

Civil Protection, Disaster Management, and Resilience

TEXTBOOK

Raul Savimaa *Editor*

Geopolitical and Security Issues in Risk Management

OPEN ACCESS



 Springer

Civil Protection, Disaster Management, and Resilience

Volume 6

Editor-in-Chief

Thomas Glade , Department of Geography and Regional Research, University of Vienna, Vienna, Austria

Editorial Board

Peter Billing , Department of Geography, University of Bonn, Bonn, Germany

Aurélia Bony-Dandrieux , Institut des Sciences des Risques, École des Mines d'Alès, Alès, France

Caroline McMullan , DCU Business School, Dublin City University, Dublin, Ireland

Raul Savimaa , Research Centre of Internal Security, Estonian Academy of Security Sciences, Tallinn, Estonia

Lothar Schrott , Department of Geography, University of Bonn, Bonn, Germany

Emanuele Sommario , Dirpolis Institute, Scuola Superiore Sant'Anna, Pisa, Italy

Cees J. van Westen , Faculty of Geo-Information Science and Earth Observation, University of Twente, Enschede, Overijssel, The Netherlands

Assistant Editors

Annika Fröwis , Department of Geography and Regional Research, University of Vienna, Vienna, Austria

Sophia Sternath , Department of Geography and Regional Research, University of Vienna, Vienna, Austria

Landslides, floods, pandemics, geopolitical unrest—disasters are increasing in frequency, severity, complexity, and emerging in unexpected locations. Addressing these escalating challenges demands comprehensive knowledge, innovative concepts, advanced methodologies, and resilience-building strategies.

The new book series, *Civil Protection, Disaster Management, and Resilience*, offers essential insights, practical tools, and proven best practices for navigating today's multifaceted risk landscapes. The series launches with seven foundational volumes aligned with the EU's EUMA postgraduate curriculum, serving as a critical resource for foundational and advanced education and real-world applications. For more details about the EUMA curriculum and its objectives, visit the EUMA homepage (<https://postgraduatecenter.univie.ac.at/en/euma>).

This book series serves as a foundational resource for professionals across various fields of Disaster Risk Management, as well as for students and researchers in related disciplines.

Looking ahead, the series remains open to new contributions, inviting academics and practitioners to expand its scope with fresh perspectives and emerging ideas. Whether you are shaping policy, advancing academic research, or implementing solutions on the ground, this series equips you to address the underlying causes and key drivers of today's dynamic risks, fostering safer, more resilient societies.

Interested in contributing? Contact the publishing editor or the assisting editor (euma@univie.ac.at) to join this vital and evolving initiative.

Raul Savimaa
Editor

Geopolitical and Security Issues in Risk Management



Funded by
the European Union



Springer

Editor

Raul Savimaa 

Research Centre of Internal Security Institute

Estonian Academy of Security Sciences

Tallinn, Estonia



ISSN 3059-2704

ISSN 3059-2712 (electronic)

Civil Protection, Disaster Management, and Resilience

ISBN 978-3-032-13839-2

ISBN 978-3-032-13840-8 (eBook)

<https://doi.org/10.1007/978-3-032-13840-8>

This work was supported by the University of Vienna and the Estonian Academy of Security Sciences.

© The Editor(s) (if applicable) and The Author(s) 2026. This book is an open access publication.

Open Access This book is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this book are included in the book's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the book's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

Unless otherwise expressly agreed by the Publisher in writing, the Publisher does not authorize use or reproduction of all or any part of this work in any manner for the purpose of training, fine-tuning, evaluating, or developing artificial intelligence models, technologies, or systems. In accordance with Article 4(3) of the EU Directive 2019/790 on copyright and related rights in the Digital Single Market, the Publisher expressly reserves all rights with respect to this work under the text and data mining exception of the directive.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Cover Image: © Estonian Academy of Security Sciences Image Archive

Disclaimer: Funded by the European Union. However, the views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

If disposing of this product, please recycle the paper.

Foreword by the Commissioner to the EUMA Book Series Volumes

Crises today are more complex and interconnected than ever before.

The world is warming at an unprecedented pace, especially in Europe, with global temperatures now approaching 1.5 °C above pre-industrial levels. In this context of growing geopolitical uncertainty, the need for strong preparedness and response systems has never been clearer.

Recent record-breaking wildfires, floods and other extreme weather events—all linked to climate change—illustrate the mounting impact of a heating planet and the urgency of building resilience not only to natural disasters but also to human-made crises such as conflict.

One of the European Commission's top priorities is to strengthen crisis management and civil preparedness across Europe—to move from reacting to crises to being ready for them. This means fostering a genuine culture of preparedness and resilience, one that is woven into every part of our societies—from schools and communities to governments and businesses.

But we cannot do this alone. Collaboration is key—and the academic community has a crucial role to play. By educating students and practitioners in Disaster Risk Management, universities help us raise awareness, build a shared understanding of the risks we face and inspire the innovation and mindset needed to turn preparedness into a way of life.

This book series marks an important milestone for the EUMA project—Creating a European Higher Education Network for Master's Programmes in Disaster Risk Management—and for the postgraduate Master's degree in International Disaster Management and Civil Protection it has developed.

Supported by the EU's preparedness capacity-building tools, the EUMA series represents a renewed drive to bring research, innovation and practical action closer together. It reflects the European Commission's commitment to embedding knowledge-based strategies into preparedness and response, and demonstrates the concrete value of EU programmes that strengthen our collective resilience.

The Preparedness Union Strategy is our compass—guiding us towards a new level of collective readiness that is proactive, interconnected and truly integrated.

This book series supports one of its key actions: bringing preparedness into education. By focusing on higher education and developing a robust Master’s programme, the EUMA project has helped build a holistic approach to preparedness—one that equips future generations with the knowledge and skills needed to manage disaster risks effectively.

I want to warmly congratulate all those who contributed to this series. I am confident that your work will offer valuable insights for our shared mission—a safer and better-prepared Europe.

As the risks we face become ever more complex, we remain committed to deepening partnerships with academic and research institutions, and to promoting lifelong learning. Together, we can harness knowledge and innovation to build a resilient Europe—one that is always ready for what lies ahead.



Brussels, Belgium

Hadja Lahbib
European Commissioner for Equality
Preparedness and Crisis Management

Funding Acknowledgements

This publication is part of the Springer book series *Civil Protection, Disaster Management, and Resilience*. The first seven open access volumes were developed within the project:

EUMA—“Creating a European Higher Education Network for Master’s Programmes in Disaster Risk Management” (2024–2025).

The project has received funding under the **Knowledge for Action in Prevention and Preparedness (KAPP) Call 2023** within the **Directorate-General for European Civil Protection and Humanitarian Aid Operations (ECHO)—Union Civil Protection Mechanism (UCPM)** programme of the **European Commission** (Grant Agreement No. 101140384).

The publication of this volume has only been made possible through the generous support of this programme.

Within the framework of the EUMA project, a curriculum for a new international Master’s programme (M.Sc.) has been developed. The postgraduate Master programme, entitled **“International Disaster Management and Civil Protection”**, will be launched in **October 2026** at the **Postgraduate Center of the University of Vienna**.

Building on the outcomes of EUMA, the follow-up project **EUMaPlus—“Creating Open Access Digital Educational Material in Disaster Risk Management and Civil Protection” (2026–2027)** is developing open access teaching and learning materials.

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

How to cite this volume:

Savimaa R., (Ed.) (2026): *Geopolitical and Security Issues in Risk Management*. In: Glade T., Billing P., Bony-Dandrieux A., McMullan C., Savimaa R., Schrott L., Sommario E., van Westen C.J. (Series Eds.): *Civil Protection, Disaster Management, and Resilience* (Vol. 6), Springer Nature: Heidelberg. <https://doi.org/10.1007/978-3-032-13840-8>

How to cite a chapter in this volume:

Savimaa R., (2026): Introduction to Geopolitical and Security Issues in Risk Management. In: Savimaa R., (Ed.): *Geopolitical and Security Issues in Risk Management*. (Vol. 6), Springer Nature: Heidelberg, pp 1–41.

Contents

1	Introduction to Geopolitical and Security Issues in Risk Management	1
	Raul Savimaa	
2	Contemporary Challenges and Needs for Civil Protection Due to Geopolitical Security Threats in Europe: The Case of Estonia	5
	Andres Parve and Jaan Tross	
2.1	Introduction	6
2.2	Current Geopolitical Security Threats in Europe	7
2.3	Contemporary Challenges for Civil Protection	9
2.4	EU Strategic Directions and Future Perspectives	11
2.5	The Estonian Experience	12
2.6	Conclusions and Recommendations	17
	References	18
3	Balancing Transparency and Security: Ensuring Chemical Safety in the European Union Amid Evolving Geopolitical Tensions	21
	Reelika Kuusik and Reet Kasepalu	
3.1	Introduction	22
3.2	Regulatory Frameworks for Chemical Safety in Europe	23
3.2.1	The SEVESO Directive	23
3.2.2	The TEIA Convention	24
3.3	The Geopolitical Dilemma: Transparency Versus Security	26
3.4	Strategies for Balancing Transparency and Security	27
3.4.1	Selective Transparency	27
3.4.2	Strengthening Cross-Border Trust and Cooperation	28
3.4.3	Case Study Examples from Estonian Enterprises	29
3.5	Conclusion	30
	References	31

4	ICT Use for Public Risk Management as a Societal Security Risk in the Digitally Enhanced State	35
	Jaanika Puusalu	
4.1	Introduction	36
4.2	Context, Motivation, and Scope	38
4.2.1	The Digitally Enhanced State and Society	38
4.2.2	Risk Management, Societal Resilience and the Importance of Path Acceptance	40
4.3	Concerns with Dependence on ICT Tools and Means	41
4.3.1	Users and Adoption-Related Concerns	41
4.3.2	The Four Phenomena Hindering ICT Adoption	41
4.3.3	Technology Use and Accessibility-Related Concerns	43
4.4	Mitigating Concerns	45
4.5	Conclusion	48
	References	48
5	The Potential Connections Between Civil Defence and the Cultural Sector	53
	Aule-Merlin Vihlver	
5.1	Introduction	54
5.2	Interdisciplinary Approaches to Civil Defence	54
5.3	Civil Defence in Estonia	55
5.4	Collaboration Between Civil Defence and the Cultural Sector: Opportunities and Challenges	57
5.4.1	Perspectives of Cultural Workers on Resilience Centres	60
5.4.2	Cultural Centres as Resources for Civil Defence	61
5.5	Conclusion	62
	References	63
6	Geopolitical Dynamics and Disaster Risk Management: Involvement of Third Countries in the COVID-19 Response in Italy	65
	Georg-Henri Kaup	
6.1	Introduction	66
6.2	Methods	67
6.2.1	Design and Scope	67
6.2.2	Data Sources and Sampling	67
6.2.3	Coding and Analysis	68
6.2.4	Limitations and Validation	68
6.2.5	Ethics and Data Availability	69
6.3	Geopolitical Context of the COVID-19 Crisis in Italy	69
6.3.1	Italy's Geopolitical Positioning Pre-COVID-19	69
6.3.2	Initial Impact of the COVID-19 Pandemic	71

6.3.3	The EU's Lack of Coordinated Response	71
6.4	Key Third-Country Interventions	72
6.5	Impact of Third-Country Involvement	72
6.6	Geopolitical Implications of Third-Country Involvement	74
6.6.1	Italy's Geopolitical Alignment	74
6.6.2	Impact on EU Unity	74
6.7	Critical Analysis of Disaster Diplomacy	75
6.8	Lessons Learned and Recommendations	76
6.8.1	Lessons	76
6.8.2	Recommendations	77
6.9	Conclusion	77
6.9.1	Summary of Findings	77
6.9.2	Final Reflections	78
6.10	Perspectives	78
6.10.1	Outlook for International Cooperation in Health Emergencies	78
	References	78
7	Resilience and Service Continuity for Vital Services Providers in Multimodal Crises	83
	Jaanus Kaugerand, Taivo Kangilaski, and Raul Savimaa	
7.1	Introduction	84
7.2	Risk Management of Multimodal Crises Perspective	85
7.2.1	Systemic View of Multimodal Crises	85
7.2.2	Risk and Crisis Management for Vital Service Providers	87
7.3	Factors to Consider When Designing a Crisis Response System for an Organization	89
7.3.1	Integrated Management Systems for Organizations	89
7.3.2	NIS 2 Directive	89
7.4	Scenario-Based Risk and Crisis Management for Multimodal Crises ...	90
7.4.1	Integrated Risk Management and the Need for Systemic Approaches	90
7.4.2	Using a Scenario-Based Approach for Crisis Management	93
7.4.3	Implementation of the Integrated Approach	94
7.5	Conclusions	95
	References	95
8	Disaster and Crisis Preparedness of Communities	99
	Raul Savimaa	
8.1	Introduction	100
8.2	Crisis Management with Communities	102
8.2.1	Levels of Crisis Management	102

8.2.2	Municipalities in Emergency Management	103
8.3	The Role of Communities in Crisis Preparedness	104
8.3.1	The Importance of Communities	104
8.3.2	Community Associations as Supporters of Crisis Management	106
8.3.3	The Potential of Prepared Communities	107
8.4	Case Study on Crisis Preparedness of Communities	108
8.4.1	Readiness for Crisis Management in Municipalities	108
8.4.2	Crisis Preparedness Studies in Muuga and Harku	110
8.4.3	Crisis Readiness of Estonian Community Associations	112
8.5	Conclusions	114
	References	115

Editor and Contributors

About the Editor

Dr. Raul Savimaa is a researcher and consultant specializing in community resilience, environmental security, and crisis preparedness. He is a research fellow in the Internal Security Institute at the Estonian Academy of Security Sciences and Editor-in-Chief of *Security Spectrum: Journal of Advanced Security Research*. With over thirty years of experience in security, civil protection, and environmental education, he combines systems thinking and modeling of heterogeneous time-critical multi-actor systems with applied research to strengthen sustainability and societal resilience. His work bridges academic and practical domains, contributing to numerous Horizon Europe, European Defense Agency, and national projects focused on risk governance, civil protection education, and the development of resilient communities across Europe.

Contributors

Taivo Kangilaski Laboratory for Proactive Technologies, Institute of Software Science, Tallinn University of Technology, Tallinn, Estonia;
Eesti Energia AS, Tallinn, Estonia

Reet Kasepalu Rescue College, Estonian Academy of Security Sciences, Tallinn, Estonia

Jaanus Kaugerand Laboratory for Proactive Technologies, Institute of Software Science, Tallinn University of Technology, Tallinn, Estonia

Georg-Henri Kaup Research Centre of the Internal Security Institute, Estonian Academy of Security Sciences, Tallinn, Estonia

Reelika Kuusik Estonian Rescue Services Agency, Tallinn, Estonia

Andres Parve Rescue College, Estonian Academy of Security Sciences, Tallinn, Estonia

Jaanika Puusalu Research Centre of Internal Security Institute, Estonian Academy of Security Sciences, Tallinn, Estonia

Raul Savimaa Laboratory for Proactive Technologies, Institute of Software Science, Tallinn University of Technology, Tallinn, Estonia;
Research Centre of Internal Security Institute, Estonian Academy of Security Sciences, Tallinn, Estonia

Jaan Tross Rescue College, Estonian Academy of Security Sciences, Tallinn, Estonia

Aule-Merlin Vihlver Estonian Academy of Security Sciences, Tallinn, Estonia



Introduction to Geopolitical and Security Issues in Risk Management

1

Raul Savimaa 

Abstract

The Europe's security landscape changes in response to converging geopolitical, technological, and environmental risks. Triggered by a number of recent transboundary crises such as migration, pandemics, and hybrid threats, the European Union faces increasing pressure to enhance resilience, strategic autonomy, and crisis preparedness. Traditional, state-centric risk management models are insufficient for addressing complex, interconnected polycrises that span sectors and borders. Case studies highlight the need for integrated, adaptive, and community-based approaches. There is emphasised the importance of inclusive governance, cross-sectoral coordination, and societal engagement in strengthening resilience. The focus is on the need for systems-based, flexible strategies that align technological capabilities with socio-political realities to safeguard stability, cohesion, and democratic integrity.

Keywords

Polycrises • Geopolitical security • Risk management • Comprehensive national defense • Civil protection

Over the past decade, Europe has undergone a profound transformation in its geopolitical and security landscape. A continent long associated with post-Cold War stability

R. Savimaa (✉)

Research Centre of Internal Security Institute, Estonian Academy of Security Sciences, Tallinn, Estonia

e-mail: raul@savimaa.eu

© The Author(s) 2026

R. Savimaa (ed.), *Geopolitical and Security Issues in Risk Management*, Civil Protection, Disaster Management, and Resilience 6, https://doi.org/10.1007/978-3-032-13840-8_1

1

and progressive integration is now confronting a convergence of systemic risks that transcend national borders and challenge traditional modes of governance. Russia's full-scale invasion of Ukraine in 2022 marked a pivotal rupture in the European security order, reintroducing military aggression as a tool of foreign policy and intensifying strategic uncertainty across the continent. The reverberations of this conflict extend far beyond Eastern Europe, reshaping the calculus of collective defense, civil protection, and crisis preparedness across the European Union and its neighborhood.

Concurrently, the European Union has faced a series of transboundary crises, from the 2015 migration wave to the COVID-19 pandemic and a persistent barrage of hybrid threats including cyberattacks, disinformation, and sabotage. These crises were complex, nonlinear, and cascading in nature. They expose structural weaknesses in Europe's capacity to respond coherently across member states and sectors. They also underscore the growing interdependence of natural, technological, and geopolitical risks in shaping public safety, political cohesion, and societal resilience.

The emergence of a multipolar world order has further complicated Europe's strategic environment. The EU faces mounting pressure to strengthen its strategic autonomy and operational readiness. This includes reevaluating the scope and scalability of its Common Foreign and Security Policy (CFSP), enhancing the resilience of its critical infrastructure, and integrating civilian, military, and societal dimensions of risk management.

Particularly for member states on the EU's eastern frontier, such as Estonia, Latvia, Lithuania, and Poland, the return of great power competition has catalyzed comprehensive national defense reforms. These encompass not only military preparedness but also civil defense, public communications, and the safeguarding of democratic institutions against foreign interference. Simultaneously, Southern Europe confronts climate-induced disasters with increasing frequency, while Central European states contend with energy security, migration pressures, and cyber vulnerabilities. This geographic variability highlights the need for differentiated but coordinated security strategies within the EU framework, including civil protection and civil defense.

Moreover, hybrid threats have become central to Europe's security concerns. The threats and actions may be intentional, ambiguous, and often below the threshold of conventional warfare. From sabotage of critical infrastructure to information manipulation and covert financial influence, these threats erode trust in institutions and strain the social fabric. The European Union and NATO have responded by intensifying collaboration, particularly on cybersecurity and the protection of undersea cables, energy systems, and transportation networks. Still, significant governance and capability gaps persist, especially in translating strategic concepts into localized, interoperable, and inclusive preparedness mechanisms.

This altered geopolitical situation also has an influence on civil protection. It emphasizes that not only should traditional areas of civil protection and assurance of public safety against natural catastrophes such as flooding, forest fires, and heat waves be considered, but also aspects of civil defense. The concept of risk management must therefore

evolve beyond technocratic models to account for the politicization of crisis response, the intersectoral nature of vulnerabilities, and the need for whole-of-society engagement. A resilient Europe will depend not only on advanced threat detection technologies or integrated command structures but also on civic education, media literacy, and adaptive governance. The interplay between geopolitics and security management is no longer a peripheral concern, but yet again a defining challenge for the continent's stability, sovereignty, and solidarity.

This book sets out to address these issues across eight chapters that explore the multidimensional nature of geopolitical and security risks in contemporary Europe. From chemical safety and digital infrastructures to cultural resilience and environmental threats, each contribution offers a focused perspective on how risk management is being reconceptualised in light of emerging challenges.

Chapter 2 by Andres Parve and Jaan Tross investigates the evolving role of civil protection in the face of Europe's growing geopolitical insecurity, using Estonia as a case study. The authors examine how transboundary crises, including military aggression and hybrid threats, challenge conventional crisis management systems. They argue for a shift from state-centric approaches to more integrated, risk-informed strategies that emphasize resilience and adaptability.

