Inter-Organisational Cybersecurity Governance

Ana-Maria Florescu, Serge Amabile, Claudio Vitari

Inter-Organisational Cybersecurity Governance

PhD Candidate: Florescu Ana-Maria
Aix-Marseille University, CERGAM, FEG
Aix-en-Provence, France
ana-maria.florescu@univ-amu.fr

Supervisor: Amabile Serge
Aix-Marseille University, CERGAM, FEG
Aix-en-Provence, France
serge.amabile@univ-amu.fr

Supervisor: Vitari Claudio
Aix-Marseille University, CERGAM, FEG
Aix-en-Provence, France
claudio.vitari@univ-amu.fr

Abstract: In recent years, rapid technological advancements have transformed the landscape of organisational operations, revolutionised processes, and increased efficiency. However, this evolution has also brought unprecedented cybersecurity risks. Organisations across industries and geographies are dealing with the challenge of keeping their digital assets from many different threats. Additionally, in today's inter-linked corporate landscape, cybersecurity isn't solely the concern of individual organisations but rather a shared responsibility.

This thesis explores the challenges, practices, and gaps in inter-organisational cybersecurity governance and tries to identify the most effective approaches for addressing cybersecurity challenges in today's inter-connected business landscape. It examines how existing governance frameworks apply, by considering Elinor Ostrom's principles on governing the commons and complexity theory. Through a comprehensive literature review and case studies analysis of real-world inter-organisational cybersecurity collaborations, this research aims to provide insights into effective governance strategies and a deeper understanding of the dynamics involved in inter-organisational cybersecurity governance.

Keywords: cybersecurity; governance; collaboration; inter-organisational governance

1. Research Motivation

Over the past years, the landscape of organisational operations has been fundamentally reshaped by rapid technological advancements. This evolution has been accompanied by unprecedented levels of efficiency, enabling organisations to organise processes. However, with these advancements come inherent risks, particularly in the realm of cybersecurity. Today, organisations of all sizes, from diverse industries and geographical locations, face a common challenge: safeguarding their digital assets from a multitude cybersecurity threats. As defined by the ISO 2700X Standard, cybersecurity encompasses the preservation of confidentiality, integrity, and availability of information within the cyberspace. Consequently, cyberspace is seen as "*a complex environment resulting from the interaction of people, software and services on the Internet, supported by worldwide distributed physical information and communications technology (ICT) devices and connected networks*" (ISO/IEC 27032:2012). Cybersecurity is completely contained in information security (von Solms & von Solms, 2018).

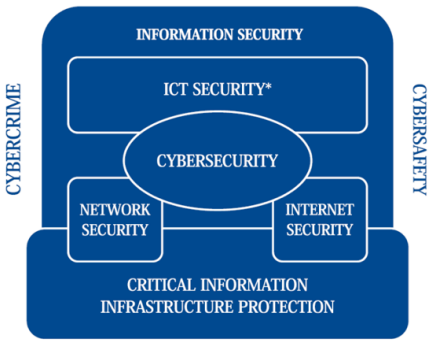

Figure 1: Relationship between cybersecurity and other security domains as interpreted by ISO/ IEC 27032:2012.

Consequently, "*cybersecurity governance, as part of information security governance, is the process of directing and controlling the protection of a company's digital information assets from the risks that are related to using the Internet*" (von Solms & von Solms, 2018, p. 7).

Addressing cybersecurity threats presents several challenges, including the increasing complexity of digital systems, lack of awareness and knowledge about cybersecurity, insufficient incentives for prioritizing cybersecurity measures, and inadequate monitoring and enforcement mechanisms (Harbers et al., 2018). The consequences of cybersecurity breaches can be severe, ranging from data and financial losses to legal repercussions for non-compliance with regulations, damage to reputation, and even service interruptions or loss of clients (Fantino, 2018).

