A Way Forward

A Way Forward

Annukka Jokipii and Aino Rantamäki

This book comprises fourteen articles that explore the concept of information resilience from various complementary perspectives. Together, they underscore the concept's diversity and complexity, presenting information resilience as a multifaceted phenomenon. Information resilience is described as not only the capacity to respond to high-quality warnings but also the development of systems and processes to ensure the continuous flow of accurate information. Information resilience also refers to the ability of individuals, communities, and societies to withstand and recover from misinformation, disinformation, and other forms of information distortion. A state possessing information resilience can anticipate challenges, allocate resources, and take preventative action, thereby enhancing overall preparedness and reducing vulnerability good quality information plays a key role and is needed after crises and disruptions.

The book's introductory article explains the current understanding of information resilience, its nature, and its connection to different sectors of society. That article relies on the work of the IRWIN research project funded by the Academy of Finland from 2021 to 2023. The project was based on observations of changes in the security environment and information-related threats that challenge society's security of supply. Our initial understanding was that information resilience and security of information supply are the same thing. However, through the project, we have realised that they are not identical, although strongly interconnected and sharing several common features. According to our interpretation, information resilience as security of information supply refers to the ability of all actors in society to support, produce, and utilise information that is correct, accessible and timely. It is formed through cooperation between actors representing different sectors of society but cannot be accounted for by any single actor. Information resilience emphasises that successful preparedness, the formation of a common situational understanding and the prevention of information-related threats are a common concern affecting several sectors and functions of society. Thus, information resil-ience is an emergent phenomenon that arises in the interaction of different actors and elements and protects societal information security. Security of information supply refers to the structures and ways of implementing cooperation that enable that emergence.

In addition to the introduction, the book addresses several research questions organised into four themes: Resilience and preparedness; complexity, governance, and legislation; counterforces and detection of disinformation; and information resilience and collective agency. In this concluding section, we aim to compile the results and contributions of the different articles and also the ideas

for further research they present. After that, we reflect on the observations made in the articles on the results of our research project.

We would like to acknowledge the collaborative effort of the various contributors in creating this shared understanding of information resilience in the context of national security. We appreciate your insightful, profound ideas and interpretations.to unexpected events. In addition, information resilience draws attention to adaptive learning, in whichresilience in the context of crises; however, the tension between openness and security is a challenge that must be accounted for in both operations and regulation. Not all information can be shared, and some information can reveal weaknesses, but excessive secrecy can reduce the chances of cooperation, shared understanding, and building a common situational awareness. Establishing a resilient information infrastructure requires negotiating different operating logics, interests, and the common good.

Establishing Governance Structures and Legislative Measures to Foster Information Resilience

The articles on the above theme discuss various aspects of governance, regulation, and preparedness in the face of complex security-related challenges. Harri Jalonen and Petri Uusikylä focus on the concept of emergent governance and argue that traditional models fail to address the layered intricacies of the global environment. They emphasise the need for adaptability, decentralisation, learning from the past, collaboration, and co-evolution in national preparedness. Paul Barnes and Harriet Lonka discuss the importance of collaboration and coordination at the regional level to enhance resilience. They argue that embedding regional resilience in Finland demands the functional alignment of governance arrangements. Anssi Keinänen, Harriet Lonka, and Leena Jukka highlight the challenges and gaps in the legislative process in Finland and the need for improvements in legislative drafting to address complex security-related issues.

In summary, the articles presented in the second theme illuminate the tensions that spur crisis-time governance. For example, Jalonen and Uusikylä argue that emergent governance may lack the necessary structure and hierarchy to ensure there is effective decision-making and coordination during crises. Similarly, Keinänen et al. note that the focus on participatory regulation may lead to delays and inefficiencies in the legislative process. In times of crisis, swift decision-making is crucial, and too much stakeholder participation can hinder the ability to respond effectively. Consequently, collaboration may not always be the most effective approach in security governance

and in certain situations, a more centralised and top-down approach may be necessary to ensure quick and decisive action.