Chapter 3 by Reelika Kuusik and Reet Kasepalu explores the dilemma between transparency and security in managing chemical risks under the EU's Seveso III Directive and the TEIA Convention. As geopolitical tensions increase, the public disclosure of information about hazardous industrial sites may expose vulnerabilities to hostile actors. The chapter proposes a calibrated approach to chemical safety governance that preserves public awareness while mitigating exploitation risks through selective transparency and strengthened international cooperation.

Chapter 4 by Jaanika Puusalu discusses the implications of digital under-adoption on societal security. Highlighting the increasing reliance on ICT tools for crisis preparedness, the author warns that uneven adoption across social groups can undermine the effectiveness of digital solutions. The chapter calls for inclusive design, usability testing, and public engagement to ensure that digital risk management tools enhance rather than hinder societal resilience.

Chapter 5 by Aule-Merlin Vihlver delves into the underexplored interface between civil defense and the cultural sector. Through empirical analysis, the chapter demonstrates how community houses and cultural institutions can function as critical resilience centers during crises. By integrating cultural resources into civil protection strategies, authorities can foster local engagement, improve communication, and expand the reach of preparedness initiatives.

Chapter 6 by Georg-Henri Kaup examines the role of third-country actors, notably Russia and China, in the early COVID-19 response in Italy. The chapter illustrates how medical and logistical assistance from these powers influenced public perceptions and challenged EU cohesion. By framing these interventions as forms of "disaster diplomacy,"

the chapter offers a geopolitical reading of humanitarian aid and its potential to shift alliance structures.

Chapter 7 addresses the limitations of traditional crisis management in the face of multimodal crises. It introduces a scenario-based risk analysis model tailored to vital service providers. The chapter argues that resilience requires accounting for compound risks and resource conflicts that arise when multiple crises occur simultaneously. A systems-thinking approach is advocated to improve prioritization, coordination, and continuity planning.

Chapter 8 explores the preparedness of local communities to confront polycrises, i.e., complex, interconnected crises spanning multiple domains. Based on recent surveys and case studies, primarily in Estonia, the chapter identifies key drivers of community resilience and proposes policy measures to strengthen local-level capacities. It emphasizes the importance of decentralized governance, public–private partnerships, and targeted risk communication in enhancing crisis readiness.

Through these chapters, this volume offers a multifaceted examination of how geopolitical and security risks are reshaping crisis management and resilience-building across Europe. By spanning topics from chemical safety and digital vulnerability to cultural infrastructures and the geopolitics of humanitarian aid, the chapters collectively underscore the inadequacy of conventional, state-centric frameworks in addressing today's complex risk landscape. Instead, they advocate for more integrated, adaptive, and community-based approaches that account for both technological and socio-political dimensions of crisis response. Through empirical insights and theoretical advancements, the book contributes to a deeper understanding of Europe's evolving security environment and presents actionable strategies for fostering resilience in an era of increasingly intertwined threats.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.





Contemporary Challenges and Needs for Civil Protection Due to Geopolitical Security Threats in Europe: The Case of Estonia

Andres Parve  and Jaan Tross

Abstract

This article examines the evolving landscape of civil protection in Europe, driven by escalating geopolitical tensions, the proliferation of transboundary crises, and the acute security threats precipitated by the Russian Federation's invasion of Ukraine. As traditional state-centric and reactive disaster management models prove inadequate against complex hybrid operations and military threats, there is a critical need for a comprehensive, whole-of-society approach. Utilizing Estonia as a longitudinal case study, the research traces the nation's civil protection policy evolution from its post-Soviet re-establishment to the contemporary Civil Protection 2.0 framework adopted in 2024. The analysis highlights how recent geopolitical shocks have catalyzed a paradigm shift, leading to the integration of civil and military preparedness, increased proactive funding, and a focus on societal resilience. The findings indicate that effective transboundary crisis management requires network-based governance, sustained financial investment, and the harmonization of civil and security crisis frameworks. The paper concludes by recommending enhanced European crisis preparedness, stronger EU-NATO cooperation, and a unified strategic direction to safeguard democratic institutions and populations against multifaceted geopolitical threats.

Keywords

Civil protection • Transboundary crises • Geopolitical security • Whole-of-society approach • Disaster management • Estonia • Resilience

A. Parve (✉) · J. Tross

Rescue College, Estonian Academy of Security Sciences, Tallinn, Estonia

e-mail: andres.parve@sisekaitse.ee

2.1 Introduction

The dynamics of crises are evolving in tandem with global geopolitical shifts and the drastic impacts of climate change. Europe increasingly faces transboundary crises, including compound crises, characterized by complex and hardly predictable trajectories (Ansell 2010). A transboundary crisis is defined by its emergence, spread, and impact across geographical, political, cultural, linguistic, and legal borders. The multifaceted nature of these crises distinguishes them from traditional crises, which are often confined to the territory of a single nation-state. Systemic disruption underscores the cascading effects and interconnectedness inherent in these crises, suggesting that conventional state-centric or sector-based crisis management approaches are inherently limited. The potential for rapid escalation and unpredictable course of transboundary crises further complicates effective response efforts.

Following the end of the Cold War, the global order transitioned to a unipolar system dominated by the United States. Simultaneously, the focus of crisis response began to broaden from military threats to natural hazards and technological disasters. The concept of disaster management was developed as a cyclical process encompassing prevention, mitigation, preparedness, response, and recovery. This wider perspective on threats and the understanding of the causes and effects of natural and technological hazards led to the emergence of “disaster management” as a more holistic approach compared to the primarily defense-oriented “civil protection.” The emphasis on the disaster cycle, vulnerability, and resilience within disaster management marked a shift from a purely reactive response model toward a more proactive and risk-informed approach (Roth 2019; Wolbers et al. 2021).

Since the beginning of the 21st century, US involvement in the Wars in Afghanistan and Iraq have contributed to the weakening of its geopolitical influence (Walt 2018). This may be attributed to a number of factors, including the protracted nature of these conflicts and expenditure incurred, leading to a reduced appetite domestically for involvement in global affairs, as well as negative coverage of the campaigns damaging US credibility on the world stage. The recent re-election of Donald Trump has also resulted in changed American strategic objectives favoring a more inward-looking stance, further rendering the prospects of Europe’s security architecture uncertain. Concurrently, the growing role of new major powers such as China, India, and Russia and their cooperation within the BRICS + alliance has created an alternative geopolitical power vertical, resulting in these countries fulfilling diplomatic and military functions that were previously the preserve of the US. Russia’s invasion of Ukraine in 2022 has significantly impacted the European security environment, highlighting the need to reassess geopolitical strategies and cooperation in the region (Qaisrani 2023). At the core of this altered security landscape is an intensified confrontation between different political, economic and societal systems. The Western value system, based on human rights, democracy and the rule of law, is under pressure, while the ideological counterweight to it is increasing (Riigikogu 2025). Covert

competition has been replaced by open opposition, and the preservation of the rules-based international order is of existential importance for the European Union. In this context, the European Union's Common Foreign and Security Policy (CFSP), whose aim is to preserve peace, strengthen international security and promote democracy and cooperation, is of critical significance.

2.2 Current Geopolitical Security Threats in Europe

Geopolitically, crises have contributed to the formation of a more multipolar global system (Lehne 2020). The European Union has been affected by several significant transboundary crises in recent years: The 2015 migrant crisis represented a substantial increase in the influx of refugees and migrants into Europe, primarily from the Middle East, Africa, and Asia; in the area of cross-border health cooperation, COVID-19 exposed shortcomings in coordination and resource sharing in transboundary health policies; and to date, the EU's central role alongside the US has become weaker and more ambiguous due to the rise of other geopolitical actors. Transboundary crises are not only internal challenges for the EU but also significantly affect its role and influence worldwide.

Different regions of Europe face highly diverse risks. While Southern Europe confronts natural hazards resulting from altered weather conditions annually, member states bordering Russia directly perceive military and non-military security risks. European countries have historically approached and organized their disaster management and civil protection structures differently, reflecting their unique historical experiences, political systems, and threat perceptions. Some countries have adopted a centralized approach to emergency management and civil protection, while others prefer decentralized systems. The roles of the military and civilian authorities in disaster management and civil protection also vary across European nations. Organizational structures for disaster management and civil protection in Europe are not uniform, reflecting diverse administrative traditions.

On February 24, 2022, Russia launched a military offensive against Ukraine, creating a new security reality in Europe and the Baltic Sea region. While not all threats and opportunities have yet materialized, they will undoubtedly impact global security. This impact is not evenly distributed, with Russia's neighbors bearing the brunt of the pressure (Saar 2024). Russia's goal and interest lie in restoring spheres of influence in Europe, and the events in Ukraine demonstrate its willingness to use direct military force indiscriminately, employing hybrid activities to achieve this. Non-military means can encompass all resources available to a state that influence actions in favor of the state employing hybrid activities. Such means can include economic pressure; restricting access to energy resources; political subversion and the incitement of internal opposition; artificially induced human migration; cyberattacks; information operations; propaganda; disinformation; diplomatic pressure; and the use of special services or private military companies. In the event of hybrid attacks, an incident may initially appear unintentional,

resembling wear and tear, a technical malfunction, or an accidental occurrence (Muuga et al. 2025). A hybrid attack or hybrid campaign is a strategic decision by an adversary to conduct coordinated attacks, often, but not always, combining multiple different attack vectors. The attack is intentional, coordinated, and driven by a conscious (state-level) intent, not an exploitation of chance; actions are deliberately taken below the threshold of military conflict or the activation of NATO Article 5.

Over the past three years, Russia has orchestrated numerous attacks and disruptions, including cyberattacks, propaganda, arson and sabotage, with the aim of sowing division, undermining support for Ukraine and weakening European governments. The Associated Press has identified 59 incidents across Europe where Russia, Russia-linked groups, or its ally Belarus have been accused of cyberattacks, disseminating propaganda, planning assassinations or perpetrating vandalism, arson, sabotage, or espionage (Burrows 2025). The EU and NATO have intensified cooperation in protecting critical infrastructure, including underwater infrastructure, following Russia's full-scale war of aggression against Ukraine on February 24, 2022 (Muuga et al. 2025).

Beyond its interest in expanding its sphere of influence, Russia is undermining the European security order and in the longer term may resort to military force against EU and NATO countries. The West and Russia are entering a new security environment characterized by military confrontation, increasing the prospects of accidental or deliberate direct conflict. This new security situation revives several Cold War concepts in a new interpretation, affecting nations' independent military and domestic defenses, international relations, resilience, and strategic communication. Additionally, a more uncertain economic outlook and the potential social impacts of an economic downturn could lead to public dissatisfaction and a decline in support for state authorities. A dissatisfied populace is highly susceptible to hostile influence operations, potentially resulting in civil unrest and an increase in public order violations/crime.

The European Union's security policy possesses both strengths and weaknesses in addressing transboundary crises. Strengths include a supranational political system that allows for the delegation of authority for crisis management. In 2025, the European Union faces a new geopolitical reality where the influence of Western nations is waning. Consequently, the EU requires a new strategic direction that considers the altered international security environment. While EU civilian missions and crisis management capabilities have proven effective in the past, they are no longer sufficient in the current geopolitical context, where major powers no longer adhere to a single dominant force.

The EU's traditional focus on economic integration is inadequate for coping with the new geopolitical reality, and stronger and more decisive leadership is required (Lehne 2020). The EU must adapt to the changing geopolitical reality by strategically leveraging its economic and institutional strengths and developing a more decisive leadership style to protect its interests and values at the global level. The weaknesses of the EU's security policy often stem from the tension between national sovereignty and the need for collective action. It is frequently unclear who the critical actors are and what their mandates

entail. Governments are reluctant to delegate decision-making authority to international institutions, and EU agencies often lack decisive decision-making powers.

2.3 Contemporary Challenges for Civil Protection

Russia's invasion of Ukraine has clearly demonstrated that security crises are not limited to military conflict but also trigger humanitarian crises, natural hazards, and economic shocks. The current situation reflects geopolitical warfare, where security policy is closely intertwined with geopolitical interests. The EU must therefore strengthen its preparedness and crisis management capabilities, encompassing both civilian and military readiness.

This field has undergone various developments since World War I, evolving to the comprehensive “whole-of-society” approach to civil protection observed today (Tross [2023a, b](#)). The aim of civil protection is to safeguard people and society in crisis situations during both peacetime and wartime. Civil protection is predicated on individuals' capacity to protect themselves and assist each other in times of crisis until help arrives. Today, disaster management and civil protection are increasingly converging, with civil protection often viewed as an essential component of broader disaster management efforts. In many areas, such as preparedness, early warning systems and emergency response, the responsibilities of disaster management agencies and civil protection organizations overlap. However, distinct areas of focus or organizational structures may remain that differentiate disaster management and civil protection in contemporary Europe.

Research methods in civil protection are extensive, covering topics ranging from crisis management and agreed-upon areas of civil protection (sheltering, evacuation, early warning) to cybersecurity and crisis communication. A primary focus of research has been on crisis management competencies such as sensemaking, a process through which individuals or groups attempt to understand a complex or ambiguous situation (Wolbers [2021](#)). Distributed sensemaking considers the complexity that arises when multiple groups simultaneously try to comprehend a situation. Ethical–political leadership is also a crucial element of crisis management (Jungwon and So [2022](#)). American management theorists distinguish between the concepts of crisis management and emergency management in the public sector (Kapucu and Van Wart [2011](#)). According to them, crisis management is more of a response function than a planning function, involving the management of change characterized by surprise due to the unexpectedness or magnitude of the event, a short timeframe, and critical importance in terms of life-and-death decisions or organizational threat.

Contemporary crises are far-reaching and necessitate a “whole-of-society” approach, involving cooperation among state authorities, international organizations, private enterprises, and civil society that must be prepared for multifaceted crises that can include both natural hazards and military conflicts. In the EU context, this also implies better cooperation with NATO and the development of stronger security mechanisms.

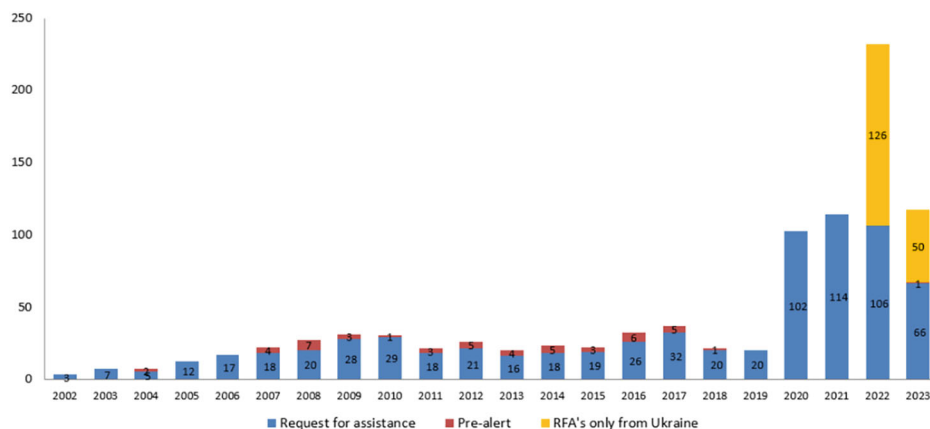


Fig. 2.1 Number of requests for assistance (RFA) to the UCPM by EU Member States and Participating States when national response capacities have been overwhelmed. (European Commission 2024)

European society faces an increasing threat from the deteriorating global security situation and the convergence of other hazards and shocks, including health and hybrid threats, earthquakes, and disruptions to critical infrastructure (European Commission 2024). While the threats are EU-wide and the need for assistance is on an upward trend (Fig. 2.1), the EU's policy and legal framework has developed to a limited extent, and the capacity for horizontal coordination in responding to crises is also lacking.

Traditional hierarchical management structures may not be sufficient for resolving transboundary crises, as these require flexibility, rapid information exchange, and collaboration among various stakeholders. Network-based governance, founded on horizontal cooperation and partnerships, offers a better approach to managing such complex situations (Ansell 2010). The success of network-based governance depends on trust, the establishment of common goals, and effective communication among the involved parties.

The Swedish Civil Contingencies Agency (MSB) has established a robust conceptual framework, asserting that society confronts a multitude of intricate threats and risks. This reality places escalating demands on preparedness and the concurrent management of diverse disruptions and events impacting society. Future preparedness and citizen resilience must address a broad spectrum of threats, ranging from accidents and natural hazards to military readiness (Swedish Civil Contingencies Agency 2023).

Furthermore, diverse engagement methods should be employed to ensure the participation of various interest groups and the diversity of their contributions. This includes interactive formats that allow participants to actively contribute and express their viewpoints. Effective communication and feedback are critical for identifying and refining capability gaps. Dialogue with participants, openness to new ideas, and a willingness to

adapt ideas based on received feedback must be maintained. This approach enhances the reliability of the analysis results and ensures broader support from stakeholders.

In this kind of situation, we should minimize hindsight bias—the systematic tendency to view past events as having been more predictable and inevitable than they were. When researchers write about crises as if their outcomes were obvious or readily preventable, they underplay the forward-looking ambiguity that decision-makers face. Depicting that ambiguity more faithfully—and analyzing events with less hindsight bias—helps practitioners appreciate that organizing under pressure is complex, contingent, and only partially controllable (Laere 2013). For crisis managers, reducing hindsight bias matters because it prevents oversimplified causal stories that misallocate blame, false confidence in one “correct” course of action, and overfitting procedures to the last event rather than preparing for non-analog futures. Accordingly, training, after-action reviews, and doctrine should foreground uncertainty and variability, not retrospective certainty; the aim is to accept and work with uncertainty rather than to narrate it away.

2.4 EU Strategic Directions and Future Perspectives

In a deteriorating security environment, it is imperative to enhance the crisis resilience of nations and populations. Within the EU, further development of a common preparedness to respond to crises and threat scenarios with severe consequences affecting the safety of member states’ populations, including military conflict, is necessary. The EU possesses several instruments to protect its interests and develop resilience; the primary issue lies in the more strategic use of existing tools and the harmonization of understanding that EU crisis resilience and security are a unified whole, and crisis resilience must be considered across all work processes. Crisis resilience ensures that the EU as an entity is harder to attack and recovers faster, whether this concerns a natural hazard, hybrid attacks or other crises. Hybrid activity presents a complex and multifaceted challenge to contemporary international security. The combined use of military and non-military means to achieve political objectives below the threshold of open conflict requires a thorough understanding and coordinated countermeasures, primarily because underestimating these multifaceted threats by perceiving them merely as “less than warfare” is a profound strategic and conceptual error (Bargaonau & Negrea-Busuioc 2024).

Several strategic documents have been prepared to strengthen the EU’s preparedness. One of the latest central guidance documents is Sauli Niinistö’s (2024) report “Stronger Together: Enhancing Europe’s Civil and Military Preparedness,” presented to the European Council in 2024. The report emphasizes that the EU and its member states’ capacity to respond to crises must be comprehensive and systemic (*Comprehensive Preparedness*). Its main objective is to ensure that the EU and its member states can continue to function under all circumstances. This comprehensive preparedness challenge is at the heart of the

report, referring to the need to strengthen Europe's ability to protect its vital governmental and societal functions against all potential threats and crises.

The principles of the Niinistö report should be reflected in future *Preparedness Union Strategy* and the *White Paper on the future of European Defence*.

The EU faces a future characterized by complex and interconnected crises driven by factors such as climate change, technological advancements, and geopolitical instability. Increasingly intricate, transboundary, and cross-sectoral crises are anticipated. This necessitates a shift from reactive management to proactive preparedness. Likely future threats include climate-induced disasters, pandemics, cyberattacks, and geopolitical conflicts. The European security landscape has changed dramatically, highlighting vulnerabilities and risks. Therefore, a proactive, integrated approach to preventing and managing these threats is required, necessitating the transcending of sectoral boundaries and the integration of civil and military preparedness.

2.5 The Estonian Experience

During the Soviet occupation, classical civil defense dominated in Estonia, based on the Soviet civil defense system. In September 1991, three weeks after the restoration of Estonia's independence, the government discussed the reorganization of the former civil defense system and decided to create a new civil protection agency under the Ministry of the Interior, the Rescue Board (Government of the Republic 1991). The Rescue Board developed a draft civil protection law, which was adopted in June 1992. The law included modern civil protection features, such as an all-hazard approach and a society-wide cooperation network, as well as several specific activities (training, early warning, evacuation, supplies, etc.) (Civil Protection Act 1992).