Furthermore, in today's inter-connected business environment, cybersecurity is not just the concern of individual organisations but is instead a shared responsibility. Organisations often collaborate with third-party vendors, for instance, in contexts such as integrated supply chain networks, international communications for maritime or air transport, or banking interconnections. These collaborations are not merely operational necessities, they are strategic endeavours that enhance efficiency, innovation, and competitiveness for all involved parties. Through the lens of game theory, these collaborations can be viewed as cooperative games where every

participant can become better off by taking part. While such collaborations enhance efficiency, they also introduce additional cybersecurity risks, as a breach in one organisation can affect others within the network, leading to disruptions in operations.

Managers and leaders must recognise cybersecurity as a shared responsibility across organisations and be aware of the potential impacts of disruptions within a network. Governance frameworks play a crucial role in managing cybersecurity risks, but their effectiveness depends on how well they are implemented within and between organisations. Inter-organisational governance, which involves coordinating collaborations among multiple companies (Bobbert & Mulder, 2013), is essential for enhancing cybersecurity in today's interconnected business landscape.

2. Research Questions

Considering the current knowledge on inter-organisational cybersecurity governance, how can Ostrom's principles on governing the commons and Complexity theory's frameworks effectively facilitate inter-organisational cybersecurity governance?

RQ1: What are the challenges, practices, and gaps in the current knowledge of inter-organisational cybersecurity governance?

This research question aims to comprehensively assess the landscape of inter-organisational cybersecurity governance by examining the challenges, existing practices, and knowledge gaps in this domain. Understanding these challenges is crucial for developing effective governance strategies that address the complexities inherent in inter-organisational cybersecurity.

RQ2: How can Ostrom's principles be leveraged to guide the design and implementation of inter-organisational cybersecurity governance frameworks?

This research question aims to explore the relevance and applicability of Elinor Ostrom's principles (Ostrom, 1990), particularly those related to the governance of common-pool resources, to the domain of inter-organisational cybersecurity. The investigation will delve into how these principles, such as clearly defined boundaries, proportional equivalence between benefits and costs, collective choice arrangements, monitoring, and graduated sanctions, can be adapted to guide the development and implementation of effective cybersecurity governance mechanisms across multiple organizations. Additionally, the research will examine potential challenges and opportunities in translating these principles into actionable strategies within the context of cybersecurity governance.

RQ3: How does complexity theory contribute to understanding and governing cybersecurity challenges across multiple organisations?

This research question focuses on exploring the role of complexity theory in enhancing our understanding of cybersecurity challenges that arise in inter-organisational contexts. Complexity theory provides a lens through which to view cybersecurity as a dynamic property of interactions within and between organisations, rather than a static phenomenon (Morçöl, 2014). The research will investigate how concepts such as self-organisation, methodological holism, and the recognition of systems' dynamics inherent in complexity theory can inform the design of

cybersecurity governance frameworks capable of addressing the dynamic and inter-connected nature of modern cyber threats. Additionally, the study will explore practical implications for leveraging complexity theory to develop more agile and responsive cybersecurity strategies that account for the diverse and evolving needs of multiple organisations collaborating in a shared cyber ecosystem.

3. Theoretical Framing

Elinor Ostrom's works on governing the commons provide a structured approach to analysing the governance of natural systems involving multiple actors, rules, and interactions. Her works are focused on self-organisation and self-governance in structured environments, such as common pool resources like forests, fisheries, and irrigation systems. Her research challenges the assumption that centralised control is necessary to manage such resources effectively. Instead, she argues that local communities can develop their own rules and norms for managing shared resources through a process of collective action (Ostrom, 1990).

While Ostrom's research recognizes the importance of the context, it tends to view the social and ecological systems as relatively static (Morçöl, 2014). In order to analyse the dynamics of inter-organisational collaboration, complexity theory is capable to provide a basis for understanding how complex systems, characterised by non-linear interactions among numerous components, self-organise. It emphasizes the dynamic and non-linear interactions between agents in a complex system, whereas Ostrom's framework focuses on identifying the conditions under which self-organisation can occur in a given system.

