the “Improving rescue services preparedness for hybrid threats” project, funded by the Fire Protection Fund and conducted in collaboration with the Finnish Association of Fire Officers. The views expressed are those of the authors, and the granting authority cannot be held responsible for them.

Ethics declaration: Ethical clearance was not required for the research.

AI declaration: The paper's spelling was verified using the artificial intelligence tool.

References

Ahmad, F. and Huvila, I. (2019) ‘Organizational changes, trust and information sharing: an empirical study’, *Aslib Journal of Information Management*, 71(5), pp. 677–692. Available at: https://doi.org/10.1108/AJIM-05-2018-0122.

Alasuutari, P. (1996) ‘Theorizing in qualitative research: A cultural studies perspective’, *Qualitative inquiry*, 2(4), pp. 371–384.

Alasuutari, P. (2004) ‘The globalization of qualitative research’, in C. Seale et al. (eds) *Qualitative research practice*. London UK: SAGE Publications Ltd, pp. 595–608. Available at: https://www.torrossa.com/gs/resourceProxy?an=5018485&publisher=FZ7200#page=526 (Accessed: 14 February 2024).

Alberts, D.S. *et al.* (2001) *Understanding Information Age Warfare:* Fort Belvoir, VA: Defense Technical Information Center. Available at: https://doi.org/10.21236/ADA386374.

Alberts, D.S. (2002) *Information age transformation: Getting to a 21st Century Military*. Revised. Washington D.C.: DoD Command and Control Research Program (CCRP) (Information Age Transformation Series).

Amir, S. and Kant, V. (2018) ‘Sociotechnical Resilience: A Preliminary Concept’, *Risk Analysis*, 38(1), pp. 8–16. Available at: https://doi.org/10.1111/risa.12816.

Benbasat, I., Goldstein, D.K. and Mead, M. (1987) 'The Case Research Strategy in Studies of Information Systems', *MIS Quarterly*, 11(3), pp. 369–386. Available at: https://doi.org/10.2307/248684.

Boehm, F. (2012) *Information Sharing and Data Protection in the Area of Freedom, Security and Justice; Towards Harmonised Data Protection Principles for Information Exchange at EU-level*. Berlin, Heidelberg: Springer. Available at: https://doi.org/10.1007/978-3-642-22392-1.

Dubé, L. and Pare, G. (2003) 'Rigor In Information Systems Positivist Case Research: Current Practices, Trends, and Recommendations', *MIS Quarterly*, 27(4), pp. 597–635. Available at: https://doi.org/10.2307/30036550.

DYNAMO project (2024) *DYNAMO Mission and Objectives*. Available at: https://horizon-dynamo.eu/about/ (Accessed: 9 January 2024).

Endsley, M. and Garland, D. (2000) 'Theoretical underpinnings of situation awareness: A critical review', *Situation awareness analysis and measurement*, 1(1), pp. 3–31.

Engeström, Y., Kerosuo, H. and Kajamaa, A. (2007) 'Beyond Discontinuity: Expansive Organizational Learning Remembered', *Management Learning*, 38(3), pp. 319–336. Available at: https://doi.org/10.1177/1350507607079032.

Gardberg, M. (2021) *Trust and routines in multi-supplier networks*. Dissertation. National Defence University.

Goldenberg, I. *et al.* (2019) 'Integrated defence workforces: Challenges and enablers of military–civilian personnel collaboration', *Journal of Military Studies*, 8(2019), pp. 28–45.

Hakanen, M. and Soudunsaari, A. (2012) 'Building Trust in High-Performing Teams', *Technology Innovation Management Review*, (June 2012: Global Business Creation), pp. 38–41.

Howah, K. and Chugh, R. (2019) 'Do We Trust the Internet?: Ignorance and Overconfidence in Downloading and Installing Potentially Spyware-Infected Software', *Journal of Global Information Management (JGIM)*, 27(3), pp. 87–100. Available at: https://doi.org/10.4018/JGIM.2019070105.