In 1993, the process of a more modern crisis management approach began in Estonia, and the implementation of the Civil Protection Act and the development of the field took a back seat. In 2001, a new Emergency Preparedness Act was adopted, based on the concept of crisis management, but it reflected most of the modern civil protection principles. The law included an all-hazard approach and aimed to create society's crisis management capability, covering all hazards between peace and war. For years, the concept of civil protection was overshadowed by the concepts and activities of emergency preparedness and crisis management (Emergency Preparedness Act 2000).

The creators of the Emergency Preparedness Act intended for the organization of emergency preparedness and crisis management measures to protect the population in both non-military and military crises (Emergency Preparedness Act 2000). However, the focus was only on peacetime crises. Even in the case of peacetime crises, the activities mainly focused on the distribution of tasks among state institutions responsible for crisis management, particularly in the case of so-called soft crises, and the perspective of protecting the

population was sidelined. Measures directly related to military crises were mostly undeveloped. There were several reasons for this. The goals were ambitious, and there was a lack of financial resources, as well as knowledge and experience, to implement what was stipulated in the law. Perhaps not everything stipulated in the law was important. The main issue was that there was no political or societal pressure to implement the measures, primarily due to changed priorities and the security environment (Tross 2023a, b). “Due to the reduction of military security threats and the need to build up basic capabilities for national defense and internal security, less and less attention was paid to wartime civil protection” (Civil Protection Concept 2018). In the years following the departure of Russian troops in 1995, there was also optimism about the possibility of democracy in Russia, and it seems that immediately after joining NATO, people felt safe under its protective umbrella (Tross 2023a, b). This was reflected in the security threat assessments and crisis scenarios of the time. The 2001 National Security Concept statement regarding military risk: “Estonia does not see a direct military threat to its security now or in the near future. The end of the Cold War has reduced the possibility of a military conflict affecting all of Europe and also the risk of conflict in the Baltic Sea region.” (National Security Concept 2001). The 2004 National Security Concept states: “The possibility of a military conflict affecting all of Europe and also the risk of conflict in the Baltic Sea region has been reduced to a minimum. Membership in NATO and the European Union further reduces the military threat to Estonia.” (National Security Concept 2004). The 2010 National Security Concept places a strong emphasis on terrorism and its prevention. In terms of security policy, it is emphasized that the state ensures the protection of the population in emergencies, with the goal of enhancing risk communication and supporting voluntary activities (National Security Concept 2010). The threat assessments of the time are reflected in sectoral documents. The concept for developing an early warning system, approved by the government’s crisis committee in 2006, focused only on non-military threats. For example, the use of sirens was only foreseen in companies handling hazardous chemicals and their danger zones, as well as areas where dangerous cargoes are concentrated (Rescue Board 2006). The Rescue Board’s crisis plan, completed in 2007, does include a separate evacuation annex, but it is stated that the document does not address scenarios of military threats (Rescue Board 2007). The 2009 revision of the Emergency Act further distances itself from the all-hazard approach and explicitly states that the law does not regulate preparation for crises caused by military threats (Emergency Act 2009).

The first clear sign of the need to adjust civil protection policy was Russia’s military action in Georgia in 2008. In the following years, the goal of ensuring the organization of civil protection was set in the documents of the Rescue Board. At the Rescue Board’s vision conference in 2012, it was emphasized that historically, rescue and civil protection activities have been combined in the Rescue Board, and an integrated civil protection agency must be re-established to always protect the population (Tross 2012). The Rescue Board’s 2015–2025 strategy, completed in 2014, emphasizes the cross-border problems

associated with globalization, including armed conflicts and terrorism, which the rescue field must address. One of the strategic goals is to transform the Rescue Board into a proactive civil protection organization (Rescue Board 2014).

A significant impetus for updating civil protection policy was Russia's annexation of Crimea in 2014 and the war in Donbass that began the same year (Tross 2023a, b, p. 50). The coalition agreement formed after the 2015 parliamentary elections in Estonia emphasized civil protection and informing and training people on how to act in crisis situations (Coalition Agreement 2015). To implement this activity, a civil protection working group force was formed, tasked with developing Estonia's civil protection concept (Government Action Program 2015). It was emphasized that the goal of civil protection is to raise the awareness, skills, and preparedness of the population for possible crisis situations (including terrorist activities and military conflict) and to ensure the protection of the population through the cooperation of various institutions (Civil Protection Concept 2018). At the NATO summit in 2016, national resilience requirements for enhancing civil preparedness were agreed upon, and this was reflected in the 2017 revision of the Emergency Act (Tross 2023a, b). The law was supplemented with several important civil protection measures, such as risk communication and the organization of large-scale evacuations (Emergency Act 2017).

The 2017 National Security Concept for the first time defined the goal of civil protection:

The goal of Estonia's civil protection is to protect people, the environment, and property on its territory in the best possible way during various human and natural emergencies, crises, and wartime situations. (National Security Concept 2017)

On February 15, 2018, the government approved the Civil Protection Concept by a decision of the government cabinet meeting. The concept outlined ten measures aimed at reducing the impact of crisis situations on people's lives and health and preventing or mitigating severe consequences as much as possible. The measures were supplemented with their approximate implementation costs (Civil Protection Concept 2018). The lack of a clear leading agency and financing were reasons why primarily teaching and risk communication measures were implemented from the concept during 2018–2021, and even these were not carried out consistently (Tross 2023a, b).

The COVID-19 crisis and the war in Ukraine, as well as the subsequent refugee migration, demonstrated to Estonia that the impact of a crisis can be faster and more unpredictable than society's preparedness to cope with it. The changed security situation does not only mean more attention to military defense; equally important is raising crisis resilience, or resilience in general, within the state and society. Resilience here primarily means the ability to withstand a crisis and, if necessary, adapt to a changed environment. Coping with crises and the success of actions during them depend on the preparedness of the entire society, meaning every stakeholder and sector must be prepared.

Ensuring security and resilience in the state and society is a continuous, ongoing, and purposeful activity. It must be reflected in the thinking, preparedness, actions, and cooperation of constitutional institutions, executive power, local governments, businesses, organizations, communities, and individuals.

Funding for civil protection and additional national defense was opened after Russia's full-scale military attack on Ukraine in the spring of 2022. The Estonian government decided to strengthen rescue and demining capabilities in ensuring civil protection, including large-scale evacuation, sheltering, chemical rescue, collapse rescue, demining operations, and medical capacity. Funding decisions for additional capability development and the strengthening of national defense were rapidly adopted in two stages: An initial €340 million for military defense and approximately €40 million for strengthening broad-based national defense, followed by a second tranche of €476 million euros for military defense and approximately 46 million euros for strengthening comprehensive national defense in the areas of civil protection and internal security (Government Security Cabinet 2022). For the first time, dedicated funding for the development of civil protection measures was allocated through the 2022 supplementary state budget law and the 2023 state budget law.¹ The Ministry of the Interior and the Rescue Board identified six problematic work directions for the coming years: public awareness, early warning, sheltering, large-scale evacuation, provision of critical services during wartime, and local-level crisis preparedness (Ministry of the Interior 2022).

In February 2023, the Estonian parliament (Riigikogu) approved an updated national security policy document, which states that the greatest security threat to Estonia is the Russian Federation, and that this threat is existential and long-term. The military threat to Estonia has also increased over the past year. The National Security Concept includes, for the first time, all the key principles of modern civil protection. The goal of civil protection is to increase people's preparedness to cope independently in crises, defined through an all-hazard approach aimed at protecting people in crises during both peacetime and wartime. An important principle is the cohesion and collective effort of the entire society, where all parties—individuals, communities, volunteers, entrepreneurs, local governments, and state institutions—play a crucial role. The document also includes the principle of task continuity, meaning that everyone performs their regular duties during crises and wartime. Additionally, it is foreseen that the state budget strategy will ensure continuous funding for the development of civil protection. (National Security Concept 2023, p. 2).

¹ The supplementary budget for 2022 allocated €17.4 million to the Rescue Board for the reinforcement of civil protection and crisis preparedness. Furthermore, decisions made within the framework of the state budget strategy (RES) for 2023–2026 provided an additional €33.8 million for the same objectives. During the formulation of RES 2024–2027, a total of €10.7 million was allocated to the Rescue Board for the execution of broad-based national defence tasks, of which €2.1 million was earmarked for utilization in 2024 (Ministry of the Interior 2024).

On February 22, 2024, the Republic of Estonia approved the civil protection goals and action plan for the next four years, known as the Civil Protection 2.0 framework document (civil protection policy), which follows the civil protection concept approved in 2018. While the previous concept focused mainly on natural or other civil crises from a civil protection perspective, the updated view places significant emphasis on the population's coping, prevention, and protection in the event of a military crisis. Based on the experiences of the war in Ukraine, traditional civil protection activities (public and local government crisis awareness, early warning, risk communication, evacuation, sheltering, etc.) have been supplemented with rescue and demining work, emergency aid and disaster medicine, emergency social assistance, mental health and psychosocial support during a crisis, and civil protection management. The civil protection framework document sets goals for Estonia to move toward over the next ten years to ensure the functioning of the state and the well-being of people even in the most extensive and demanding crises (Civil Protection Framework Document 2024). Over the next four years, the state will develop crisis awareness and self-sufficiency, early warning solutions, local government crisis capabilities and the business continuity of institutions involved in crisis resolution from a civil protection perspective (Civil Protection Working Plan 2024–2027 2024). The crisis resilience of the population is a priority for Estonia's European Union policy for 2023–2025 as well.

Comparing the 2018 and 2024 concepts, one of the most significant differences in risk mitigation is the absence of planned targeted funding in the earlier document and the planning of budgetary resources and/or the provision of guidelines for their planning in the new document. For example, the goal of rescue operations in wartime is to ensure the survival of human lives in accidents. The existing base budget does not allow for the resolution of long-term large-scale crises and/or preparation for military crises. The experience in Ukraine has shown that more rescue equipment, protective clothing, machinery, vehicles, etc. are consumed or destroyed in wartime. It is important to increase the continuity, autonomy, and supply security of the Rescue Board, as well as the awareness and skill level of its personnel (Civil Protection Framework Document 2024).

In conclusion, the various events of the last six years have increasingly highlighted that the existence of financial resources and the certainty that these are permanent resources are the foundation for risk prevention and crisis preparedness. There remains a need to increase the crisis resilience of the state and the population, with the focus directed toward preparedness to respond to crises, and rapid assistance in the event of threats crossing national borders, including requesting and receiving assistance in the event of major security threats.

Currently, the Estonian government has focused on actively developing the field of civil protection and allocating the necessary resources from the state budget for this purpose. An important conclusion for the future, in the context of the Ukraine-Russia war, is the continuous preparedness for crisis management and the implementation of measures

to increase societal resilience, with the overarching theme being comprehensive preparedness. This must be a broad, all-encompassing planning basis for the protection of people in both peacetime and wartime. It is necessary to create societal cohesion and a collective effort where cooperation with various partners plays a crucial role.

In the changed security environment and in the context of threat assessments, it is necessary to act quickly and decisively (see e.g., National Security Concept 2023). It is essential to find the broadest possible support in society for decisions, make critical decisions, and implement them.

2.6 Conclusions and Recommendations

Transboundary crises represent a significant and evolving threat to the security and stability of the European Union, challenging its governance structures and necessitating a fundamental reassessment of its security policy. While the EU has developed considerable crisis management capabilities, persistent weaknesses stemming from the complexity of multi-level governance and the tension between national sovereignty and the need for collective action hinder the realization of its full potential. The increasing frequency and complexity of future challenges, ranging from climate change to cyber threats and geopolitical instability, demand further strengthening of the EU's security policy through enhanced preparedness, coordination and resilience. By learning from past crises, fostering cooperation among member states and international partners, and embracing a comprehensive, whole-of-society approach to security, the EU can enhance its capacity to effectively address the dynamics of transboundary crises and safeguard its citizens and interests in an increasingly uncertain world.

Ensuring security and crisis resilience in society is a continuous, ongoing, and purposeful activity. It must be reflected in the thinking, preparedness, actions, and cooperation of constitutional institutions, the executive branch of government, local government units, businesses, organizations, communities, and individuals. Against the backdrop of Nordic initiatives, Europe is strengthening its civil defense² capabilities. It is likely that today's view of civil protection will be broadened to encompass the needs of civil defense.

The EU's security policy must evolve to respond to the rapidly changing geopolitical situation and emerging crisis threats. Key recommendations at the EU level include:

- **Harmonization of Civil and Security Crises:** Civil and security crises must be treated as a unified whole to prevent crises and respond effectively.

² In its broadest sense, civil defence constitutes non-military defence activities, while in a narrower sense, it refers to the protection of civilians during wartime. In this form, it can be found within the framework of total defence and various other national defence concepts, with the central tenet being the protection of civil society from an armed adversary.

- **Enhancing European Crisis and Defense Preparedness:** This includes strengthening both civilian structures and military readiness.
- **Strengthening EU-NATO Cooperation:** To create a common security architecture and ensure the unity of member states in security policy.
- **Promoting a More Federal Approach within the EU:** To reduce the divergence of member states' political interests and accelerate joint security decisions.

In conclusion, the EU's challenges are linked to geopolitical changes, transboundary crises, and the need to reform security policy. The Europe of the future must be stronger, more united, and strategically prepared for various threats and crises.

References

- Ansell C et al (2010) Managing transboundary crises: identifying the building blocks of an effective response system. *J Contingencies Crisis Manag* 18(4):195–207. <https://doi.org/10.1111/j.1468-5973.2010.00620.x>
- Bărgăoanu A, Negrea-Busuioac E (2024) Hybrid Warfare is Less Than Warfare: A Dangerous Illusion. <https://irregularwarfarecenter.org/publications/perspectives/hybrid-warfare-is-less-than-warfare-a-dangerous-illusion/>
- Rescue Board (2006) Raidla O, Salong R, Tross J (eds) Overview of the early warning system and possible development opportunities in Estonia. Rescue Board, Tallinn
- Burrows E (2025) Western officials say Russia is behind a campaign of sabotage across Europe. <https://apnews.com/article/russia-ukraine-war-europe-hybrid-campaign-d61887dd3ec6151adf354c5bd3e6273e>
- Civil Protection Act (1992) RT 1992, 24, 334
- Civil Protection Concept (2018) <https://kriis.ee/media/2048/download>
- Civil Protection Framework Document (2024). <https://kriis.ee/sites/default/files/documents/2024-02/Elanikkonnakaitse%20raamdokument.pdf>
- Civil Protection Working Plan 2024–2027 (2024). <https://kriis.ee/media/2485/download>
- Coalition Agreement (2015) Agreement between the Estonian Reform Party, the Estonian Social Democratic Party and the Isamaa and Res Publica Alliance on the formation of a government and the fundamentals of the coalition's action program. <https://www.err.ee/532757/taismahus-koalitsioonilepe>
- Emergency Act (2009) RT I 2009, 39, 262
- Emergency Act (2017) RT I, 03.03.2017, 1
- Emergency Preparedness Act (2000) RT I 2000, 95, 613
- European Commission (2024) Preventing and managing disaster risk in Europe. Report from the Commission to the European Parliament and the Council on progress on implementation of article 6 of the Union Civil Protection Mechanism (Decision No 1313/2013/EU). Brussels, 12.3.2024. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2024:130:FIN>
- Government Action Program (2015) Order No. 180 of the Government of the Republic of 24 April 2014. https://www.riigiteataja.ee/aktilisa/3290/4201/4007/VV_180k_lisa.pdf
- Government of the Republic (1991) Regulation on the establishment of the National Rescue Board of the Republic of Estonia. RT 1991, 31, 386

- Government Security Cabinet (2022) Minutes of the meeting of the National Defense and Crisis Management Subcommittee on April 11, 2022
- Jungwon Y, Jeon SH (2022) Leading amid pandemic: conceptual framework on ethical-political leadership for crisis management. *Public Integr* 24(7):680–691. <https://doi.org/10.1080/1099922.2021.1972610>
- Lehne S (2020) How the EU Can Survive in a Geopolitical Age. Carnegie Europe. <https://carnegieendowment.org/research/2020/02/how-the-eu-can-survive-in-a-geopolitical-age?lang=en¢er=europe>
- Ministry of the Interior (2022) Civil Protection Plan 2022–2023. <https://www.rescue.ee/files/2022-04/2022.04.06-elanikkonnakaitse-plaan.pdf>
- Ministry of the Interior (2024) Answer to a written question. 29.12.2024
- Muuga E, Loik, R, Kaup G et al (2025) Security threats to the undersea connections related critical infrastructure of the Baltic States: Baltic Sea in the focus of hybrid warfare. Estonian Academy of Security Sciences. <https://doi.org/10.15158/nv7t-kg46>
- National Security Concept (2001) RT I 2001, 24, 134
- National Security Concept (2004) RT I 2004, 49, 344
- National Security Concept (2010) RT I 2010, 22, 110
- National Security Concept (2017) RT III, 06.06.2017, 2
- National Security Concept (2023) RT III, 28.02.2023, 1
- Strengthening Europe's civil and military preparedness and readiness: Report by Special Adviser Niinistö (2024). https://commission.europa.eu/document/5bb2881f-9e29-42f2-8b77-8739b19d047c_en
- Qaisrani IH, Qazi, BH, Abbas H (2023) A Geopolitical war in Europe: Russia's invasion of Ukraine and its implications. *J Eur Stud* 39(1). <https://doi.org/10.56384/jes.v39i1.285>
- Rescue Board (2007) Rescue Board emergency response plan. Rescue Board, Tallinn
- Rescue Board (2014) Rescue Board strategy 2015–2025. Rescue Board, Tallinn
- Riigikantselei (2025) Eesti seisukohad Euroopa tsiviil- ja sõjalise valmisoleku tugevdamise kohta. 06.02.2025. <https://www.riigikogu.ee/tegevus/dokumendiregister/dokument/d912532d-24e3-48cc-97bd-2c042922da3b/>
- Riigikogu (2023) Eesti julgeolekupoliitika alused. https://www.kaitseministeerium.ee/sites/default/files/eesti_julgeolekupoliitika_alused_est_22.02.pdf
- Roth F, Prior T, Käser M (2019) Natural hazards governance in Western Europe. Oxford University Press. <https://doi.org/10.1093/acrefore/9780199389407.013.225>
- Saar J, Sinisalu A, Loik R et al (2024) The impact of Russia's alternative future developments on Estonian Security. Sisekaitseakadeemia, Tallinn. <https://doi.org/10.15158/99wh-c506>
- Research for a Safer Society. Research Agenda 2024–2028 (2023) Swedish Civil Contingencies Agency (MSB). <https://rib.msb.se/filer/pdf/30469.pdf>
- Tross J (2012) Summary of the 3rd workshop of the Rescue Board's vision conference "Safe Future". Rescue Board, Tallinn
- Tross J (2023) Development of civil protection in Estonia in the period after restoration of independence. *Turvalisuskompass: turvalisuse ja julgeoleku teadusajakiri* 4:41–61. <https://doi.org/10.15158/txa4-gd86>
- Tross J (2023) Teekond tsiviilkaitsest elanikkonnakaitсени. *Turvalisuskompass: turvalisuse ja julgeoleku teadusajakiri* (4):167–185. <https://doi.org/10.15158/s9q9-wv11>
- van Laere J (2013) Wandering through crisis and everyday organizing: revealing the subjective nature of interpretive, temporal and organizational boundaries. *J Contingencies Crisis Manag* 21(1):17–25. <https://doi.org/10.1111/1468-5973.12012>
- Van Wart M, Kapucu N (2011) Crisis management competencies: the case of emergency managers in the USA. *Public Manag Rev* 13(4):489–511. <https://doi.org/10.1080/14719037.2010.525034>

- Walt SM (2018) The hell of good intentions: America's foreign policy elite and the decline of U.S. primacy. Farrar, Straus and Giroux
- Wolbers J (2021) Understanding distributed sensemaking in crisis management: the case of the Utrecht terrorist attack. *J. Contingencies Crisis Manag.* 30:401–411. <https://doi.org/10.1111/1468-5973.12382>
- Wolbers J, Kuipers S, Boin A (2021) A systematic review of 20 years of crisis and disaster research: trends and progress. *Risk Hazards Cris. Public Policy* 12(3):374–392. <https://doi.org/10.1002/rhc3.12244>

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.