4. Research Approach/ Methodology

This article delineates a robust methodology designed to explore the multifaceted realm of inter-organizational cybersecurity governance. The research commences with an systematic literature review, utilising the Web of Science database, to identify the prevailing challenges, practices, and gaps within the field. This foundational phase involves the meticulous screening of 721 articles, employing both Covidence and Zotero for systematic inclusion and exclusion based on specific criteria, ultimately narrowing the focus to 140 pertinent papers. These articles undergo a grounded theory analysis, supported by NVivo, to rigorously synthesize emerging themes and insights related to cybersecurity governance frameworks and inter-organizational collaboration.

Following the literature review, a case study approach is implemented to validate and extend the theoretical findings through practical examination of real-world inter-organizational cybersecurity strategies. With the help of Elinor Ostrom's principles on governing the commons and complexity theory, an analysis of cybersecurity governance frameworks will be held. A comparative analysis of various frameworks will be conducted to ascertain the most effective approach.

5. Preliminary Findings

The conducted literature review showed several insights on the topic of inter-organisational cybersecurity governance. As presumed, there are some attempts to apply alternative governance models and frameworks typically utilised in natural sciences, such as Ostrom's

Institutional Analysis and Development IAD (Chang & Huang, 2023), a framework that offer valuable insights into understanding the formal and informal rules governing inter-organisational cybersecurity collaborations. These frameworks provide a structured approach to analysing and designing governance mechanisms that promote trust, cooperation, communication, and effective decision-making among diverse stakeholders in cybersecurity networks.

The role of blockchain technology and other decentralised frameworks in enhancing cybersecurity governance within inter-organisational structures is analysed (Fabian et al., 2015; Carminati et al., 2018). Trust emerges as a critical factor in facilitating secure collaboration and information sharing among organisations, particularly in the context of cybersecurity networks (Kapucu, 2012; Deljoo et al., 2018).

Numerous researchers have made significant contributions to the advancement of governance mechanisms, collaborative models, and trust frameworks within the realm of cybersecurity inter-organizational governance. Vinnakota (2016) conducted a comprehensive analysis of cybersecurity, cyber-risks, and information security governance, proposing a cybernetic model tailored for information security governance within enterprises. Ramirez & Choucri (2016) introduced standardised terminology to enhance inter-disciplinary communication in cybersecurity research. Naicker & Mafaiti (2019) discussed the establishment of collaboration in managing information security through multi-sourcing. Ghadge et al. (2020) highlighted the importance of managing cyber risks in supply chains and emphasised the need for raising risk awareness, standardising policies, and developing collaborative strategies for creating supply chain cyber-resilience. Tagarev (2020) identified and prioritized governance requisites for collaborative networked organizations in cybersecurity, encompassing a spectrum of issues such as standards, decision-making processes, transparency, trust, resilience, leadership, competencies, and organizational culture, etc. (Tagarev, 2020).

Tier	Governance Objectives	Features of CNOs
1	Geographical representation or exclusion; Involving external stakeholders; Representation; Decision making; Auditing; Confidentiality and Security; Knowledge management; Standards and methodologies; Long-term perspective on collaboration; Competences; Risk management; Evidence-based decision-making	Adaptiveness; Cohesion; Trust; Competitiveness
2	Supply chain security; Dispute/conflict management arrangements; Intellectual Property management; Ethics code; Gender policies and representation; Transparency; Accountability; Integrity/anti-corruption policy	Innovation; Leadership
3	Communication and engagement	Organisational culture; Sustainability
4	'Green' policies; Slave labour, labour of minors; Interoperability	Resilience

Figure 2: Prioritisation of governance needs, objectives, and requirements (Tagarev, 2020)

Tagarev's prioritisation (Figure 2) emphasizes the importance of addressing a wide range of governance objectives to ensure the effectiveness, resilience, and sustainability of Collaborative Networked Organisations in the cybersecurity domain.