Hytönen, E. and Ruoslahti, H. (2024) 'Business Continuity Management– Building Block of Dynamic Resilience', *Critical Information Infrastructures Security Lecture Notes in Computer Science*, pp. 120–134. Available at: https://doi.org/10.1007/978-3-031-62139-0_7.

Johnson, C.S. *et al.* (2016) *Guide to Cyber Threat Information Sharing*. NIST SP 800-150. Gaithersburg, MD: National Institute of Standards and Technology, p. NIST SP 800-150. Available at: https://doi.org/10.6028/NIST.SP.800-150.

Kitchenham, B. (2004) *Procedures for Performing Systematic Reviews*. Technical report TR/SE-0401. Eversleigh Australia: Keele University, p. 33.

Lansing, A.E. *et al.* (2023) 'Building trust: Leadership reflections on community empowerment and engagement in a large urban initiative', *BMC Public Health*, 23(1), p. 1252. Available at: https://doi.org/10.1186/s12889-023-15860-z.

Lim, W.M., Kumar, S. and Ali, F. (2022) 'Advancing knowledge through literature reviews: "what", "why", and "how to contribute"', *Service Industries Journal*, 42(7–8), pp. 481–513. Available at: https://doi.org/10.1080/02642069.2022.2047941.

Liu, P. and Chetal, A. (2005) 'Trust-Based Secure Information Sharing between Federal Government Agencies', *JASIST*, 56(3), pp. 283–298. Available at: https://doi.org/10.1002/asi.20117.

Mirkovski, K., Davison, R.M. and Martinsons, M.G. (2019) 'The effects of trust and distrust on ICT-enabled information sharing in supply chains: Evidence from small- and medium-sized enterprises in two developing economies', *The International Journal of Logistics Management*, 30(3), pp. 892–926. Available at: https://doi.org/10.1108/IJLM-06-2017-0155.

Mizrak, K.C. (2024) 'Crisis Management and Risk Mitigation: Strategies for Effective Response and Resilience', in *Trends, Challenges, and Practices in Contemporary Strategic Management*. Hershey PA: IGI Global, pp. 254–278. Available at: https://doi.org/10.4018/979-8-3693-1155-4.ch013.

Patton, M.Q. (2002) *Qualitative Research & Evaluation Methods*. 3rd edn. Thousand Oaks, California: Sage Publications.

Pilerot, O. (2013) 'A practice theoretical exploration of information sharing and trust in a dispersed community of design scholars', *Information Research: An International Electronic Journal*, 18(4), p. 26.

Pirinen, R. (2015) 'Studies of Externally Funded Research and Development Projects in Higher Education: Knowledge Sources and Transfers', *Creative Education*, 6(3), pp. 315–330. Available at: https://doi.org/10.4236/ce.2015.63030.

Pöyhönen, J. *et al.* (2020) 'Cyber Situational Awareness in Critical Infrastructure Protection', *Annals of Disaster Risk Sciences : ADRS*, 3(1), pp. 0–0. Available at: https://doi.org/10.51381/adrs.v3i1.36.

Rajamäki, J. (2020) 'Resilience Management Framework for Critical Information Infrastructure: Designing the Level of Trust that Encourages the Exchange of Health Data', *Information & Security: An International Journal*, 47(1), pp. 91–108. Available at: https://doi.org/10.11610/isij.4706.

Rajamäki, J. (2024) 'Trust Environment for Cyber-Physical Systems: The DYNAMO Approach', *International Journal on Applied Physics and Engineering*, 3, pp. 1–10. Available at: https://doi.org/10.37394/232030.2024.3.1.

Rajamäki, J. and 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.

Rajamäki, J., Tikanmäki, I. and Räsänen, J. (2019) 'CISE as a Tool for Sharing Sensitive Cyber Information in Maritime Domain', *Information & Security: An International Journal*, 43(2), pp. 215–235. Available at: https://doi.org/10.11610/isij.4317.

Rolland, N. and Chauvel, D. (2012) 'Knowledge transfer in strategic alliances', in *Knowledge Horizons*. 1st edn. Routledge, pp. 225–236.