Balancing Transparency and Security: Ensuring Chemical Safety in the European Union Amid Evolving Geopolitical Tensions

3

Reelika Kuusik^{ID} and Reet Kasepalu^{ID}

Abstract

In an era of heightened geopolitical tensions, ensuring chemical safety across the European Union presents a critical dilemma: Balancing the transparency required for public safety and environmental protection with the need to safeguard sensitive information from potential security threats. The SEVESO Directive mandates EU member states to publicly disclose information about industrial sites handling hazardous chemicals, fostering transparency, and risk awareness. Similarly, the TEIA Convention obligates member states to consult neighboring countries on hazardous industrial activities with potential transboundary effects. Hereon with Russia's and Belarus' accession to the convention, this obligation takes on heightened significance, raising questions about trust, transparency, the potential misuse of publicly available data, and the reliability of cross-border information sharing in the current geopolitical climate. This chapter explores whether public transparency remains the optimal approach for chemical safety in the current security climate. It examines whether restricting access to sensitive data could reduce vulnerability to malicious actors, while acknowledging the inherent visibility of large-scale industrial sites, which cannot be entirely concealed, even from basic aerial surveillance. The chapter proposes a nuanced approach, advocating for selective transparency and reinforced international cooperation mechanisms to ensure

R. Kuusik (✉)

Estonian Rescue Services Agency, Tallinn, Estonia

e-mail: reelika.kuusik@paasteamet.ee

R. Kasepalu

Rescue College, Estonian Academy of Security Sciences, Tallinn, Estonia

e-mail: reet.kasepalu@sisekaitse.ee

both public safety and national security in chemical risk management across the EU and its neighboring regions.

Keywords

Chemical safety • Transparency • Geopolitical tensions

3.1 Introduction

Chemical safety is a critical concern in Europe due to the potential risks associated with hazardous industrial activities. The chemical, petrochemical, and metal refining industries play a crucial role in the European economy, yet they also pose significant safety and environmental hazards. Accidents involving dangerous substances can lead to catastrophic consequences, including explosions, toxic releases and contamination of water sources, affecting human health, ecosystems and infrastructure. The need for strong regulatory measures to prevent industrial disasters and mitigate their effects has been a longstanding priority within the European Union (EU) and beyond.

Ensuring chemical safety requires a delicate balance between transparency and security. Transparency is essential for public safety, as communities have the right to be informed about potential hazards, safety measures and emergency procedures. However, excessive disclosure of sensitive information—such as the locations, operational details and hazardous substances stored at industrial sites—may inadvertently create security vulnerabilities. Hostile state or non-state actors could exploit public databases, open-source intelligence (OSINT) and modern surveillance technologies to target critical infrastructure for sabotage, cyberattacks or other forms of hybrid warfare.

To address chemical safety risks, the EU and the United Nations Economic Commission for Europe (UNECE) have established two key regulatory frameworks: the Seveso III Directive and the TEIA (Transboundary Effects of Industrial Accidents) Convention. This chapter explores the complex relationship between transparency and security in chemical safety regulation. It examines:

- The evolution of the Seveso Directive and its increasing emphasis on transparency,
- The TEIA Convention's role in transboundary cooperation, as well as Russia's and Belarus' historical involvement in its framework,
- The security risks associated with public disclosure in an era of hybrid warfare, cyber threats and geopolitical instability,
- The legal and strategic challenges of restricting public information while maintaining sufficient public awareness and regulatory oversight.

By analyzing these aspects, the chapter seeks to answer a critical question: how can Europe maintain high standards of chemical safety while minimizing the risks associated with transparency in an increasingly complex geopolitical landscape?

3.2 Regulatory Frameworks for Chemical Safety in Europe

3.2.1 The SEVESO Directive

A series of major accidents in the European chemical industry in the 1970s led to long discussions in the European Parliament on the need for regulation. Although most European Union member states had national systems in place for regulating hazards at that time, it was still necessary to establish measures at the international level. The Seveso Directives aim to regulate the activities of the chemical industry (Versluis et al. 2010). Over the years, the Seveso Directive has been updated, and new requirements have been adopted to reduce the likelihood of accidents and establish a higher level of protection (Swuste and Reniers 2017):

- Seveso I directive (Council Directive 82/501/EEC of 24 June 1982)—minimum requirements were set for harmonization, focusing on the handling of hazardous substances. The main requirements included, for example: The designation of a competent authority; obligations for establishments (such as preparing documentation) and for the competent authority to prepare an external emergency response plan; the obligation to notify the European Commission of major accidents; and the maintenance of an accident database by the European Commission.
- Seveso II Directive (Council Directive 96/82/EC of 9 December 1996)—this directive supplemented the Seveso I Directive, for example: greater emphasis on domino effects; an expanded list of hazardous chemicals; the introduction of two threshold quantities; the establishment of an inspection requirement; and the introduction of land-use planning.
- Seveso III Directive (European Parliament and Council Directive 2012/18/EU, 4 July 2012; came into force on 1 June 2015)—completely replaced the Seveso II Directive. The third directive is largely linked to the implementation of the CLP Regulation. Several other amendments were made to the directive. This included modifications requiring that information be provided to the public electronically; that authorities share information with the public regarding major accidents; that public participation be required in land-use planning; and that inspection requirements be expanded.

The Seveso III Directive applies to all European Union member states as it is a European Union regulation. This means that all European Union member states must transpose this Directive into their law. Estonia has transposed the Seveso III Directive with the

Chemicals Act (Riigikogu 2015). Additionally, the Directive is also implemented in non-European Union countries such as Norway and Iceland, as well as Canada and New Zealand. The Seveso III Directive establishes a framework for preventing major accidents involving hazardous substances and mitigating their effects on human health and the environment. It aims to ensure a high and uniform level of protection across the Union through consistent and effective measures (European Parliament and Council 2012). The Seveso III Directive applies to approximately 12,000 industrial sites across the European Union that store or handle chemical and petrochemical substances or conduct metal refining processes (Hollá et al. 2021).

The Seveso III Directive places strong emphasis on transparency by mandating public disclosure of information regarding hazardous industrial sites. The Directive requires operators and authorities to ensure that the public have access to the information, such as information on safety measures and requisite behavior in the event of a major accident, general information on major-accident hazards and on potential effects on human health and the environment in the event of a major accident and the inventory of dangerous substances. Some information must be made available permanently and some upon request. Furthermore, transparency is reinforced through active public participation in the land-use planning process, thereby allowing communities to be involved in the decision-making related to industrial site development (European Parliament and Council 2012). By fostering greater openness, transparency helps to improve public awareness, preparedness and engagement in decision-making related to industrial accident prevention and emergency response.

3.2.2 The TEIA Convention

Since the early 1990s, the United Nations Economic Commission for Europe (UNECE) has concentrated its efforts on preventing industrial accidents and especially their transboundary effects in its region, which stretches from Canada and the United States of America in the west to the Russian Federation and Central Asia in the east. Its work led to the adoption of the Convention on the Transboundary Effects of Industrial Accidents (TEIA Convention) on March 17, 1992. It was signed by 26 UNECE member countries and the European Union, and entered into force on April 19, 2000. It now has over 40 contracting Parties (United Nations Economic Commission for Europe). Estonia ratified the TEIA Convention in 2000 (Piiriülese Toimega Tööstusõnnetuste Konventsiooni Ratifitseerimise Seadus 2000).

The TEIA Convention aims at protecting human beings and the environment against industrial accidents by preventing accidents as far as possible, preparing and responding to potential inland industrial accidents that have the capacity to produce transboundary effects. TEIA ultimately strives to protect nations and local people from the catastrophic

impacts of these industrial accidents. The TEIA Convention fosters proactive international collaboration among contracting Parties before, during, and after an industrial accident.

The TEIA Convention has three official languages: English, French, Russian. These languages are used for official documents, communication, and interpretation within the framework of the convention. The Russian Federation ratified the TEIA Convention in 1994 and Belarus in 2003 (United Nations Treaty Collection 1992). Both countries have actively participated in activities related to the Convention. Their members have participated in the work of the Bureau (United Nations Economic Commission for Europe) and the Working Group on Implementation (United Nations Economic Commission for Europe), but at present, their representatives no longer take part. It needs to be noted that at the last meeting of the Conference of the Parties in 2024 (COP-13), a Belarusian member once again applied for a position in the Working Group on Implementation (WGI), a subsidiary body set up to address matters related to the implementation and development of the UNECE Industrial Accidents Convention. However, no consensus was reached, and a secret vote was held, resulting in the Belarusian member not being elected to the working group. (General Secretariat of the Council 2024) The TEIA Convention assumes that all parties provide financial resources for the implementation of the workplan activities. At the COP-13 meeting, an overview of financial contributions was presented, with Russia notably absent from the report (United Nations: Economic and Social Council 2024). Russia has not contributed to the TEIA Convention since 2020. The COP-13 resources report for 2023–2024 lists country-by-country contributions and shows the Russian Federation with no entry, while the last documented payment is a July 2020 transfer of \$250,000 to a dedicated trust fund for a Central Asia project. (United Nations: Economic and Social Council 2024).

The Seveso III Directive and the TEIA Convention both focus on the prevention of major accidents involving hazardous chemicals and mitigating their consequences for human health and the environment. However, the TEIA Convention specifically addresses transboundary industrial accidents, emphasizing transparency and cooperation between countries to ensure effective accident prevention and response. While the Seveso III Directive applies to the European Union and its member states, focusing primarily on national accidents, it does not explicitly cover transboundary effects. However, transparency obligations require that affected countries be notified if a cross-border accident is likely. In contrast, the TEIA Convention has a broader geographical scope, directly addressing transboundary industrial accidents and fostering open information sharing and collaboration among nations. Together, these frameworks strengthen industrial safety and transparency, ensuring both regional and international protection against major accidents while enhancing public trust and cross-border cooperation.

3.3 The Geopolitical Dilemma: Transparency Versus Security

Hybrid warfare methods have become a widespread geopolitical tool, particularly in the context of Russia's efforts to destabilize the European Union (EU) and NATO member states without direct military confrontation. Russia's hybrid strategy includes cyberattacks, disinformation campaigns and energy coercion, all aimed at exploiting vulnerabilities and weakening Western cohesion. This has been formally acknowledged in joint statements by the European Commission and NATO, emphasizing that countering hybrid threats is now a priority in the EU's security policy (European Commission & High Representative of the Union for Foreign Affairs and Security Policy 2016; NATO 2024). One of the most prominent elements of hybrid warfare is disinformation, which Russia has systematically used to manipulate public opinion and erode trust in democratic institutions. For instance, the EUvsDisinfo platform documented over 14,000 cases between 2015 and 2023 where Russia deliberately spread false narratives targeting the EU's stability (East Stratcom Task Force 2023).

Russia, in its war against Ukraine, has demonstrated its willingness to attack civilian infrastructure, causing extensive damage to critical service providers such as power plants and district heating facilities (Kalniete and Pildegovičs 2021). These attacks are strategically aimed at deepening societal crises, instilling fear, weakening resistance, and disrupting emergency response operations. Such hybrid threats are increasingly recognized as both societal and legal challenges, typically addressed by civil authorities rather than military forces (Borch and Heier 2024). Given this pattern of targeting essential infrastructure, there is a growing concern that industries handling hazardous chemicals could become potential targets in future conflicts. A deliberate attack on chemical production or storage facilities could result in toxic releases, contamination of water supplies, and mass casualties, further exacerbating chaos and undermining public safety. A crucial challenge in addressing hybrid warfare lies in the legal and strategic limitations of international law. While hybrid operations may cause severe disruptions, they do not always constitute an "armed attack" under international law, making military retaliation legally complex (Krishnan 2024). This legal ambiguity allows Russia to operate in a gray zone, where provocative actions escalate tensions without crossing the threshold of formal warfare.

The academic world is particularly vulnerable to hybrid threats due to its openness, commitment to academic freedom, institutional autonomy and extensive global cooperation. According to EU documents, these characteristics make universities and research institutions prime targets for foreign interference, disinformation and intellectual property theft (The European Centre of Excellence for Countering Hybrid Threats 2024). However, if openness and transparency make academia susceptible to hybrid threats, could the same risks extend to broader regulatory frameworks, such as the Seveso III Directive and the TEIA Convention? Both frameworks emphasize public disclosure and cross-border cooperation, particularly regarding hazardous industrial sites and accident prevention. While

these policies are essential for safety and environmental protection, they may unintentionally create vulnerabilities by making sensitive industrial and chemical information more accessible—not just to the public but potentially to hostile state and non-state actors.

This raises a critical security dilemma: how do we balance transparency and accessibility with the need to safeguard critical infrastructure and research from foreign manipulation or sabotage? As with academia, ensuring robust security measures, controlled information access and international risk assessments may be necessary to prevent hybrid threats from exploiting well-intentioned regulatory frameworks. That said, while limiting public access to industrial data may seem like a security measure, it does not eliminate the visibility of critical infrastructure. Refineries, chemical plants, and other hazardous facilities cannot be hidden from modern surveillance tools, such as:

- **Satellite Imagery and Aerial Reconnaissance:** High-resolution satellite images are widely available, providing detailed views of industrial sites.
- **Drone Surveillance:** Even commercially available drones can be used to monitor infrastructure.
- **Publicly Available Maps and Open-Source Intelligence:** Platforms such as Google Maps, OpenStreetMap, and other geospatial tools already make industrial sites easy to locate.

Thus, even if public databases restrict certain details, key infrastructure remains identifiable. This raises the question: does restricting public databases meaningfully reduce security risks, or does it merely shift the focus from open transparency to clandestine surveillance by hostile actors?

3.4 Strategies for Balancing Transparency and Security

3.4.1 Selective Transparency

The Seveso III Directive requires operators and authorities to ensure that the public has access to necessary information, but it also requires the classification and restriction of certain types of sensitive information for security reasons. The main aim is to strike a balance between the public's right to know and the protection of critical infrastructure that could be exploited for malicious purposes. There are different approaches.

In accordance with Article 21, Paragraphs 3 and 4 of the Seveso III Directive, the European Commission has established two databases: one related to establishment data (eSPIRS (European Commission JRCentre [2023](#))) and the other concerning past accidents (eMARS (European Commission (n.d.))).

- In eSPIRS, Member States are permitted to classify certain establishment information as confidential and therefore not accessible to the public, for any reasons specified in Directive 2003/4/EC of the European Parliament and Council of 28 January 2003 regarding public access to environmental information.
- In the public version of eMARS reports, do not disclose the location or names of companies involved in accidents to prevent the database from being used for criticizing countries or companies or for legal proceedings. In a login-restricted view, the authorized person sees that information.

In the Netherlands, a map application (Interprovinciaal Overleg) is in use that provides an overview of hazards, including a specific map layer that displays the locations of Seveso establishments along with some related data. The purpose of the risk map is to enhance public awareness of environmental risks in their living areas. Another goal is to assist specialists in preventing disasters and serious accidents.

In Canada, the database ECCC E2 Online Reporting System (Government of Canada 2022) is in use, in which company data is collected, including company locations, chemical names and quantities, and other relevant information. The locations of companies are also mapped. This is a portal accessible only to registered users, such as company employees and competent authorities. The database does not have a public view. In Croatia, the PROT/OVPN register (Republika Hrvatska 2024) is in use and provides an overview of companies and past incidents. The register has both a public view and a login-restricted view. In Belgium, a dedicated website (Belgian Federal Government Seveso Risk (n.d.)) is available to the public, providing information about Seveso establishments, competent authorities, and guidelines on how to act in case of an accident. The website also includes a map application showing the locations of the establishments and a list of them.

3.4.2 Strengthening Cross-Border Trust and Cooperation

According to Article 23 of the TEIA Convention, the member parties must report periodically on the implementation of the convention. To assist all the parties in the completion of the reporting on implementation, they can use the countries' reports that were submitted during the previous rounds and which can be found on a special password-protected webpage. (UNECE).

Additionally, a dedicated website (United Nations Economic Commission for Europe) has been created, which acts as a repository for good practices reported by the committed parties and countries in their national implementation reports. This includes additional good practices identified by the WGI through its analysis of those reports and other communications. An e-tool has also been created under the leadership of the Russian Federation, which is based on a document (United Nations Economic Commission for Europe 2014) "User-friendly version of the Benchmarks for the implementation of the

residents. However, it was also acknowledged that, under the Seveso III Directive, establishments with a high risk of major accidents are required to publicly disclose information electronically about potential risks, safety measures, and recommended actions in case of an incident. Ultimately, a publicly accessible version of the data was maintained, albeit with certain restrictions: information on chemical quantities is no longer disclosed, and for pyrotechnic and explosive activities, details on operations and specific chemicals are not provided.

3.5 Conclusion

Chemical safety in Europe operates at the intersection of public transparency, regulatory oversight, and security concerns. The Seveso III Directive and the TEIA Convention have played a vital role in preventing major industrial accidents, improving emergency preparedness, and ensuring public access to safety-related information. However, the increasing complexity of hybrid threats, geopolitical tensions, and technological advancements have raised new challenges in balancing open information sharing with the need to protect critical infrastructure from potential misuse.

One of the key dilemmas in modern chemical safety governance is the tension between transparency and security. On the one hand, public disclosure of industrial hazards enhances community awareness, risk preparedness, and regulatory accountability. On the other hand, excessive transparency may expose vulnerabilities, particularly when dealing with strategic infrastructure that could become a target for cyberattacks, sabotage or geopolitical exploitation. The Seveso III Directive, for example, mandates public access to safety measures and hazardous substance inventories, a policy that strengthens industrial safety but also raises concerns about security risks in an era of heightened global instability.

While restricting public access to industrial data might seem like a viable solution to mitigate security threats, it does not eliminate the visibility of critical sites. Modern surveillance tools, including satellite imagery and drone reconnaissance, make it virtually impossible to conceal chemical facilities from potential adversaries. Belarus and the Russian Federation remain Contracting Parties to the TEIA Convention, with the attendant rights to participate in its institutions. At the same time, Belarus's 2024 candidacy for the Working Group on Implementation was not elected, and the Russian Federation has not made a financial contribution since 2020. Against this backdrop, it is prudent to foreground a governance risk: information-sharing arrangements designed for cross-border safety (e.g., hazard notifications, inventories of hazardous installations, mutual-assistance planning) may become vulnerable to strategic instrumentalization under adverse geopolitical conditions. The point is not to allege misuse, but to make explicit that TEIA's cooperative data flows require proportionate safeguards (access control, auditable use, reciprocity rules, and clear redress mechanisms) to protect their safety purpose without

eroding international cooperation. As international trust becomes increasingly fragile, regulatory bodies must reassess the security risks associated with cross-border transparency obligations.

Moving forward, chemical safety governance must evolve to address these emerging challenges. Potential solutions might include refining selective transparency policies, such as implementing tiered access models where public safety information remains available while sensitive operational details are restricted to verified authorities. Additionally, data classification frameworks within eMARS and eSPIRS, as well as national databases to prevent unintended information exposure. Security-driven resilience measures could also be enhanced by investing in cybersecurity protections for industrial facilities, particularly intrusion detection systems and industrial control systems security. Cooperation between regulatory agencies and intelligence services could be increased to mitigate hybrid threats targeting industrial sites. Information-sharing protocols within TEIA to ensure that geopolitical tensions do not compromise industrial safety cooperation, and developing regional security frameworks that address the intersection of transparency obligations and critical infrastructure protection to strengthen international trust and risk management.

The future of chemical safety governance will depend on striking a balance between public right-to-know policies and the necessity of safeguarding industrial infrastructure. The Seveso III Directive and TEIA Convention have established robust safety standards, but as geopolitical risks evolve, policymakers must ensure that regulatory transparency does not inadvertently expose Europe's chemical sector to new forms of security threats. The next phase of industrial safety policy must be guided by a nuanced approach that upholds public safety, regulatory accountability, and national security in equal measures.