Determining and defining roles, accountabilities and responsibilities when identifying and assessing levels of risks around cybersecurity is one of the key practice (Bobbert & Mulder, 2013), alongside with security awareness, incident response, communication, transparency, risk appetite, and regularity (Figure 3).

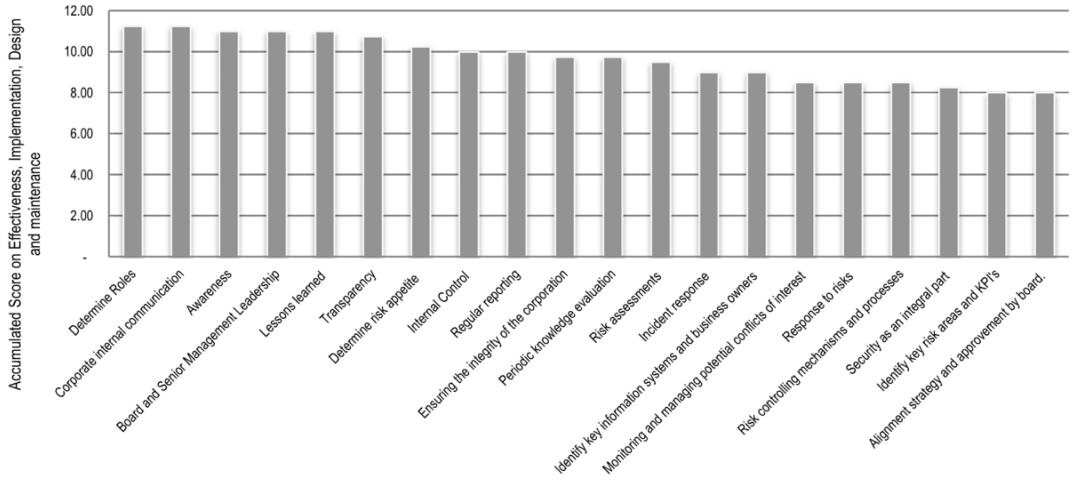

Figure 3: Top 20 practices for Business Information Security Governance BISG (Bobbert & Mulder, 2013)

When it comes to information sharing, that does not necessarily mean open exchange of data, but rather a shared responsibility towards achieving cross-organizational goals, Crowther (2014) identifies following common failures (Figure 4) that lead to failed collaborative outcomes: failure of partnership (ambiguous responsibilities/ relations, rivalries, distrust), failure of communication (poor messaging, inadequate sharing or discovery), failure of fusion/ actions (inadequate or incorrect details for decisions), failure of feedback (inadequate detection/ correction of failures) (Crowther, 2014).