Ruoslahti, H. (2018) 'Co-creation of knowledge for innovation requires multi-stakeholder public relations', in S. Bowman et al. (eds) *Public Relations and the Power of Creativity*. Emerald Publishing Limited, pp. 115–133.

Ruoslahti, H. and Hyttinen, K. (2017) 'A Co-created Network Community for Knowledge and Innovations: Promoting Safety and Security in the Arctic', in *Engaging people in a disengaged world. 23rd International Public Relations Research Symposium BledCom*, Bled, Slovenia: University of Ljubljana: Faculty of Social Sciences, pp. 100–106. Available at: https://www.theseus.fi/handle/10024/141233 (Accessed: 3 November 2023).

Ruoslahti, H., Rajamäki, J. and Koski, E. (2018) 'Educational competences with regard to resilience of critical infrastructure', *Journal of Information Warfare*, 17(3), pp. 1–16.

Ruoslahti, H. and Tikanmäki, I. (2019) 'Complex Authority Network Interactions in the Common Information Sharing Environment', in J. Bernardino, A. Salgado, and J. Filipe (eds) *11th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management*. *IC3K 2019*, Vienna, Austria: SCITEPRESS – Science and Technology Publications, pp. 159–166. Available at: https://doi.org/10.5220/0007946501590166.

Sankowska, A. (2013) 'Relationships between organizational trust, knowledge transfer, knowledge creation, and firm's innovativeness', *The Learning Organization*, 20(1), pp. 85–100. Available at: https://doi.org/10.1108/09696471311288546.

Sedenberg, E.M. and Dempsey, J.X. (2018) 'Cybersecurity Information Sharing Governance Structures: An Ecosystem of Diversity, Trust, and Tradeoffs'. Cornell: arXiv. Available at: https://doi.org/10.48550/arXiv.1805.12266.

Soderlind, G. (2009) *Reflections on Networking & Information Exchange: Dealing with Sensitive Data amongst Public and Private Actors*. Scientific and Technical Reports EUR 23693 EN-2008. Ispra, Italy: 'European Commission Joint Research Centre. Available at: https://publications.jrc.ec.europa.eu/repository/handle/JRC49481 (Accessed: 17 May 2023).

Stanciugelu, I. *et al.* (2013) 'Perception and communication of terrorism risk on food supply chain: A case study (Romania and Turkey)', in *Applied Social Sciences: Communication Studies*. Newcastle upon Tyne, UK: Cambridge Scholars Publishing, pp. 189–196.

Staples, D.S. and Webster, J. (2008) 'Exploring the effects of trust, task interdependence and virtualness on knowledge sharing in teams', *Information Systems Journal*, 18(6), pp. 617–640. Available at: https://doi.org/10.1111/j.1365-2575.2007.00244.x.

Tikanmäki, I. (2017) 'Common Information Sharing on Maritime Domain - A Qualitative Study on European Maritime Authorities' Cooperation', in, pp. 283–290. Available at: https://doi.org/10.5220/0006582502830290.

Tikanmäki, I. and Ruoslahti, H. (2019) 'How Are Situation Picture, Situation Awareness, and Situation Understanding Discussed in Recent Scholarly Literature?', in *International Conference on Knowledge Management and Information Systems*. *International Conference on Knowledge Management and Information Systems*, Wien: SCITEPRESS Science And Technology Publications, pp. 419–426. Available at: https://doi.org/10.5220/0008494104190426.

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

World Energy Council (2019) *Cyber challenges to the energy transition*. Insight Brief 2019. London UK: The World Energy Council, p. 11. Available at: https://www.worldenergy.org/assets/downloads/Cyber_Challenges_to_the_Energy_Transition_WEC_MMC_2019.pdf?v=1583317261.

Yin, R.K. (2009) *Case study research: Design and methods*. 4th edn. Thousand Oaks, California: SAGE Publications Ltd.

Zaerens, K. (2022) *Utilizing Trust Management in a High-Security Context*. Academic Dissertation. National Defence University.