References

- Belgian Federal Government Seveso Risk. (n.d.) What to Do in case of an industrial accident? In: <https://www.seveso.be/en>. <https://www.seveso.be/en>. Accessed 18 Mar 2025
- Borch OJ, Heier T (2024) Toward a hybrid threat response model. In: Preparing for hybrid threats to security. Routledge, pp 271–282
- East Stratcom Task Force (2023) Database of disinformation cases. In: <https://euvsdisinfo.eu/disinformation-cases/>
- Estonian Rescue Services Agency (n.d.) Avaandmed: Suurõnnetuse ohuga ja ohtlikud ettevõtted. In: Estonian Rescue Board. <https://www.rescue.ee/et/juhend/avaandmed/suuronnetuse-ohuga-ja-ohtlikud-ettevotted>. Accessed 18 Mar 2025
- European Commission (n.d.) About eMARS. <https://emars.jrc.ec.europa.eu/en/emars/content>. Accessed 18 Mar 2025
- European Commission & High Representative of the Union for Foreign Affairs and Security Policy (2016), Joint communication to the European parliament and the council: joint framework on countering hybrid threats—a European Union response (JOIN(2016) 18 final)
- European Commission JRCentre (2023) eSPIRS dashboard. MINERVA Portal. <https://espirs.jrc.ec.europa.eu/en/espirs/content>. Accessed 18 Mar 2025

- European Parliament and Council (2012) Directive 2012/18/EU. Official Journal of the European Union
- Government of Canada (2022) Public safety authorities user guide—environmental emergency regulations reporting system database. https://www.canada.ca/en/environment-climate-change/services/environmental-emergencies-program/public-safety-authorities-user-guide.html?utm_source=chatgpt.com. Accessed 18 Mar 2025
- Hollá K, Polorecká M, Kubás J, Ballay M (2021) Validity of the Seveso II and III directive in the EU. In: Transportation research procedia. Elsevier B.V., pp 1506–1513
- Interprovinciaal Overleg Risicokaart. (n.d.) In: <https://www.risicokaart.nl/>. <https://www.risicokaart.nl/>. Accessed 18 Mar 2025
- Kalniete S, Pildegovičs T (2021) Strengthening the EU's resilience to hybrid threats. Eur View 20:23–33. <https://doi.org/10.1177/17816858211004648>
- Krishnan A (2024) Fifth generation warfare. Dominating the human domain. Routledge Studies in Conflict, Security and Technology
- Kuusik (n.d.) Ohtlikud ja suurõnnetuse ohuga ettevõtted. In: Estonian Rescue Services Agency. <https://www.rescue.ee/et/ohtlikud-ettevotted>. Accessed 7 Oct 2025
- Kuusik R (2025) Ettevõtteväline hädaolukorra lahendamise plaan. In: Estonian Rescue Services Agency. <https://www.rescue.ee/et/ettevottevaeline-haadaolukorra-lahendamise-plaan>. Accessed 7 Oct 2025
- Maa- ja Ruumiamet (2025) X-GIS 2.0 Ohtlikud kätised, veevarustus, veeohutus. https://xgis.maaamet.ee/xgis2/page/app/paasteamet_ohtvesi. Accessed 18 Mar 2025
- NATO (2024) Countering hybrid threats. https://www.nato.int/cps/el/natohq/topics_156338.htm. Accessed 16 Dec 2024
- Republika Hrvatska (2024) Registar postrojenja u kojima su prisutne opasne tvari/Očevidnik prijavljenih velikih nesreća (RPOT/OPVN). <https://rpot.azo.hr/rpot/#>. Accessed 18 Mar 2025
- Riigikogu (2015) Chemicals act. RT I, 10.11.2015, 2
- Swuste P, Reniers G (2017) Seveso inspections in the European Low Countries: history, implementation, and effectiveness of the European Seveso directives in Belgium and the Netherlands. J Loss Prev Process Ind 49:68–77. <https://doi.org/10.1016/j.jlp.2016.11.006>
- The European Centre of Excellence for Countering Hybrid Threats (2024) Building resilience to hybrid threats: best practices in the Nordics. Hybrid CoE Working Papers c
- United Nations: Economic and Social Council (2024) Use of financial and in-kind resources to implement the workplan in 2023–2024
- United Nations: Economic and Social Council (2022) Use of financial and in-kind resources to implement the workplan in 2021–2022
- United Nations Economic Commission for Europe (n.d.) Introduction to the convention on the transboundary effects of industrial accidents. In: United Nations economic commission for Europe (UNECE). <https://unece.org/introduction-10>. Accessed 18 Mar 2025a
- United Nations Economic Commission for Europe Bureau (n.d.). In: United Nations economic commission for Europe. <https://unece.org/environmental-policy/industrial-accidents/bureau>. Accessed 18 Mar 2025b
- United Nations Economic Commission for Europe (n.d.) Working Group on Implementation. In: United Nations economic commission for Europe. <https://unece.org/environmental-policy/industrial-accidents/working-group-implementation>. Accessed 18 Mar 2025
- United Nations Economic Commission for Europe (n.d.) Good practices in implementing the industrial accidents convention. <https://unece.org/environmental-policy/industrial-accidents/good-practices-implementing-industrial-accidents>. Accessed 18 Mar 2025

United Nations Economic Commission for Europe (2014) User-friendly version of the Benchmarks for the implementation of the convention on the transboundary effects of industrial accidents. <https://unece.org/environment-policy/publications/user-friendly-version-benchmarks-implementation-convention>. Accessed 18 Mar 2025

United Nations Treaty Collection (1992) Convention on the transboundary effects of industrial accidents. In: United Nations treaty collection. https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtsg_no=XXVII-6&chapter=27&clang=_en. Accessed 18 Mar 2025

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.





ICT Use for Public Risk Management as a Societal Security Risk in the Digitally Enhanced State

4

Jaanika Puusalu 

Abstract

Recognition of the growing number of threats to both the well-functioning of the state and its individual resident's well-being has led many countries to identify and develop novel means for societal resilience-building as central components of any risk management programmes. In keeping with more general trends towards technologically and digitally enhanced states, digital and ICT solutions are widely seen as a suitable development path. Where the goal is to boost resilience through increasing crisis preparedness, any means introduced must reach as wide an audience as possible to be effective; thus, accessibility is a central consideration in their selection and development. This is reflected in the increasing popularity of relatively simple digital means such as web pages, social-media profiles and applications. Even if the introduced tools are sufficiently accessible and suitable in other ways, however, if they are to fulfil their purpose, and indeed, not undercut societal resilience, they must still be adopted for use across the relevant social groups. This chapter explores this problem of adoption or uptake and the various concerns, including security concerns that it raises.

Keywords

Risk management • Resilience • Societal resilience • Digitalisation • Digital enhancement

J. Puusalu (✉)

Research Centre of Internal Security Institute, Estonian Academy of Security Sciences, Tallinn, Estonia

e-mail: jaanika.puusalu@sisekaitse.ee

4.1 Introduction

Risk management and crisis management concerning societal threats have long been fundamental aspects of building state resilience. However, faced with growing geopolitical tensions, new security challenges, the rise of climate-change-triggered extreme weather events and the experience of a global pandemic, many states are developing new risk and crisis management measures and programmes. These programmes typically include measures to enhance societal resilience, whereby the aim is to prepare the members of society for identified possible crisis situations and enhance the capacity of society to continue functioning during them (i.e. build social crisis preparedness).¹ Information and technology tools (ICT) are at the core of many of these initiatives. Yet, more action is called for, especially in Europe (Niinistö 2024). In this regard, the European Electronic Communications Code (Directive 2018/1972) established in 2018 required states to develop a cell-broadcasting-based public warning system by 2021. By the beginning of 2024, however, several countries were still only in testing and launch phases (EENA n.d.), while an EU-wide plan for further crisis preparedness was only introduced in 2025 (European Commission 2025).

Crisis management refers to an entity's capacity to respond to crises when they happen and are ongoing. ICT introduced for this purpose ranges from complex censoring technologies to automated systems for searching for survivors and identifying (invisible) hazards at disaster sites to Internet of Things devices that can be used for real-time monitoring.² Cellular alert systems are also common solutions due to the robustness of the underlying infrastructure.³ Simple web-based means can also be an effective component of crisis-response, as they provide efficient, accessible channels for sharing real-time data and information with the public—e.g. information about evacuations, shelters, and so on—as can the dissemination of more general guidance materials (Santos-Reyes and Beard 2011). A good example of the latter is how effectively ICT means have been used to communicate essential security information to the public during Russia's full-scale invasion of Ukraine (Zarembo et al. 2024).

¹ It is worth noting that, understood this way, societal resilience is a wider concept than civic resilience, which focuses more specifically on the crisis resilience of civil infrastructure and civil dimensions of the state—i.e., processes and functions such as healthcare that formally support state functioning in times of crisis, including during the time of war (NATO 2024).

² The author acknowledges that different countries across the world develop and adopt distinct satellite and cell broadcast means for up-to-date information sharing and public warning. Due to these services using distinct infrastructure, demanding different type of commitments, and being primarily used as a means of crisis management, this chapter will not consider the implementation and public adoption concerns that might emerge with these technologies. For a fuller discussion of these aspects, see Goniewicz and Burkle (2019).

³ Indeed, whilst the device settings might differ, as does who has access to the messages, services that use mobile broadband and/or location to send push notifications do not demand prior installation of an app or signing up to a service from the users.

Risk management encompasses any activity that entails planning for and mitigating different (crisis) scenarios that might occur in the future. The aim of risk management is, therefore, to enhance societal preparedness for possible crises by being sufficiently prepared to respond to *unforeseen* events. One aspect of this (and where risk management and crisis management overlap) is building the capacity to keep any relevant services or processes operating as smoothly as possible, even during the event. Just as important, however, is ensuring that the public are properly informed and educated. Similarly to crisis management, ICT tools as information channels have become common, with custom-made or customised apps, web pages, and public profiles for the relevant institutions on popular social media platforms all widely used for this purpose. Examples include rescue services using Meta or X profiles and the designated “Kyiv Digital”⁴ or “Ole valmis!”⁵ introduced by Ukraine and Estonia, respectively. Despite the broad range of means that have been introduced in the EU, however, analysis has also shown that the systems currently in place still require improvement as well as more frequent testing (Niinistö 2024).

The following discussion is concerned principally with risk management. It focuses on some of the simpler ICT tools that can be incorporated into risk management procedures as a means to disseminate public information about measures that can be taken to increase societal resilience, including crisis preparation means, and for enhancing public awareness of possible threats, early warning systems and alert procedures. These kinds of tools are especially suitable for public risk management because of their ease of use and accessibility. Despite these strengths, however, it cannot be assumed that there will be broad public adoption of any such tools introduced and, crucially, it must be considered whether increasing dependence on such means can actually contribute to undermining public awareness and preparedness-raising efforts.

The aim of this chapter is to draw out and help understand the opportunities and potential negative effects of adoption. To do so, it draws on recent research to provide a theoretical overview of the general concerns that come with implementing digital tools and (online) means in risk management—especially those used as public information channels regarding crisis preparation—and situates the issue of uptake within this.⁶

The general takeaway of the discussion is that overreliance on ICT tools and online applications in risk management can lead to serious security concerns at the levels of societal resilience, safety and individual well-being. Mitigating these concerns thus demands critical assessment and understanding of when and in what form ICT means are suitable

⁴ “Kyiv Digital” is a multifunctional Ukrainian application for residents of and visitors to the capital that was launched in 2021 and has been customised following the outbreak of the war to provide, for example, information about air alerts.

⁵ “Ole valmis!” (Be Prepared!) is an Estonian mobile app that provides instructions for preparing for different (crisis) situations, e.g., in the event of a power outage, natural disaster, or the disruption of vital services.

⁶ It is worth noting that these concerns also apply to the use of similar technologies in crisis management. For example, the use of mobile applications (with push notifications) or sharing relevant information on official social media accounts.

for risk management and raising resilience through crisis preparedness, as well as identification of any associated risks—both in general and with specific means. The more specific takeaway is that—though ICT means are generally seen as efficient and suitable for societal crisis preparedness on a large scale—it is crucial that there is sufficient public adoption of any means introduced, as well as that it is possible for all of the population to use them. If either of these goals is not secured, the utility of any means introduced will be greatly reduced, and so dependence on them can prevent both individuals and society from being sufficiently prepared for crises. Crucially, though, efforts to meet both goals can be hindered in a number of ways. Direct attacks on infrastructure are, of course, a major source of risk. Yet, there are other concerns that can also play a role and which have received less attention. A number of these will be discussed in this chapter.

The issues discussed in this chapter emerge from the broader phenomenon of digitalisation and the increasing dependence on ICT at a global level. Given that scope, the discussion is not focussed on any specific state. Before moving on, then, it is important to recognise that the precise nature of the concerns faced by specific states will always differ, depending upon factors such as the socio-cultural acceptance of technology, economic welfare, and so on.

The discussion is divided into three sections: Sect. 4.2 explains the context, motivation and scope of the chapter's topic; Sect. 4.3 discusses the two dimensions of risk—users and services/products; Concluding Sect. 4.4 suggests some methods for mitigating the risks described in Sect. 4.3.

4.2 Context, Motivation, and Scope

4.2.1 The Digitally Enhanced State and Society

The rapid development and adoption of digital tools, i.e. digitalisation, at all levels of society has led to a situation where the majority of formal as well as informal societal functions and processes are, in one form or another, supported by digital tools. Although the precise level of adoption is contingent on various factors such as societal openness to new technology, the accessibility to territory and what can be afforded, the phenomenon is experiencing accelerated growth, catalysed by the COVID-19 pandemic (Grinin et al. 2022) and commercial generative AI solutions (Kelley et al. 2021; Roberts and Cand 2024).

As digital technologies have come to enhance both the everyday lives of individuals *and* state functioning, it is important to recognise that it is both modern society *and* the modern state that are becoming digitally enhanced as a result. This encompasses governance, both public and private sectors, and many societal interactions. One aspect of this is how digitalisation can enhance and facilitate the interactions between a state and its residents. For instance, digitalisation can make bureaucratic processes easier to access,

e.g. online tax declarations or applications for benefits; it also provides new means with which the state can inform and monitor its residents more effectively, e.g. COVID-19 tracing apps. Such enhancements can, in turn, potentially increase the state's capacity to fulfil the expectation/responsibility of ensuring—and even enhancing—the well-being of the individual.

The other side of this process of digital enhancement, however, is digital dependence. Gregersen et al. define this at the individual level as “a non-voluntary dependence on digital devices and platforms for social interactions across all spheres of social life” (Gregersen et al. 2023, p. 973). Following this, digital dependence at the *state level* might be described as a necessary dependence on digital devices and platforms across all spheres of *state functioning* and all spheres of *societal functioning*. Increasing digital dependence across these two spheres, however, generates two broad areas of risk: possible threats to the underlying ICT infrastructure and possible threats associated with the adoption and use (or uptake) of digital technologies.

The threats to services and infrastructure, and how they can undermine societal functioning, have been widely discussed. ICT infrastructure consists of both physical objects and virtual services (Sachs 2004; Thedéen 2006). These are vulnerable to damage caused by accidents, extreme weather conditions, human error, incompatibility between technologies and various other factors. Importantly, the increase in societal dependence on digital solutions has also made ICT infrastructure a target for intentional and purposeful efforts to compromise the systems' functioning. This has, for one, attracted malicious activities aimed at financial or ideological gain, e.g. sabotage and cyberattacks. At the same time, the means for exploiting the risks inherent in digital dependence have also become part of the *hybrid warfare* toolkit that can be used to systematically undermine the functioning of the state itself. Within the context of current geopolitical tensions, Russian and Chinese efforts to exploit the EU's digital dependence offer a good example of this. As in other domains, direct attacks on infrastructure can be employed to undermine any systems in place as a part of risk management programmes and, consequently, weaken societal resilience by way of societal crisis preparedness—or even to create a crisis situation directly.

Though the infrastructural risks have received much discussion, there is another, less discussed aspect to digital dependence that also raises significant concerns with respect to risk management—technological *path dependency* (Puffert 2004). The concept of path dependency is grounded in the economic constraint that, when carrying out any policy or plan involving technology, a specific technological path must be chosen, and once chosen, the continuity of that technology must be ensured. In the context of the digitally enhanced state or society, path dependence is grounded in the ways that ICT tools and services are deeply embedded into the functioning of both the state and society and, consequently, the ways in which both state and society become dependent on the continuing provision and updating of such services. That is to say that once the methods of providing services are chosen, keeping those services operating becomes an imperative for the state. Insofar

as this happens under the conditions of limited resources, the possibility of developing alternative solutions therefore becomes severely restricted. This dependence on one path chosen raises two core concerns. First, the sustainability of the path depends on the availability of the tools and services needed to ensure continuity. Second, once a path has been chosen, it is necessary that *that* path is accepted and adopted by all relevant parts of society, which then requires that the necessary ICT resources for providing the given services are available to all relevant parts of society. Thus, any gap in the resources necessary for sustainable service provision or a shortfall in acceptance of the chosen path can undermine whatever services the state provides. It may also engender ill-feeling and distrust towards the particular parties that instigated the installation of the ICT tools and services in question.

4.2.2 Risk Management, Societal Resilience and the Importance of Path Acceptance

Risk management can be undertaken in smaller- or larger-scale units. Societal resilience, in this regard, is the largest unit to which risk management practices are applied.

The importance of societal resilience is twofold. On the one hand, society, more so than any specific organisation, institution or specific group of people, is a complex system, entailing many greatly differing processes. To enhance the resilience of a society as a whole, therefore, it is necessary to recognise that all society members—as a part of one of these different processes—need to recognise their contribution to the overall resilience of the society and act accordingly. On the other hand, society consists of distinct individuals who differ in age, gender, beliefs, skills, experiences and many other categories, and every one of them is a contributor to the well-functioning of the society. Since this last consideration includes societal resilience, therefore, the societal resilience of individuals is of central importance to societal resilience at the largest unit of scale. And since every individual fits in many categories, the full range of those categories must be accommodated to ensure their resilience.

It is because of the importance of individual resilience, then, that public technological path acceptance—and especially the adoption of relevant technologies among the relevant parts of the population—is central to risk management in the digitally enhanced state. For, to the extent risk management becomes dependent on ICT tools—especially for risk management communication—individual resilience will also become dependent on those tools. Thus, if those tools are not adopted, societal resilience will be compromised.

Having given a general overview of the importance of technological path acceptance and adoption to risk management with respect to societal resilience—and why this should be a concern—the next section will look at two more specific areas of concern when it comes to the use of ICT solutions: concerns relating to the users and concerns relating to the service providers.

4.3 Concerns with Dependence on ICT Tools and Means

4.3.1 Users and Adoption-Related Concerns

The key point in the following discussion is that individual engagement with any means of risk mediation is mostly a matter of voluntary choice. There are some exceptions—for instance, early warning and crisis management tools can include location- and mobile network-based push notification systems. And as these systems have become crucial components of ensuring individual well-being in crises situations, the relevant tools are often “enforced” upon the population by the state. Still, these are exceptions, and voluntary initiatives remain the rule. Reflecting that, many state and relevant institutions have made significant efforts to develop online tools that can help residents better understand and recognise the kinds of threats that can lead to a crisis. Threat education often also includes providing instructions on how individuals (and small social units such as families) can prepare for crisis situations so as to be self-sufficient during the crisis as much as possible. Whatever effort is put into providing these resources, however, it is still necessary for individuals to adopt and use them. This extends to any technologies necessary for that. Yet, while this requirement hardly goes unrecognised, it seems to be widely assumed that, in a digitally enhanced state, it will be met as a matter of course—as, for example, with the, in retrospect, grossly inflated expectations concerning the adoption rate of COVID-19 mobile applications in the US (Li et al. 2021) as well as in the UK and mainland Europe (Sujarwoto and Maharani 2023) at the height of the pandemic. Technology acceptance research, however, has long emphasised that perceived usefulness as well as perceived ease of use are crucial for any technology adoption, alongside contextual social factors and individual attitude (Davis 1989) (For contemporary discussion on technology use for democracy, see Ceccarini et al. (2023)).

4.3.2 The Four Phenomena Hindering ICT Adoption

The assumption of adoption, then, is challenged further by research into ICT use that has identified four phenomena of modern digitalised processes that could plausibly hinder the adoption of novel technological means to building societal resilience—no matter how digitally enhanced the state is.