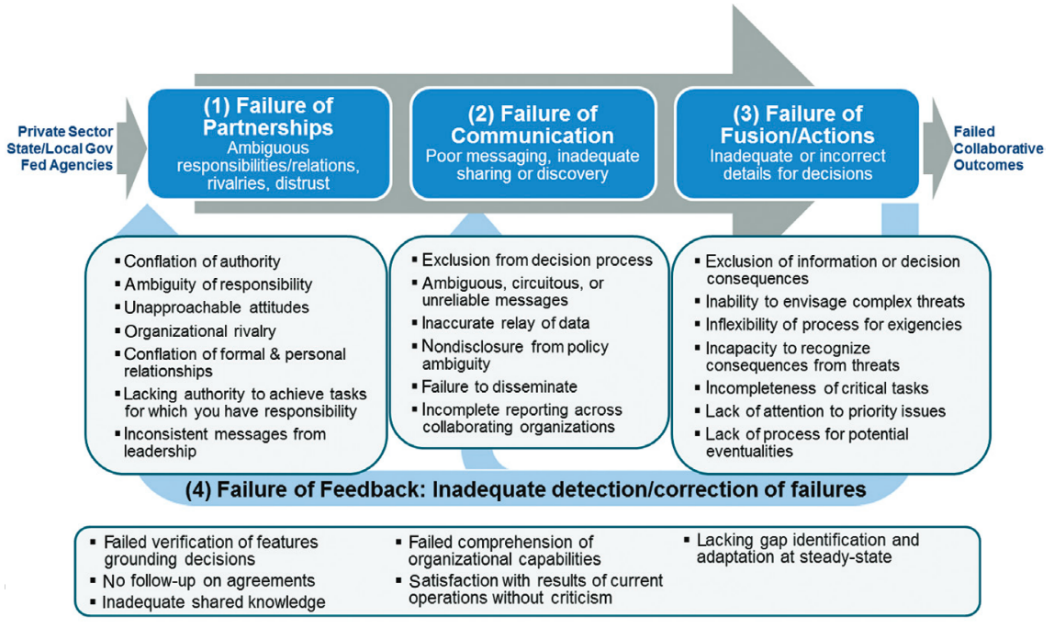

Figure 4: Common information sharing failures, grouped in 4 categories (Crowther, 2014)

In order to obtain a successful collaboration and information sharing activities, there's a need of some common qualities: "*clear identification of stakeholders, forward-looking leadership, and well-defined business processes*" (Crowther, 2014, p. 135). Consequently, an information sharing cycle is proposed, that includes (1) building and sustaining partnerships, (2) communication for information discovery and dissemination, (3) information fusion for decision and action, (4) feedback from collaborative outcomes in order to obtain a shared understanding, consistent decisions, coordinated actions. Crowther (2014) proposes common features of information sharing activities that produced collaborative outcomes, including good governance of information sharing activity; clear and effective business processes and methods; adaptive, role-driven, and security-conscious operations; acceptance and adoption driven by stakeholders; monitored and measures performance; managed and sustained resources. "*Effective information sharing elevates the ability of multiple organisations to collectively handle complex threats*" (Crowther, 2014, p. 151). Additionally, authors propose five information sharing capabilities that are critical to safeguard against all common failures (Figure 5).

Capability	Description
Leadership	Involvement of leaders to provide authority, motivate, build commitment, guide activities, encourage innovation, and mobilize resources; they see the goal and craft plans to achieve it.
Business Modeling and Architecture Development	Formal descriptions of the service and operational components of the cross-organizational activity, how they are connected to each other, and what technologies are used to implement them.
Inter-Organizational Structuring	The degree to which the work styles and relationships, participation in decision-making, levels of competition and collaboration, and styles of conflict resolution support information sharing.
Stakeholder Identification and Engagement	The extent of awareness of, and interaction with, the persons or groups with an interest in the information sharing activity and capacity to influence it.
Performance Measurement	Skills, resources, and authority to observe, measure, and document how well activities are executed, whether information goals are achieved, and how they impact infrastructure resilience.

Figure 5: Five information sharing capabilities critical to safeguard against all common failures (Crowther, 2014).

In their analysis of information-sharing networks, Chang & Huang (2023) establish a connection between the management of multi-sectoral cybersecurity and Ostrom's Institutional Analysis and Development IAD framework. This framework aids in understanding how various institutions regulate their rules (Figure 6). It is particularly applicable to scenarios where there is a potential risk of depleting universally accessible resources, like fish in the ocean or trees in a forest.