Detecting and Countering the Impact of Misinformation and Disinformation Campaigns

The next section includes three topics related to information resilience in national security viewed from different perspectives. Each article examines why not all information necessarily supports the functioning or security of society. Silvia Sommarberg, Maro Ketola, Aki-Mauri Huhtinen, and Teija Sederholm focus on countering and detecting disinformation, highlighting the importance of information resilience, media literacy, and debunking false information. They address the need for a wide range of countermeasures targeting different parts of society and the importance of tailoring strategies to local institutions and populations. Marko Juntunen and Olli Ruohomäki focus on countering violent extremism in the arc of instability and reflect on Iraq post-ISIS. The article concludes by empha-sising the need for viable alternatives and improvements in living conditions to counter the appeal of extremist narratives. Rebekah Rousi, Leena Kunttu, and Juhani Merilehto explore the complex relationship between governance, AI, and national security. The article argues that while regulations like the General Data Protection Regulation have been implemented, they have had unintended consequences, such as hindering innovation and favouring big tech companies. The article also explores the intersection of AI governance and national security, emphasising the importance of cybersecurity in an increasingly interconnected world. The authors conclude by suggesting that a balance must be struck between regulation and innovation to ensure both national security and technological advancement.

The articles on this theme highlight the changes in the information environment and the prerequisites they create for strengthening information resilience. Both information overproduction and false information present challenges to operating in the changed information environment. The media has its place as a filterer of information, but society's ability to strengthen citizens' information literacy is increasingly important. That ability encapsulates utilising various aids and technological solutions to make information meaningful and useful. The articles also link to the theme of transparency discussed previously. Alternative perspectives may argue that the balance between regulation and innovation should favour regulation to ensure the protection of individual privacy, prevent the concentration of power in the hands of big tech companies, and mitigate the potential risks associated with AI systems. There is also an argument for stronger regulations, ethical frameworks, and accountability mechanismsto govern the use of AI in national security and

beyond. Nevertheless, innovation and flexible planning are seen as one of the key ways to strengthen crisis-resilient preparedness.

Fostering Collective Agency Among Stakeholders to Enhance Information Resilience and National Security

The final theme encompasses articles that address the roles of citizens and communities in building information resilience. Valdemar Kallunki contributes to information resilience by emphasising the importance of involving all of society in preparedness. He introduces the concept of a relational infrastructure to understand the interdependencies between informational infrastructures, societal institutions, and citizens. He also discusses the challenges of misinformation and disinformation, the need for informational integration, relational work, and relational openness in promoting information resilience. Jan-Erik Johanson, Alisa Puustinen, and Oliver Saal explore how risk perceptions are structured in the human mind and present a cognitive network model of risk perception. They also present the connections between different components of risk perception. Understanding that concept could help inform risk prevention and preparedness efforts. Pasi Mäenpää, Maija Faehnle, and Henrietta Grönlund discuss the role of civil society in information resilience and crisis management. Their article emphasises the importance of collective informational capacity in local communities and explains how it contributes to the resilience of society.

In summary, the articles under the last theme highlight the need to involve citizens in promoting security and preparedness, which is also presented in the Security Strategy for Society (2017). Information-related preparedness must be a joint effort with citizens and not just for them. The articles highlight the dualistic nature of the information infrastructure. Although infrastructure often refers to different structures and, for example, functional telecommunications connections, the relative infrastructure formed by different relationships and networks also plays a key role in it. The finding resonates with our idea of the interplay between information resilience and the security of information supply.

Future Research Steps and Further Ideas

In addition to insightful findings, the articles offer a wide variety of future research agendas. We found that the ideas were connected to three specific themes, namely (1) challenges and

opportunities related to the openness of information, (2) collaborative governance and inclusion of citizen knowledge, and (3) the role of technology. The challenges related to the openness of information are discussed in the articles in this book from, for example, the perspective of regulation. In addition, transparency is challenged by, for example, risks related to companies' business operations. However, social security of supply relies heavily on companies and the operations of the National Emergency Supply Agency. The role of companies in building information resilience should be studied in more detail in the future. The inclusion of companies is also related to the previously mentioned observation about the systemic nature of information resilience and constructing it being a matter of voluntary national preparedness. Information resilience as a systemic phenomenon highlights the fact that its construction is based on collective action and networks supporting interaction. The responsibility for enhancing it cannot be placed on any single actor, an understanding that underlines the importance of citizens' actions. Getting citizens involved in preparedness is an important, but still limited, way of strengthening preparedness work and crisis resilience. As prior research reports, technology undeniably plays a role in building information resilience. Various technological solutions, such as social media and generative artificial intelligence, the benefits and opportunities they produce, and the challenges involved in their use will be key research topics in the future.

This book sets out to advance the understanding of the role of information resilience in the context of national preparedness and the security of supply in a complex environment. The underlying proposal is that traditional governance and regulation models must be challenged to enhance information resilience. Overall, this book presents a diverse set of complementary articles that build a picture of the complex emergence of information resilience: a phenomenon with multiple interconnected factors. We are convinced that the holistic view we have developed highlights the various aspects of information resilience and ways of strengthening its emergence in a way that will benefit researchers, decision-makers, and practitioners alike.