Firstly, the move by many risk management-related institutions to use custom apps, websites and social media websites as public information sources marks a departure from more traditional hierarchical approaches to risk communication. This allows for information dissemination to be decentralised, including enabling users to contribute to the information field (Kar 2016). There are clear benefits to this approach, yet opening contributions up in this way also gives rise to several areas of concern. One problem is that the information users provide may not come from verified sources and, correspondingly,

may include misinformation (Aven and Thekdi 2022; Mayorga et al. 2020; Pennycook and Rand 2021). Insofar as individuals might believe this misinformation, as Newman et al. (2022) point out, they may become vulnerable to harms that, if they engaged with a more hierarchical system, they would be more aware of. Another related problem is that any social media platforms and apps that are publicly open might also attract malicious actors interested in identifying and exploiting the particular vulnerabilities of any target community or society (Zarembo et al. 2024). Allowing user contributions may raise the possibility that the information that would help such actors achieve those goals would be shared and accessible to those actors.

A growing awareness of these problems with the mixed quality and veracity of information that can be encountered online may help with these issues. Yet it remains often difficult for individuals to distinguish between good information and misinformation or to separate the genuine contributor or source from the fraudulent one. Correspondingly, there are and remain many people who prefer not to engage with the relevant communication platforms and apps for the sake of safety—even as, and indeed because, they have become more informed about the risks.

Secondly, as well as trust in the information provider, the success of awareness-raising programmes, as well as the likelihood that people will follow the guidance provided, also depends on individuals *trusting* the state directly when it comes to doing its part in ensuring their individual well-being. As Wong and Jensen explain:

If the public trusts the authorities to fulfil their duty of care, the persuasiveness of risk information will be higher, the public will be more accepting of risks and uncertainties, and discursive conflicts will be significantly reduced (Wong and Jensen 2020, p. 1).

However, as the introduction of COVID-19 safety measures demonstrated, gaining trust involves striking a fine balance, where individuals need to recognise the validity and relevance of the measures implemented while being confident that the state will not use them in inappropriate ways and will lift them when they are no longer relevant. The positive side of this equation was evidenced by a study by Fischer et al., which found that “if people perceive that they will receive relevant, accurate, and timely warnings, they are more likely to use a warning app and comply with the information received” (Fischer et al. 2019, p. 642). The failure to achieve sufficiently widespread adoption of contact tracing apps introduced during COVID-19 illustrates the other side, with individual concerns about data security, and trust in the state to satisfy these concerns, considered to be significant causes of that failure (White and van Basshuysen 2021). Cultivating trust thus depends upon making the right judgements about any measures introduced. Over-implementation and over-use might hinder future uptake because the citizens deemed the measures introduced before to be irrelevant or intrusive (Sorell 2023). Under-implementation may lead them to lose confidence in the state’s capacity to fulfil its duty of care.

Thirdly, given how significant a part of many people's daily lives technology has become, the suggestion that one needs to engage with another digital venue—even for the sake of enhancing one's own preparedness for crisis—might have a reverse effect. For instance, the conditions of so-called technostress (from work or study environments) can also spill over to other fields of life, e.g. personal well-being (Batta and Kar 2023; Chen and Muthitacharoen 2016), while cognitive overload from too many information streams can lead to a decreased capacity to process information (Arnold et al. 2023; Yu et al. 2023). In either case, this may result in a lack of enthusiasm or interest in engaging with any technology-based risk-management resources provided by the state.

The fourth concern is the most pressing and likely to be the largest contributor to any discrepancy between the digital path taken and society's uptake of the relevant technologies: the digital divide. As noted before, the adoption and use of online means in digitally enhanced states is something that is often taken for granted, and the future vision is usually that this will increase. However, there are in any society people who either cannot use or access the relevant digital technologies—due to a lack of skills, access to the technology, access to an Internet connection, and so on—or do not want to—for ideological reasons, for example. Because this digital divide is unlikely to disappear, therefore, the more communication with the state, as well as awareness raising, is funnelled through digital and online channels, the more essential information those society members on the wrong side of that divide will miss. By streamlining the communication channels in such a way then, some people will be in a vulnerable position from the get-go. If that threat is neglected and the equal importance of those groups' preparedness is overlooked, instead of increasing societal resilience, it may be that further security threats are introduced.

A further dimension of societal resilience in digitally enhanced states is digital resilience—that is the resilience of the digital services, tools and devices that the state and society have come to depend upon (Wright 2016). The next section discusses various challenges states can face with regard to this as an aspect of societal resilience.

4.3.3 Technology Use and Accessibility-Related Concerns

States differ in the resources—physical as well as economic—they have available to build an ICT infrastructure that could support any digital tools that might help enhance social resilience and preparedness for crisis. One consequence of this is that states may have to rely on private companies (including global ones) and solutions (Breagh et al. n.d.) to provide relevant services. Moreover, it can be assumed that the smaller the state and scarcer the resources, the more they must rely on private entities for the development and maintenance of ICT resources. In regard to this concern, Europe is upping efforts to gain technological sovereignty (Bauer and Erixon 2020) in response to its recognised high level of dependence on foreign technological input (Edler 2024). Another reason states might be attracted to solutions provided by private companies is if those services

have already become established as popular among the groups relevant to the state's risk management approach (e.g. as with official use of Twitter (Panagiotopoulos et al. 2016), Facebook (Lwin et al. 2018), Weibo and WeChat (Feng and Umaier 2023), and TikTok (Zhang et al. 2024). However, attempts to streamline risk management by adopting private, global services (including popular ones) can raise problems with regard to continuity, accessibility, and the actual utility of the tools they provide.

As far as continuity goes, a dependence on either custom-developed or customised application-based solutions may become problematic down the line due to the inevitable need for operating systems and applications to be updated. Updates are necessary to ensure that both operating systems and applications remain secure and, relatedly, to ensure user safety and privacy. However, every new update also brings changes to how operating systems and applications interoperate and how they do so securely. When it is the operating system that is updated, it is very often the case that the relevant applications must also be updated if they are not to become incompatible and, due to that, unusable or dysfunctional. Whenever a state provides any services via custom/customised applications, therefore, the digital resilience of the state becomes dependent on the developers' long-term commitment to ensuring continuing compatibility with the latest operating system updates.

Similar concerns arise from the longer-term direction of technological progress as it applies to both operating systems and the underlying technologies that support any such systems. Every generation of an operating system will at some point be gradually phased out (including, eventually, the cessation of security updates) and replaced with a newer one. If an application used in a state's risk management approach is only compatible with a specific operating system or specific technologies any utility it might offer will at some point disappear. Having noted this concern, however, it is worth emphasising that it is less often the case that applications are tied to specific generations of operating system or technology to this extent than some other solutions are tied to underlying technologies. Hence the principal concern with regard to continuity remains the support needed to maintain up-to-date compatibility.

When it comes to accessibility, depending on external private companies and the services they provide to enhance or maintain societal resilience is also a gamble. The social media platform X (previously known as twitter.com) offers a telling example of this and how access issues can emerge suddenly and in a way that is entirely out of the state's hands. Twitter had long been a popular social media platform among public institutions and socially relevant movements as a key part of their online presence. During the COVID-19 pandemic, it was not uncommon for public institutions to use their Twitter profiles for risk and crisis management purposes as public information channels. At this time, the platform was not only widely adopted but entirely free of charge to users and, crucially, accessible to people who did not have user accounts. Following Twitter's change of ownership in 2023 and its rebranding as X.com, however, this changed, with some features of the platform being made paid only and, most significantly, full access to

profiles now requiring a user account. These changes in accessibility therefore compromised the approach of institutions who were using the platform to share information with the public, or of users who had adopted it as an information source.

A related problem with using other organisations' platforms as public information channels means that the information provider is subject to the rules imposed by those organisations on how the platform is used. In particular, the organisations that provide the platforms are the ultimate gatekeepers when it comes to what information is shared on those platforms and—though subject to local regulations—they have the power to decide who or what can post on the platforms. These decisions can be influenced by the platform owners' views, local political interests, and actors and so on. Due to the subjective nature of this control mechanism, therefore, the rules and access conditions that institutions must operate within can easily change in a way that states cannot directly manage. This problem is exacerbated when the platforms used are global as well as provided by global private companies and so may be influenced by actors and concerns otherwise entirely disconnected from the local population who are the intended recipients of the risk management information. Due to that, institutions that are responsible for providing public safety-related information may lose the ability to post to the platforms they use as information channels even though their function is a politically neutral one. Indeed, this possibility has arguably become a reality in 2025 under the new administration in the USA (where the major platform operators are based), as represented, for instance, by the wide application of newly introduced prohibitions against diversity, equity, and inequality (DEI) programmes (The White House 2025). In January 2025, for example, The Centers for Disease Control and Prevention (CDC) were required to withdraw publications containing any of a list of terms associated with DEI movements (gender, LGBT, biologically female), as well as temporarily taking down critical safety information associated with that work previously available online (Incorvaia 2025).

4.4 Mitigating Concerns

While novel ICT means might be relatively easy to develop and ICT solutions might offer relatively easy means with which to enhance societal resilience and crisis preparedness, the factors that might affect path acceptance and adoption need to be assessed alongside the uses and opportunities they offer. And indeed, there is evidence that in different countries societal attitudes vary when it comes to technologically enhancing state services, in general and with respect to societal security (Kaun et al. 2024). A survey conducted by Kaufhold et al. (2020) between 2017 and 2019 in Germany, which by then had already developed several crisis information applications, found that while people with experiences of apps did consider these to be useful tools, radio, TV and communication with other people as well as directly approaching rescue services remained more popular as information sources.

Furthermore, the positive attitudes towards the relevant apps and actual usage showed discrepancies—i.e. the support for state-provided apps was higher than the actual usage of those already introduced (Kaufhold et al. 2020). This attitude—a technological positivism that is not correlated with the acceptance and adoption of the available technologies—is also well illustrated by the fate of several contact tracing apps developed during the COVID-19 pandemic. For example, despite initial optimism, Estonia’s HOIA app failed to reach the necessary population-wide adoption level for it to serve its purpose (Allik 2021). Of course, a state-mandated approach, even if in breach of individual rights, may have had a larger impact without needing to establish trust in the state’s use of technology. Indeed, this was just the case with South Korea’s successful introduction of similar track-and-trace applications during the pandemic. Such an approach, however, can only ever be a short-term crisis solution (in democratic states at least) if it is not to damage societal trust in the state, which, as discussed before, is a necessary component of any measures introduced to maintain societal resilience (Sorell 2023).

While adoption is a necessary consideration for any ICT means aimed at enhancing societal resilience, it is just as necessary that those measures be developed according to the needs of the communities that they are intended for. Baibarac and Petrescu (2019) suggest that any proposed means aimed at enhancing *urban* resilience collectively via information sharing and support must be developed via co-design processes.

In this regard, the community’s contribution plays an important role in determining whether a resilience tool is effective on multiple levels, most importantly:

- (i) Communities need to be involved to identify how the tool can work for their good, and
- (ii) Key members of that community need to be adopters and supporters of the tool for it to garner a wide userbase.

As noted earlier, among the concerns about adoption are those stemming from just how much digital technologies and information flow are embedded in daily lives. Firstly, there is a concern that there is a technological saturation point, beyond which individuals may feel overwhelmed and be resistant to engage with yet another information channel. Secondly, the saturation of technology might be accompanied by a glut of information, whereby people consider themselves to have no need for further tools, as they feel they are already sufficiently informed with respect to their safety. To mitigate both of these risks, the current technological and informational situation of the potential audience should be critically analysed prior to introducing any new channels of information. And an important aspect to this is that the state must get its messaging right—with respect to both specific means and, more importantly, its general programme of technological development. Even if they are all aimed at simplifying the user’s engagement with the state and minimising the need for individual users’ interactions, for example, introducing too many ICT solutions without communicating their benefits is likely to hinder their adoption.

For example, Estonia's Digital Agenda 2030 promises to simplify and reduce individual users' need to interact with the state (Ministry of Economic Affairs and Communications 2021). However, so many ICT solutions have been introduced without doing the work to ensure potential users understand how they are all linked that there is a risk of the message getting lost, which may, in turn, lead to a decline in interest—especially in those tools that do not suit users' immediate and everyday needs. The European Digital Identity Regulation, for example, is harmonising national electronic identification schemes by requiring every member state to introduce by 2026 a digital ID wallet to be issued either by public authorities or recognised private entities (Regulation 2024/1183). While national digital ID systems have been recognised in the EU for a decade already, they have, so far, become an essential part of life online in only a few countries (e.g. Estonia and Denmark) (Henley and Krupa 2025). As discussed earlier, voluntary adoption requires the public to trust the state, therefore it is necessary for state institutions to make sure individuals recognise the relevance of those tools to their own lives and negotiate between communicating trustworthiness, timeliness, and not seeming overbearing. Particularly with the capacity of digital technologies to be used to impose social control and large-scale surveillance, this also involves finding the correct balance between the state ensuring security and oppressing members of society—and again communicating that to the potential users (Bell 2006; Asgarinia 2023). In the EU, the collection and processing of application and website users' data, for example, is regulated by the General Data Protection Regulation (GDPR); however, there is a notable lack of communications explaining those regulations, the reasons for their introduction, and what compliance with them would require. The importance of messaging, then, requires continuous explanation via public awareness campaigns. Continuing to provide alternative, non-digital messaging and communicate their availability may also help support such campaigns by mitigating fears of imposed social control.

Finally, similarly to resilience building in any specific company or process, when developing tools to bolster societal resilience, it is important to recognise that no tool should be too situation-specific if it is to be effective in the middle of an ongoing crisis—as any such situation will be unique, comprising a complex set of interacting factors (Aven 2016; Langeland et al. 2016); therefore, tools deployed should be broadly applicable to a range of situations. While in the EU public warning capabilities have been improved considerably by the requirement under the European Electronic Communications Code to implement a mobile-based warning system, the rapidly changing climate and security situation also demands robust plans and processes regarding how and when they are to be used.

4.5 Conclusion

Recognition of the growing number of threats to both the well-functioning of the state and its individual residents' well-being has led many countries to identify and develop novel means for societal resilience building as central components of any risk management programmes. In keeping with more general trends towards technologically and digitally enhanced states, digital and ICT solutions are widely seen as a suitable development path. Where the goal is to boost resilience through increasing crisis preparedness, however, any means introduced must reach as wide an audience as possible to be effective. Yet, as discussed in this chapter, even if the introduced tools are sufficiently accessible and suitable in other ways, if they are to fulfil their purpose, and indeed, not undercut societal resilience, they must still be adopted for use across the relevant social groups.

References

- Allik H-L (2021) Series of flops or how HOIA failed, Postimees. Available at: <https://news.postimees.ee/7185647/series-of-flops-or-how-hoia-failed>. Accessed 31 Mar 2025
- Arnold M, Goldschmitt M, Rigotti T (2023) Dealing with information overload: a comprehensive review. *Front Psychol* 14:1122200. <https://doi.org/10.3389/fpsyg.2023.1122200>
- Asgarinia H (2023) Big data as tracking technology and problems of the group and its members. In: Macnish K, Henschke A (eds) *The ethics of surveillance in times of emergency*. Oxford University Press, Oxford, pp 60–75
- Aven T (2016) Risk assessment and risk management: review of recent advances on their foundation. *Eur J Oper Res* 253(1):1–13. <https://doi.org/10.1016/j.ejor.2015.12.023>
- Aven T, Thekdi SA (2022) On how to characterize and confront misinformation in a risk context. *J Risk Res* 25(11–12):1272–1287. <https://doi.org/10.1080/13669877.2022.2142950>
- Baibarac C, Petrescu D (2019) Co-design and urban resilience: visioning tools for commoning resilience practices. *CoDesign* 15(2):91–109. <https://doi.org/10.1080/15710882.2017.1399145>
- Batta A, Kar AK (2023) How does technostress during a pandemic affect employee attrition in IT/ITeS industries? Insights from India. *First Monday* 28(2). <https://doi.org/10.5210/fm.v28i2.11412>
- Bauer M, Erixon F (2020) Europe's quest for technology sovereignty: opportunities and pitfalls. ECIPE Occasional Paper, No. 02/2020, European Centre for International Political Economy (ECIPE). Brussels. <https://hdl.handle.net/10419/251089>. Accessed 25 Oct 2025
- Bell C (2006) Surveillance strategies and populations at risk: biopolitical governance in Canada's national security policy. *Secur Dialogue* 37(2):147–165. <https://doi.org/10.1177/09670106060606168>
- Breaugh J, Hammerschmid G, Rackwitz M et al (n.d.) What does private sector involvement in government digitalisation mean for public values? CIVIVA. Retrieved 24 Oct 2025, from <https://www.civica.eu/news-events/news-blog/detail/what-does-private-sector-involvement-in-government-digitalisation-mean-for-public-values>
- Chen L, Muthitacharoen A (2016) An empirical investigation of the consequences of technostress: evidence from China. *Inf Resour Manage J* 29(2):14–36. <https://doi.org/10.4018/IRMJ.2016040102>

- Ceccarini L, Newell LJ, Turato F (2023) Civil society and the platform society in the age of post-representative politics. *Studia Politologiczne* 70(2):33–51. <https://doi.org/10.33896/SPolit.2023.70.2>
- Davis FD (1989) Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Q* 13(3):319–340. <https://doi.org/10.2307/249008>
- Directive 2018/1972. Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L1972>
- Edler J (2024) Technology sovereignty of the EU: needs, concepts, pitfalls and ways forward. Fraunhofer Institute for Systems and Innovation Research ISI, Karlsruhe & Manchester Institute of Innovation Research, University of Manchester. Belgium. <https://coilink.org/20.500.12592/hzjqm40>
- EENA (n.d.) Public warning, the European emergency number association. Retrieved 24 Oct 2025, from <https://eena.org/our-work/eena-special-focus/public-warning/>
- European Commission (2025) Joint communication to the European Parliament, the European Council, the Council, the European economic and social committee and the committee of the regions on the European preparedness union strategy JOIN/2025/130 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025JC0130>
- Feng C, Umaier K (2023) Risk communication during the COVID-19 pandemic in the era of social media. *J Disaster Res* 18(1):34–39. <https://doi.org/10.20965/jdr.2023.p0034>
- Fischer D, Putzke-Hattori J, Fischbach K (2019) Crisis warning apps: investigating the factors influencing usage and compliance with recommendations for action. In: Proceedings of the 52nd Hawaii international conference on system sciences, pp 639–648. <https://doi.org/10.24251/HICSS.2019.079>
- Goniewicz K, Burkle FM (2019) Disaster early warning systems: the potential role and limitations of emerging text and data messaging mitigation capabilities. *Disaster Med Public Health Prep* 13(4):709–712. <https://doi.org/10.1017/dmp.2018.171>
- Gregersen EM, Astrupgaard SL, Jespersen MH, Gårdhus TP, Albris K (2023) Digital dependence: online fatigue and coping strategies during the COVID-19 lockdown. *Media Cult Soc* 45(5):967–984. <https://doi.org/10.1177/01634437231154781>
- Grinin L, Grinin A, Korotayev A (2022) COVID-19 pandemic as a trigger for the acceleration of the cybernetic revolution, transition from e-government to e-state, and change in social relations. *Technol Forecast Soc Change* 175:121348. <https://doi.org/10.1016/j.techfore.2021.121348>
- Henley J, Krupa J (2025) ‘Starmer’s ID plan has caused upset, but in the EU the debate has long been settled’, *The Guardian*, 26 September. Available at: <https://www.theguardian.com/world/2025/sep/26/starmer-id-card-plan-has-caused-upset-but-in-the-eu-the-debate-has-long-been-settled>. Accessed 24 Oct 2025
- Incorvaia D (2025) ‘UPDATED: CDC withdraws new scientific publications to scrub specific words: reports’, *Fierce Biotech*, 4 February. Available at: <https://www.fiercebiotech.com/research/cdc-halts-scientific-publications-scrub-forbidden-words-report>. Accessed 27 Oct 2025
- Kar B (2016) Citizen science in risk communication in the era of ICT. *Concurr Comput Pract Exp* 28:2005–2013. <https://doi.org/10.1002/cpe.3705>
- Kaufhold M, Haunschild J, Reuter C (2020) Warning the public: a survey on attitudes, expectations and use of mobile crisis apps in Germany. In: European Conference on Information Systems (ECIS). https://aisel.aisnet.org/ecis2020_rp/84
- Kaun A, Larsson AO, Masso A (2024) Automation scenarios: citizen attitudes towards automated decision-making in the public sector. *Inf Commun Soc* 28(7):1–18. <https://doi.org/10.1080/1369118X.2024.2375261>