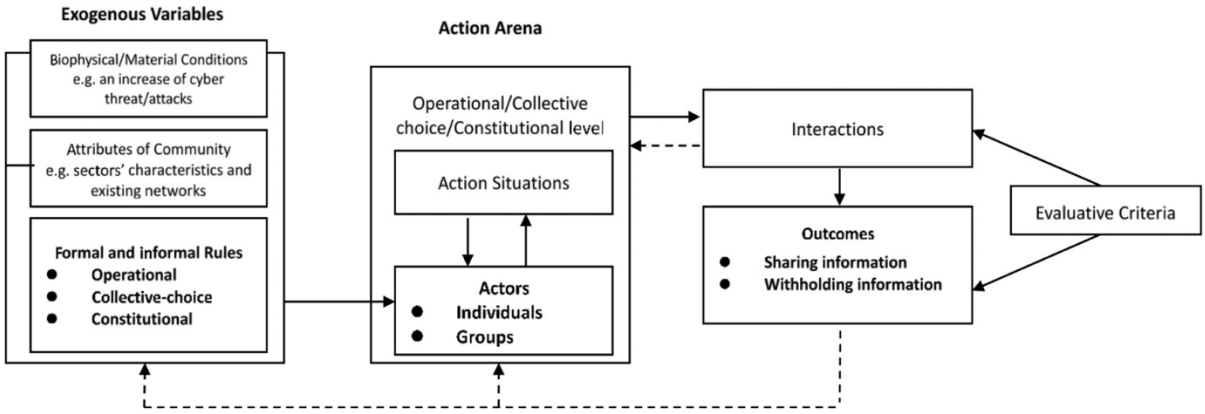

Figure 6: Ostrom's adapted Institutional Analysis and Development IAD framework, modified by authors (Chang & Huang, 2023)

This risk arises when the users lack effective communication or collective decision-making capabilities regarding resource management, as "*rules-in-use are determined from an interactive top-down and bottom-up mechanism*" (Chang & Huang, 2023, p. 4). Drawing a parallel to the internet, which is also a universally accessible resource with immense potential and significant risks, such as cyber-attacks, the IAD framework can be effectively applied for its study. Previously, this framework was used to analyse how groups work together and create rules for managing natural resources, to understand how to manage the global network of connected devices known as the Internet of Things and how to build a cooperative network using blockchain technology (Chang & Huang, 2023). The main insight of this research is that "*institutional arrangements should be understood holistically across the three levels of rule-making logic: legal/ constitutional level, organisational/ collective-choice level and operational level*" (Chang & Huang, 2023, p. 12).

6. Expected Contributions

Expected contributions rely on both theoretical and practical development of the topic inter-organisational cybersecurity governance. Practically, the research will provide guidelines for designing effective cybersecurity governance systems, identify best practices, and offer solutions for challenges. The findings will aid policymakers, cybersecurity professionals, and organisational leaders in improving collaboration and coordination across organisational boundaries, ensuring more resilient cybersecurity strategies.

References

Bobbert, Y., & Mulder, H. (2013). Group Support Systems Research in the Field of Business Information Security; a Practitioners View. In R. Sprague (Ed.), *PROCEEDINGS OF THE 46TH ANNUAL HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES* (pp. 589–598). IEEE. https://doi.org/10.1109/HICSS.2013.244

Carminati, B., Ferrari, E., & Rondanini, C. (2018). Blockchain as a platform for secure inter-organizational business processes. In *2018 4TH IEEE INTERNATIONAL CONFERENCE ON COLLABORATION AND INTERNET COMPUTING (CIC 2018)* (pp. 122–129). IEEE COMPUTER SOC. https://doi.org/10.1109/CIC.2018.00027

Chang, K., & Huang, H. (2023). Exploring the management of multi-sectoral cybersecurity information-sharing networks. In *GOVERNMENT INFORMATION QUARTERLY* (Vol. 40, Issue 4). ELSEVIER INC. https://doi.org/10.1016/j.giq.2023.101870

Crowther, K. G. (2014). Understanding and Overcoming Information Sharing Failures. In *JOURNAL OF HOMELAND SECURITY AND EMERGENCY MANAGEMENT* (Vol. 11, Issue 1, pp. 131–154). WALTER DE GRUYTER GMBH. https://doi.org/10.1515/jhsem-2013-0055