- Kelley PG, Yang Y, Heldreth C et al (2021) Exciting, useful, worrying, futuristic: public perception of artificial intelligence in 8 countries. In: *Proceedings of the 2021 AAAI/ACM conference on AI, ethics, and society*, pp 627–637. <https://doi.org/10.1145/3461702.3462605>
- Langeland KS, Manheim D, McLeod G et al (2016) How civil institutions build resilience: organizational practices derived from academic literature and case studies. RAND Corporation: Research Report. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1200/RR1246/RAND_RR1246.pdf
- Li T, Cobb C, Yang J et al (2021) What makes people install a COVID-19 contact-tracing app? Understanding the influence of app design and individual difference on contact-tracing app adoption intention. *Pervasive Mob Comput* 75:101439. <https://doi.org/10.1016/j.pmcj.2021.101439>
- Lwin MO, Lu J, Sheldenkar A et al (2018) Strategic uses of Facebook in Zika outbreak communication: implications for the crisis and emergency risk communication model. *Int J Environ Res Public Health* 15(9):1974. <https://doi.org/10.3390/ijerph15091974>
- Mayorga MW, Hester EB, Helsel E et al (2020) Enhancing public resistance to “Fake News”. In: O’Hair HD, O’Hair MJ (eds) *The handbook of applied communication research*. Wiley, Hoboken, pp 197–212
- Ministry of Economic Affairs and Communications (2021) Digital agenda 2030. <https://mkm.ee/en/e-state-and-connectivity/digital-agenda-2030>. Accessed 31 Mar 2025
- NATO (2024) Resilience, civil preparedness and Article 3. https://www.nato.int/cps/en/natohq/topics_132722.htm. Accessed 31 Mar 2025
- Newman EJ, Swire-Thompson B, Ecker UKH (2022) Misinformation and the sins of memory: false-belief formation and limits on belief revision. *J Appl Res Mem Cogn* 11(4):471–477. <https://doi.org/10.1037/mac0000090>
- Niinistö S (2024) Safer together—strengthening Europe’s civilian and military preparedness and readiness. European Commission Report. https://commission.europa.eu/document/5bb2881f-9e29-42f2-8b77-8739b19d047c_en
- Panagiotopoulos P, Barnett J, Bigdeli AZ et al (2016) Social media in emergency management: Twitter as a tool for communicating risks to the public. *Technol Forecast Soc Change* 111:86–96. <https://doi.org/10.1016/j.techfore.2016.06.010>
- Pennycook G, Rand DG (2021) The psychology of fake news. *Trends Cogn Sci* 25(5):388–402. <https://doi.org/10.1016/j.tics.2021.02.007>
- Puffert DJ (2004) Path Dependence, Network Form, And Technological Change. In: Guinnane T, Sundstrom W, Whatley W (eds) *History matters: essays on economic growth, technology, and demographic change*. Stanford University Press, Stanford, pp 63–95
- Regulation 2024/1183. Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32024R1183>
- Roberts DL, Cand M (2024) Artificial intelligence and innovation management: charting the evolving landscape. *Technovation* 136:103081. <https://doi.org/10.1016/j.technovation.2024.103081>
- Sachs MH (2004) The Cyber adversary in groups: targeting nations’ critical infrastructures. In: Parker T, Devost MG, Sachs MH, Shaw E, Stroz E (eds) *Cyber adversary characterization*. Syngress, Oxford, pp 205–230
- Santos-Reyes J, Beard AN (2011) Information communication technology and a systemic disaster management system model. *Int J Distrib Syst Technol* 2(1):29–42. <https://doi.org/10.4018/jdst.2011010103>
- Sorell T (2023) Pandemic population surveillance: privacy and life-saving. In: Macnish K, Henschke A (eds) *The ethics of surveillance in times of emergency*. Oxford University Press, Oxford, pp 15–29

- Sujarwoto S, Maharani A (2023) Facilitators and barriers to the adoption of mHealth apps for COVID-19 contact tracing: a systematic review of the literature. *Front Public Health* 11:1222600. <https://doi.org/10.3389/fpubh.2023.1222600>
- The White House (2025) Ending radical and wasteful government DEI programs and preferencing. The White House. Retrieved 27 Oct 2025, from <https://www.whitehouse.gov/presidential-actions/2025/01/ending-radical-and-wasteful-government-dei-programs-and-preferencing/>
- Thedéen T (2006) Setting the stage: the vulnerability of critical infrastructures. In: Frolov KV, Baecher GB (eds) *Protection of civilian infrastructure from acts of terrorism*. Springer, Dordrecht, pp 33–40
- White L, van Basshuysen P (2021) Without a trace: why did corona apps fail? *J Med Ethics* 47:e83. <https://doi.org/10.1136/medethics-2020-107061>
- Wong CML, Jensen O (2020) The paradox of trust: perceived risk and public compliance during the COVID-19 pandemic in Singapore. *J Risk Res* 23(7–8):1021–1030. <https://doi.org/10.1080/13669877.2020.1756386>
- Wright DJ (2016) Toward a digitalresilience. *Elementa: Sci Anthropocene* 4:000082. <https://doi.org/10.12952/journal.elementa.000082>
- Yu L, Chen Y, Gong M (2023) The duality of ICT-mediated overload: its nature and consequences. *Inf Manage J* 60(8):103864. <https://doi.org/10.1016/j.im.2023.103864>
- Zarembo K, Knodt M, Kachel J (2024) Smartphone resilience: ICT in Ukrainian civic response to the Russian full-scale invasion. *Media War Confl* 18(3):305–324. <https://doi.org/10.1177/17506352241236449>
- Zhang W, Yuan H, Zhu C et al (2024) Factors influencing public engagement in government TikTok during the COVID-19 crisis. *Elect Lib* 42(2):210–229. <https://doi.org/10.1108/EL-06-2023-0150>

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.





The Potential Connections Between Civil Defence and the Cultural Sector

5

Aule-Merlin Vihlver

Abstract

The concepts of Risk Society, Multidimensional Crises, and Polycrises have become increasingly embedded in contemporary discourse, reflecting a world where individuals, businesses and states face both local and global risks. These evolving threats pose complex challenges for crisis preparedness and response. This chapter examines the principles of civil defence in Estonia. It outlines the institutional framework for safeguarding the population during crises and examines potential ways to integrate the cultural sector into civil defence efforts, primarily through community houses as resilience centres. Drawing on expert interviews and survey data collected through an empirical study, the chapter highlights key opportunities and challenges in fostering collaboration between the civil defence and cultural sectors (The author has utilised AI tools in the preparation of this chapter but assumes full responsibility for its content.).

Keywords

Civil defence • Resilience centres • Community houses • Cultural workers • Local government

A.-M. Vihlver (✉)
Estonian Academy of Security Sciences, Tallinn, Estonia

5.1 Introduction

Civil defence encompasses efforts to prepare a nation's population for crises and a set of actions to safeguard people when a crisis occurs. The goal of civil defence is to ensure the protection of people in any crisis. It involves a range of measures undertaken by governments, local authorities, organizations, communities, and individuals. Typically, national civil defence organizations serve as lead agencies responsible for coordinating other entities involved in civil protection efforts. The duties of civil protection agencies include the effective implementation of strategies aimed at protecting both the population and the state during periods of threat and danger (Akimbayev et al. 2024).

Research by Parker et al. (2019) on civil defence and crisis management within the EU has revealed significant differences among national systems in terms of administrative responsibilities, legal frameworks, and operational procedures. In most European member states, civil defence responsibilities are managed by national civil defence organizations, which typically operate under the administration of the Ministry of the Interior, the Ministry of National Defence, or the Ministry of Citizen Protection.

5.2 Interdisciplinary Approaches to Civil Defence

The field of civil protection is inherently interdisciplinary, as it requires collaboration across various disciplines to effectively prepare for and manage risks associated with emergencies and disasters. This interdisciplinarity is particularly evident in two key areas: crisis classification and the implementation of civil defence measures. Broadly speaking, crises can be categorized into two types: (1) natural crises and (2) human-induced (man-made) crises. Depending on the origin of the crisis, both preventive and reactive civil defence measures must be tailored to the specific situation.

For example, territorial threat analysis enables authorities to allocate resources more efficiently before and during natural disasters. This process, which involves assessing geographical variations, often requires input from environmental scientists and geographers (Pokorny et al. 2020). Similarly, a study by Sobolewski (2020) highlights the role of military support in non-military crises, using the Polish Armed Forces as a case study. Additionally, if any danger to the health and life of the population arises, the health sector becomes involved. Education is another essential component of civil protection, as it is crucial for both the general population and public sector (and private sector) employees. Research by Soumaya (2024) demonstrates that training significantly enhances the performance of civil defence workers by improving their skills and increasing their ability to adopt new methods. Moreover, regulatory and legal considerations—both domestic and international—are integral to civil defence planning and execution. These examples illustrate that the development and implementation of civil defence measures are at the intersection of many different areas and disciplines.

5.3 Civil Defence in Estonia

Like the United States and many other European countries, Estonia follows an all-hazards approach to civil defence. This approach ensures preparedness for both military and peacetime crises, encompassing measures that account for the full scope of emergencies and disasters (Tross 2023).

This section provides an overview of the fundamental principles of civil defence in Estonia, drawing on national policy documents and regulations that shape the field. According to the Preamble of the Constitution of the Republic of Estonia, the state has an obligation to safeguard internal and external peace and ensure societal security (The Constitution of the Republic of Estonia). This includes planning and, when necessary, implementing measures to protect residents in emergency situations. Systematic and coordinated civil defence measures are employed to manage various crises, encompassing preventive, preparatory, reactive and restorative activities.

In 2023, the Estonian parliament (Riigikogu) approved the Estonian National Security Concept.¹ This document defines the objectives of security policy, emphasizing Estonia's comprehensive national defence strategy. This strategy integrates military and non-military capabilities and resources while involving the public, private, and third sectors. The framework document outlines sector-specific objectives essential for safeguarding Estonia's sovereignty and independence. The primary goal of civil defence is to support the population during crises, including wartime, and to enhance self-reliance. Civil defence during crises entails preparedness for early warning systems, rescue operations, evacuation, sheltering, first aid, disaster medicine, essential social assistance, psychosocial crisis intervention and other critical services. For civil defence to function effectively, individuals must be able to support themselves and assist others until official help arrives. The Concept underscores that the resilience of both the state and society must be developed comprehensively and in a coordinated manner, requiring effective cooperation between constitutional institutions, national authorities and local governments. It also adheres to the principles of continuity and subsidiarity, ensuring that responsibilities are fulfilled both in peacetime and during crises or war (Ministry of Defence 2023).

Estonia's first Concept for Civil Defence was published in 2018 and defines civil defence as follows: "Civil protection is a system of measures aimed at protecting people in emergency situations and against threats to national security or constitutional order" (Government Office and Ministry of Interior 2018, p. 7). The term "emergency" is legally defined in the Emergency Act (*Hädaolukorra seadus*) as "an event, a chain of events, or a disruption of a vital service that poses a threat to public health and safety, causes significant material or environmental damage, or leads to severe disruptions in essential services. Managing such situations necessitates rapid and coordinated action across multiple agencies, alternative management structures, and the mobilization of additional personnel and

¹ The edition is the fifth Estonian National Security Concept, the previous concept being devised in 2017. The document is drafted by the government and approved by parliament.

resources” [Emergency Act § 2(1)]. The same Act also defines “vital service” as “a service critical to societal functioning, the disruption of which poses an immediate risk to life, health, other essential services, or national security” [Emergency Act § 2(4)]. According to § 36 of the Emergency Act, vital services include mobile telecommunications, digital identification, electricity and natural gas supply, road infrastructure maintenance, healthcare services, financial transaction systems, and water supply and sewerage management. The Act also specifies the authorities responsible for ensuring continuity in these services.²

In February 2024, the Estonian government approved the second framework documents for civil defence: the Civil Defence Framework Document and Civil Defence Action Plan 2024–2027³ (Government Office et al. 2024a, b). This document defines sectoral objectives and roles within the framework of comprehensive national defence, responding to the evolving security landscape. The framework builds upon the Estonian National Security Concept and aims to provide a structured and coherent development strategy for civil defence, emphasizing clarity of roles. The document designates the Government Office as the coordinating entity for civil defence activities, with various ministries responsible for implementation. Relevant institutions are tasked with peacetime preparations, ensuring operational readiness in collaboration with partner organizations. The key stakeholders include the Ministry of the Interior, the Ministry of Social Affairs, the Social Insurance Board, the Health Board, the State Chancellery, the Estonian Rescue Board, local governments, and private and third-sector organizations (Government Office et al. 2024a, b).

The framework document outlines nine key civil defence measures, setting target activity levels and preventive development actions to ensure their effectiveness during crises. These measures prioritize readiness for worst-case scenarios, ensuring the country can also manage less severe crises effectively. The primary areas of focus include:

1. Warning messages,
2. Rescue operations,
3. Mass evacuation,
4. Sheltering,
5. First aid and disaster medicine,
6. Essential social assistance,
7. Psychosocial crisis intervention,
8. Crisis preparedness for the public and local governments,
9. Crisis management and coordination.

² Authorities organising continuity thereof: The Ministry of Justice and Digital Affairs, The Ministry of Climate, The Ministry of Social Affairs, The Ministry of Culture, The Bank of Estonia, The Ministry of Regional Affairs and Agriculture, and local authorities.

³ Neither the entire Civil Defence Framework Document nor Civil Defence Action Plan 2024–2027 is intended for public use.

The priority areas of civil defence include enhancing public crisis awareness and independent readiness, developing emergency warning solutions, strengthening local governments' crisis capabilities, and ensuring service continuity among agencies responsible for crisis response (Government Office et al. 2024a, b). Volunteerism and public engagement are crucial for societal crisis preparedness, with the state actively supporting and promoting volunteer contributions to crisis resilience and response (Government Office 2025). The Estonian Concept for Civil Defence categorized civil defence activities into three areas: raising awareness, ensuring population protection, and providing assistance (Government Office and Ministry of Interior 2018). These activities are guided by the National Risk Assessment, which is overseen by the Government Office (2025). Across all policy documents, the emphasis remains on institutional cooperation to safeguard residents during crises.

Estonia's crisis management cycle adheres to the Principle of Subsidiarity, whereby the responsibility for managing a crisis event rests with the lowest and most appropriate administrative level. Local governments are the first responders to crises within their jurisdictions. If the situation escalates, higher-level authorities such as the Rescue Board intervene. The Rescue Board functions as Estonia's national civil defence organization under the Ministry of the Interior (Ministry of Interior 2021).

In summary, the key trends in Estonian civil defence focus on increasing public readiness to withstand crises independently and strengthening cooperation among stakeholders. Civil defence planning follows an all-hazards approach, addressing the nature of potential threats rather than their origins. This ensures that measures are applicable to all types of crises, whether civil or military, while maintaining the principles of continuity and subsidiarity in crisis management.

5.4 Collaboration Between Civil Defence and the Cultural Sector: Opportunities and Challenges

The principles and measures of Estonian civil defence emphasize the importance of cooperation among various stakeholders to enhance the resilience of both individuals and the state while ensuring public safety during crises. The Civil Defence Framework Document and the Civil Defence Action Plan 2024–2027 outline civil defence measures, target levels and responsible agencies. However, the pathways to achieving these targets remain largely unrestricted, apart from regulatory constraints. Given the increasing number of diverse and unpredictable risks, it is essential to analyse and, where feasible, implement innovative approaches to strengthen resilience. As civil defence in Estonia is fundamentally built on contributions from multiple societal sectors, this section explores the intersection of civil defence and the cultural sector in achieving civil defence objectives.

As civil defence in Estonia is fundamentally built on contributions from multiple societal sectors.

The cultural sector is a vast domain encompassing a range of institutions and activities across private, public, and third-sector organizations. Due to its broad scope, a comprehensive list of activities is difficult to compile. Within this context, the role of cultural institutions will first be examined as physical spaces. Secondly, the professional perspective of those working in the cultural sector will be considered. Lastly, public attitudes towards the cultural sector and its integration with civil defence will be analysed.

In the context of this chapter, the terms cultural institution, cultural centre, and community house⁴ are not interchangeable, even though they are often used in overlapping ways in policy and practice. For analytical clarity, this chapter employs the following distinctions. The term cultural institution is used as the broadest category, encompassing museums, theatres, galleries, archives, and other organizations dedicated to cultural production, preservation, and dissemination. Within this domain, cultural centres and community houses are understood as locally accessible, publicly oriented facilities that provide opportunities for cultural participation, learning, and social engagement. They are multi-functional spaces that often act as hubs for community activities in addition to hosting professional cultural performances. In the Estonian context, a cultural centre (*rahvamaja*) is a public space where local residents can participate in various cultural and community leisure activities, either by creating their own cultural content or by enjoying professional cultural performances. As of May 2023, there were 376 cultural centres in Estonia (Kulbok-Lattik et al. 2023).

Cultural institutions serve as multifunctional spaces beyond their primary cultural purpose. A qualitative content analysis by Pfeifere (2022) on the role of cultural centres in European countries underscores this notion. Her study categorizes cultural centre functions into four key areas: arts and culture, education, leisure and recreation, and social engagement. Educational functions include informal learning opportunities, lifelong learning programmes, and interactive activities such as workshops, debates, and lectures. Social functions encompass integration activities, cross-cultural dialogue, and community engagement through artistic and cultural initiatives (Pfeifere 2022). Likewise, modern museums foster a dynamic relationship between culture and learning, offering educational programmes through exhibitions, guided tours, lectures, seminars, and workshops (Tišliar 2017). These examples highlight cultural institutions as community hubs rather than mere venues for professional artistic pursuits.

Given these existing roles, cultural institutions could be leveraged to support civil defence objectives. According to the Estonian Civil Defence Framework Document, public awareness and training are essential for enhancing crisis preparedness (Government Office et al. 2024a, b). Cultural institutions could serve as ideal venues for civil defence education, offering lectures, seminars, workshops, and training exercises. Additionally, they could be utilized as crisis response facilities, providing essential services such as first aid, emergency social care, evacuation shelters, and resilience centres.

⁴ In this chapter, the terms “community house” and “cultural centre” are used interchangeably.

Ownership structures must also be considered when integrating cultural institutions into civil defence frameworks. Cultural institutions are categorized into three primary ownership types: governmental, private, and public–private partnerships. From a civil defence perspective, collaboration with government-owned institutions is often the most efficient, posing fewer administrative challenges than partnerships with private institutions. However, further academic and participatory research is needed to draw definitive conclusions. An expert interview with a representative from the Estonian Rescue Board highlights that community centres owned by local governments are well-suited for civil defence initiatives due to their structured governance, which ensures systematic implementation of national civil defence measures (Vihlver 2025).

Ownership structures must also be considered when integrating cultural institutions into civil defence frameworks.

Cultural managers play a crucial role in facilitating cultural engagement by creating opportunities for participation in cultural activities, both as creators and consumers (Mets and Viia 2019). The field of cultural management requires a blend of leadership, communication, creativity, cultural intelligence, and specialized knowledge. Many of these competencies—such as effective communication, adaptability, and organizational skills—are also critical in civil defence contexts. The Estonian Civil Defence Framework Document includes several measures requiring such skills, particularly in organizing essential services and disseminating crisis-related information.

Creative professionals, too, contribute significantly to society. Their skills, characterized by innovative thinking, adaptability, collaboration, curiosity, emotional intelligence, and a willingness to take risks, could be harnessed for civil defence efforts. To enhance crisis awareness and resilience, national authorities and local governments could collaborate with creative professionals to use artistic mediums as information dissemination tools. Examples include thematic exhibitions, documentary content for social media, and television campaigns to raise awareness of civil defence measures. For example, at the end of 2022, the Estonian National Museum opened the exhibition “*Be Prepared! My Story of Coping in a Crisis.*” The exhibition presented the experiences and advice of Estonian citizens on how to manage in emergency situations. Under the initiative of the Estonian National Museum, the Estonian Rescue Board, and the Women’s Voluntary Defence Organisation, stories, photographs, and artefacts were collected, while actors from Paide Theatre produced thematic video narratives. (Estonian National Museum 2022).