Deljoo, A., van Engers, T., Koning, R., Gommans, L., & de Laat, C. (2018). Towards Trustworthy Information Sharing by Creating Cyber Security Alliances. In *2018 17TH IEEE INTERNATIONAL CONFERENCE ON TRUST, SECURITY AND PRIVACY IN COMPUTING AND COMMUNICATIONS (IEEE TRUSTCOM) / 12TH IEEE INTERNATIONAL CONFERENCE ON BIG DATA SCIENCE AND ENGINEERING (IEEE BIGDATASE)* (pp. 1506–1510). IEEE. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00213

Fabian, B., Ermakova, T., & Junghanns, P. (2015). Collaborative and secure sharing of healthcare data in multi-clouds. In *INFORMATION SYSTEMS* (Vol. 48, pp. 132–150). PERGAMON-ELSEVIER SCIENCE LTD. https://doi.org/10.1016/j.is.2014.05.004

Fantino, B. (2018). *Quels élements d'influence pour l'adoption symbolique de la sécurité des systèmes d'information?* [These de doctorat, Aix-Marseille]. https://www.theses.fr/2018AIXM0586

Ghadge, A., Weiss, M., Caldwell, N. D., & Wilding, R. (2020). Managing cyber risk in supply chains: A review and research agenda. In *SUPPLY CHAIN MANAGEMENT-AN INTERNATIONAL JOURNAL* (Vol. 25, Issues 2, SI, pp. 223–240). EMERALD GROUP PUBLISHING LTD. https://doi.org/10.1108/SCM-10-2018-0357

Harbers, M., Bargh, M., Pool, R., Van Berkel, J., Van den Braak, S., & Choenni, S. (2018). *A Conceptual Framework for Addressing IoT Threats: Challenges in Meeting Challenges*. http://hdl.handle.net/10125/50166

ISO/IEC 27032:2012(en), Information technology—Security techniques—Guidelines for cybersecurity. (n.d.). Retrieved 27 March 2024, from https://www.iso.org/obp/ui/

Kapucu, N. (2012). Disaster and emergency management systems in urban areas. In *CITIES* (Vol. 29, Issues 1, SI, pp. S41–S49). ELSEVIER SCI LTD. https://doi.org/10.1016/j.cities.2011.11.009

Morçöl, G. (2014). Self-Organization in Collective Action: Elinor Ostrom's Contributions and Complexity Theory. *Complexity, Governance & Networks*, *1*(2), 9. https://doi.org/10.7564/14-CGN14

Naicker, V., & Mafaiti, M. (2019). The establishment of collaboration in managing information security through multisourcing. In *COMPUTERS & SECURITY* (Vol. 80, pp. 224–237). ELSEVIER ADVANCED TECHNOLOGY. https://doi.org/10.1016/j.cose.2018.10.005

Ostrom, E. (1990). *Governing the Commons: The Evolution of Institutions for Collective Action*. Cambridge University Press.

Ramirez, R., & Choucri, N. (2016). Improving Interdisciplinary Communication With Standardized Cyber Security Terminology: A Literature Review. In *IEEE ACCESS* (Vol. 4, pp. 2216–2243). IEEE-INST ELECTRICAL ELECTRONICS ENGINEERS INC. https://doi.org/10.1109/ACCESS.2016.2544381

Tagarev, T. (2020). Towards the Design of a Collaborative Cybersecurity Networked Organisation: Identification and Prioritisation of Governance Needs and Objectives. In *FUTURE INTERNET* (Vol. 12, Issue 4). MDPI. https://doi.org/10.3390/fi12040062

Vinnakota, T. (2016). A second order cybernetic model for governance of cyber security in Enterprises. In M. Raju, D. Garg, S. Raju, & K. Raju (Eds.), *2016 IEEE 6TH INTERNATIONAL CONFERENCE ON ADVANCED COMPUTING (IACC)* (pp. 706–710). IEEE. https://doi.org/10.1109/IACC.2016.136

von Solms, B., & von Solms, R. (2018). Cybersecurity and information security – what goes where? *Information & Computer Security*, *26*(1), 2–9. https://doi.org/10.1108/ICS-04-2017-0025