Thirdly, there is the issue of public attitudes towards cultural sector integration with civil defence. Empirical evidence suggests that cultural centres have already played a role in civil defence efforts in Estonia. For instance, during the COVID-19 pandemic, cultural centres facilitated vaccination programmes and rapid testing initiatives (Väre 2021; Tallinn 2022). Similarly, following the outbreak of the full-scale war in Ukraine, community centres became focal points for grassroots mobilization, such as organizing sock-knitting campaigns for Ukrainian soldiers (Kulbok-Lattik et al. 2023). Further support for this

integration comes from the research of Paton (2007), who examined the factors influencing trust in information sources during natural disasters. His study found that people are more likely to trust and follow instructions from an informant in a crisis if they have had prior positive interactions with them. These interactions do not necessarily need to be related to disaster preparedness but can stem from previous engagement in other areas, such as regular contact with officials from public institutions. This finding is particularly relevant in rare and unfamiliar crisis situations, such as volcanic eruptions or earthquakes, where people tend to seek guidance from institutions they already trust.

These instances indicate a willingness within the cultural sector to engage in civil defence efforts. However, fully institutionalizing this integration will require time, both in terms of organizational adaptation and shifts in public perception.

5.4.1 Perspectives of Cultural Workers on Resilience Centres

This and the following section build upon the author's article, "The Potential of Using Local Government's Community Houses (*Rahvamajad*) as Resilience Centres," published in 2025 (Vihlver 2025).

Effective and timely crisis communication supports appropriate resident responses during emergencies, whereas slow or ineffective communication can lead to misinformation, panic and inappropriate behaviour. A well-structured information flow system must be established before a crisis occurs, taking into account regional specificities and community size. Additionally, it must be tested in advance to identify potential weaknesses and failures (Comfort and Haase 2006). The Civil Defence Framework Document emphasizes the necessity of utilizing multiple threat notification and crisis communication channels (Government Office et al. 2024a, b). One effective approach is the establishment of resilience centres—physical locations managed by local governments or communities, where residents can access information, guidance, and assistance during a crisis (Estonian Rescue Board 2024). These centres must be prepared during the crisis readiness phase, ensuring that residents are informed in advance about where to seek help in times of emergency (Government Office et al. 2024a, b).

Survey results indicate a high willingness among cultural workers to support resilience centre operations, though some expressed concerns regarding their crisis-related expertise. Cultural workers were asked to rate, on a six-point scale, the suitability of incorporating a resilience centre function within cultural centres, with 6 representing "very suitable" and 1 indicating "not suitable at all." A majority—61% of cultural workers—considered this integration suitable. However, responses varied based on experience, with cultural workers having over ten years of experience rating suitability lower (4.48) than those with up to ten years of experience (4.86).

The overall readiness of cultural workers to engage in resilience centre operations is high, with 81% of respondents willing to participate. Respondents showed a slightly

higher willingness to serve as support workers rather than information mediators. Information mediators are responsible for communicating with crisis management personnel and conveying essential guidelines to residents, whereas support workers assist in logistical tasks, such as operating diesel generators and organizing spaces. Five respondents indicated that they were unwilling to take on either role.

The overall readiness of cultural workers to engage in resilience centre operations is high.

Cultural workers identified a lack of knowledge as the main obstacle to their participation in resilience centres, while personal qualities were seen as their strongest assets in fulfilling these roles. Additional barriers included a lack of relevant skills and health conditions. Notably, nearly half of the respondents reported no hindrances to their participation, while two respondents stated that no conditions would support their involvement.

Engaging cultural workers in crisis management and resident protection efforts can be highly beneficial, as they are familiar with local residents, facilitating swift and effective crisis response. Based on the findings of this study, future research could focus on identifying the key competencies required for resilience centre personnel and the most effective training methods for cultural workers. Such research would help assess whether training cultural workers within cultural centres is a viable and resource-efficient approach to enhancing community resilience during crises.

5.4.2 Cultural Centres as Resources for Civil Defence

This section provides an overview of empirical evidence suggesting that cultural centres have already played a role in civil defence efforts in Estonia. An expert interview with a representative from the Estonian Rescue Board indicates that, if a cultural centre has a basement or other suitable shelter space, it could be used as a refuge during military conflicts. Additionally, cultural centres could serve as evacuation sites. However, the expert suggests that cultural centres would primarily be suitable for responding to milder civil crises, such as prolonged power outages (Vihlver 2025).

Vihlver (2025) conducted a survey among local governments to assess their perspectives on the role of cultural centres in civil defence. Respondents identified several key functions, including providing information and guidelines, serving as gathering points, and facilitating the distribution of food and drinking water. Evacuation and sheltering functions were also mentioned. Furthermore, local government representatives highlighted the importance of preparedness activities, such as organizing training sessions and emergency drills. These findings indicate a shared view among experts and local officials that cultural centres could integrate civil defence functions, particularly those related to disseminating information and fostering community resilience.

Experts suggest that cultural centres are well-suited to function as resilience centres due to their existing infrastructure and human resources. Cultural centre employees are often deeply embedded in the local community, facilitating effective communication and coordination during crises. Additionally, cultural centres are well-known landmarks, making them easily accessible. Local government representatives recognize the potential to expand these functions, noting that many cultural centres have ample space for gatherings. Moreover, during crises, cultural activities are typically suspended, ensuring the availability of these spaces. Some centres are also equipped with autonomous power sources, such as generators or wood-burning stoves. However, it is acknowledged that not all centres have sufficient storage capacity for emergency supplies or the necessary level of autonomy.

Cultural centres are well-suited to function as resilience centres due to their existing infrastructure and human resources.

The Kaja Cultural Centre in Tallinn exemplifies the potential for cultural centres to serve as resilience hubs. Its designated functions include disseminating information, providing first aid and offering temporary accommodation—an essential function of an evacuation site. The building has an independent power supply, ensuring warmth and lighting for several days (Tallinn.ee 2023). Similarly, the Sõmeru Centre is prepared to function as a resilience hub, offering heated spaces, water, and sanitation facilities during crises (Rakvere Municipality [s.a.]). The centre accommodates municipal offices, a community club, a day centre, and a library (Aasa 2020).

5.5 Conclusion

This chapter builds on the principles of Estonian civil defence and the role of culture in resilience, aiming to introduce a fresh and unexplored dimension of civil defence. Estonia's civil defence policy prioritizes increasing the population's ability to cope independently in crisis situations, a goal that necessitates multifaceted efforts and innovative solutions.

The chapter explored the interaction between civil defence measures and the cultural sector using Estonia as a case study. Findings indicate that the cultural sector holds significant potential for supporting civil defence initiatives. Cultural institutions can function as centres for crisis education and resilience, while cultural workers offer valuable skills for crisis management. Precedents from Estonia also suggest a degree of public readiness for such integration. However, to fully realize this potential, further research and structured collaboration between civil defence authorities and cultural institutions will be essential.

References

- Aasa A (2020) Sõmeru keskusehoone 10. <https://dea.digar.ee/article/rakverevalla/2020/09/01/2>. Accessed 27 April 2025
- Akimbayev Y, Akhmetov Z, Abdykalykov A, Kuanyshbayev M, Kulshimbayev I (2024) Operation procedures of civil defence authorities in time of war. *Soc Leg Stud* 7:9–17. <https://doi.org/10.32518/sals1.2024.09>
- Comfort LK, Haase TW (2006) Communication, coherence, and collective action: the impact of hurricane Katrina on communications infrastructure. *Public Works Manage Policy* 10:328–343. <https://doi.org/10.1177/1087724X06289052>
- Estonian National Museum (2022) Ole valmis! Minu kriis hakkama saamise lugu. <https://www.erm.ee/et/ole-valmis-naitus>. Accessed 4 Oct 2025
- Estonian Rescue Board (2024) Kerkuskeskus: eesmärk, toimimise põhimõtted ja kirjeldus. <https://www.rescue.ee/files/Juhendid/kerkuskeskuse-toimimise-pohimotted.pdf?66412ac290>. Accessed 26 Feb 2025
- Government Office (2025) National risk analysis. <https://www.riigikantselei.ee/en/national-risk-analysis/national-risk-analysis#preparedness>. Accessed 27 Feb 2025
- Government Office, Ministry of Interior (2018) Elanikkonnakaitse kontseptsioon. <https://kriis.ee/media/2048/download>. Accessed 27 Feb 2025
- Government Office, Ministry of Social Affairs, Ministry of Interior (2024a) Civil defence framework document. <https://kriis.ee/sites/default/files/documents/2024-02/Elanikkonnakaitse%20raamdokument.pdf>. Accessed 27 Feb 2025
- Government Office, Ministry of Social Affairs, Ministry of Interior (2024) Civil defence action plan 2024–2027. <https://kriis.ee/media/2485/download>. Accessed 27 Feb 2025
- Kulbok-Lattik E, Roosalu T, Saro A (2023) Eesti Rahvamajade uuring 2022–2023. <https://www.kul.ee/sites/default/files/documents/2023-12/Eesti%20rahvamajade%20uuringu%202022-2023.pdf>. Accessed 28 Feb 2025
- Mets U, Viia A (2019) Tulevikuvaade tööjõu- ja oskuste vajadusele—kultuur ja loometegevus: etenduskunstid, käsitöö, museoloogia, muusika, raamatukogundus, sport. *Uuringuaruanne*. https://oska.kutsekoda.ee/wp-content/uploads/2017/10/OSKA-Kultuur-ja-loometegevus_I-osa_uuringuaruanne_2019_06.04.20.pdf. Accessed 07 Mar 2025
- Ministry of Defence (2023) Estonian national security concept. https://www.kaitseministeerium.ee/sites/default/files/eesti_julgeolekupoliitika_alused_eng_22.02.2023.pdf. Accessed 28 Feb 2025
- Ministry of Interior (2021) Kriisireguleerimispoliitika ülevaade 2021. <https://www.siseministeerium.ee/media/1470/download>. Accessed 28 Feb 2025
- Parker CF, Persson T, Widmalm S (2019) The effectiveness of national and EU-level civil protection systems: evidence from 17 member states. *J Eur Public Policy* 26:1312–1334. <https://doi.org/10.1080/13501763.2018.1523219>
- Paton D (2007) Preparing for natural hazards: the role of community trust. *Disaster Prev Manage Int J* 16:370–379. <https://doi.org/10.1108/09653560710758323>
- Pfeifere D (2022) The issues of defining and classifying cultural centres. *J Cult Econ* 19:28–37. <https://doi.org/10.2478/jec-2022-0013>
- Pokorný J, Machalova B, Slivkova S, Brumarova L, Vlcek V (2020) Planning of safety of cities and territory from the point of view of population protection in the Czech republic. *Sustainability* 12:9487. <https://doi.org/10.3390/su12229487>
- Sobolewski G (2020) Possibilities of using the polish armed forces in non-military crises in the aspect of changes in the command and control system. *Sci J Mil Univ Land Forces* 198:874–889. <https://doi.org/10.5604/01.3001.0014.5873>

- Soumaya Z (2024) Impact of training on employees' performance: a case study of civil protection institution of Annaba. *J Econ Bus Financ* 8:99–107. <https://doi.org/10.58205/fber.v8i4.1903>
- Tallinn (2022) Lindakivi kultuurikeskuses saab teha tasuta kiirtesti. <https://www.tallinn.ee/et/uudis/lindakivi-kultuurikeskuses-saab-teha-tasuta-kiirtesti>. Accessed 28 Feb 2025
- Tallinn.ee (2023) Tallinn loob igasse linnaosasse kriisideks ja kodanike abistamiseks kerkuskeskused. <https://www.tallinn.ee/et/kriisiennetus/uudis/tallinn-loob-igasse-linnaosasse-kriisideks-ja-kodanike-abistamiseks-kerkuskeskused>. Accessed 27 Feb 2025
- The Constitution of the Republic of Estonia (1992). RT, vol. 26, p. 349
- Tišliar P (2017) The development of informal learning and museum pedagogy in museums. *Eur J Contemp Educ* 6:586–592. <https://doi.org/10.13187/ejced.2017.3.586>
- Tross J (2023) Elanikkonnakaitse areng Eestis iseseisvuse taastamise järgsel perioodil. *Turvalisuskompas* 1:143–165. <https://doi.org/10.1515/txa4-gd86>
- Väre H (2021) Koroona vastu saab süstida mitmel pool maakonnas. <https://sakala.postimees.ee/7312390/koroona-vastu-saab-sustida-mitmel-poolmaakonnas>. Accessed 26 Feb 2025
- Vihlver A-M (2025) Kohalike omavalitsuste rahvamajade perspektiiv kerkuskeskustena ning kultuuritöötajate valmisolek kerkuskeskuse funktsiooniks. *Turvalisuskompas* 2:79–106. <https://doi.org/10.1515/9d8h-4n59>

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.



Geopolitical Dynamics and Disaster Risk Management: Involvement of Third Countries in the COVID-19 Response in Italy

6

Georg-Henri Kaup 

Abstract

This chapter examines how non-EU, i.e., “third” countries—namely China and Russia—exercised influence through medical assistance during the early months of the COVID-19 pandemic in Italy. By analyzing government documents, media coverage, and policy communications from February to May 2020, the chapter shows that third-country aid arrived at a pivotal moment when Italy’s healthcare system, lacking critical resources, was overwhelmed. Swift, highly visible support from China and Russia significantly shaped Italian public opinion, raising questions about the reliability of traditional partners such as the European Union and the United States. Although these interventions momentarily boosted the popularity of closer ties with non-EU actors, the chapter argues that deep-rooted political affiliations and economic interdependencies ultimately reaffirmed Italy’s traditional geopolitical orientation. Over time, more cohesive EU policies—ranging from emergency funding measures to a comprehensive recovery plan—mitigated early skepticism about European solidarity. In assessing the short- and long-term repercussions of this “disaster diplomacy,” this chapter demonstrates how acute crises can serve as catalysts for geopolitical maneuvering and tests of international alliances. It concludes that, based on the Italian case, while immediate displays of foreign aid can shift public perception, entrenched alliances tend to endure once the immediate crisis subsides.

G.-H. Kaup (✉)

Research Centre of the Internal Security Institute, Estonian Academy of Security Sciences, Tallinn, Estonia

e-mail: georg-henri.kaup@sisekaitse.ee

Keywords

COVID-19 • Disaster diplomacy • European union • Humanitarian aid • Soft power

6.1 Introduction

With 519 COVID deaths per 100,000 people (as of June 2024), Italy was struck worst among Western¹ nations by the COVID-19 pandemic (Mathieu et al. 2020). On March 19, 2020, Italy surpassed China to become the country with the biggest number of COVID deaths in the world at the time (Coronavirus, l'Italia supera la Cina 2020). With over 700 thousand deaths, 2020 ended up becoming the deadliest year in Italy since the Second World War (WWII) (skytg24 2021).

Barnett (2005) observes that humanitarianism has, by the third millennium, become “firmly part of politics” (Barnett 2005). Drury et al. (2005), examining U.S. humanitarian aid policies between 1964 and 1995, likewise conclude that American aid officials “do what is politically relevant,” and that “U.S. humanitarian aid is strongly political” (Drury et al. 2005). In the context of disaster risk management, this intertwining of humanitarian action and geopolitics underscores the influence of powerful states and their strategic interests on aid distribution. Barnett and Weiss (2011) further illustrate how:

“Humanitarianism cannot help but become part of politics and governance, and even coincide with the grand strategies of powerful states” (Barnett and Weiss 2011).

Thus, Barnett and Weiss (2011) reinforce the idea that geopolitical dynamics hold a central place in shaping not only the allocation of resources but also the broader frameworks within which disasters are anticipated and addressed.

This chapter examines the involvement of non-EU countries—primarily China and Russia—in Italy’s COVID-19 emergency response, highlighting how these interventions intersected with broader geopolitical strategies. The analysis begins by situating Italy in its historical and geopolitical context, followed by case studies of aid and “disaster diplomacy” by third countries. Section 6.5 explores the impact of these interventions on Italy’s immediate risk management, while Sect. 6.6 delves into the longer-term geopolitical implications for Italy’s foreign policy alignment and EU unity. Section 6.7 offers a critical assessment of how “disaster diplomacy” played out in this scenario, and Sect. 6.8 puts forward lessons learned and recommendations for future crises. Finally, Sect. 6.9 concludes with reflections on the complexities of managing disasters amid competing geopolitical interests, while Sect. 6.10 offers prospects for international cooperation in health emergencies. This chapter employs documentary sources, media content analysis, and targeted policy review to examine how Chinese and Russian aid intersected with Italy’s crisis management and to what extent this influenced Italy’s geopolitical alignment.

¹ Defined here as “a member of the Western European and Others Group at the United Nations.”

6.2 Methods

6.2.1 Design and Scope

This chapter uses a mixed-methods design combining (i) documentary research, (ii) qualitative media content analysis, and (iii) targeted policy review to examine how third-country assistance (notably from China and Russia) interacted with Italy's emergency management during the first wave of the COVID-19 pandemic (February–May 2020). The unit of analysis for the media component is the individual newspaper article; for the documentary/policy component it is the individual official document or communication. The geographical focus is national-level (Italy), with the EU-level included where it is pertinent, i.e., where it directly affected Italy's public debate (e.g., export controls, Civil Protection Mechanism activations, SURE/NextGenerationEU).

The chapter's analytic aims are to: (a) reconstruct a time-sequenced event log of requests, shipments, and policy decisions; (b) characterize how aid from non-EU states was framed in Italian mass media at the time; and (c) interpret short-term perception shifts and longer-term geopolitical continuity in light of EU actions that followed.

6.2.2 Data Sources and Sampling

Primary materials comprised press releases, situation reports, and official bulletins from the Italian Ministry of Health/Protezione Civile, the European Commission, and the World Health Organization. Where relevant, Prime Minister's Office and Ministry of Foreign Affairs statements, and embassy communiqués (e.g., Chinese Embassy announcements) were captured to contextualize bilateral aid. These documents anchor dates and quantities (e.g., shipments, staffing deployments) and the sequence of EU measures (from initial export restrictions to emergency financing and the recovery plan).

The media sample consisted of seven of Italy's highest-circulating newspapers, selected to reflect ideological diversity and editorial breadth (including *La Stampa*, *Corriere della Sera*, *La Repubblica*, plus four other national dailies of comparable reach). The time window was February 1 –May 31, 2020. Inclusion criteria: articles that mention foreign assistance, assess solidarity/inaction, or take a stance toward China, Russia, the EU, or the US in the context of Italy's COVID-19 emergency. Articles were identified via site searches and public archives using Italian keywords (illustrative terms included “Cina,” “Russia,” “aiuti,” “mascherine,” “ventilatori,” “solidarietà,” “Unione Europea,” “export,” “divieti”).

Where available, contemporaneous polls (e.g., the SWG survey reported 7 April 2020) and selected social media posts of official channels (e.g., the Chinese Embassy in Italy) were treated as contextual evidence to triangulate media frames with public sentiment.

6.2.3 Coding and Analysis

A structured event log was compiled with fields for date, actor (China, Russia, EU, Italy, US/other), measure or shipment (e.g., masks, ventilators, medical teams; EU instruments), source(s) (official and/or media), and verification status. Inclusion rule: claims about shipments or policy acts were logged only when corroborated by either (i) an official communication and at least one mainstream outlet, or (ii) two mainstream outlets of record (national or international). This yielded a chronology used to interpret perception swings versus subsequent policy stabilization.

Articles were coded by the author using a pre-specified codebook with the following top-level categories:

- Aid source (China/Russia/EU/US/other).
- Aid modality (PPE/ventilators/medical staff/logistics/financial/policy).
- Frame (e.g., solidarity/helpfulness, strategic opportunism/“disaster diplomacy,” EU inaction/fragmentation, EU responsiveness/recovery, skepticism/controversy).
- Stance/valence toward the aid source (positive/neutral/negative), based on headline language and lead paragraphs.
- Visibility markers (e.g., visuals of cargo planes, numbers emphasized, mentions of high-profile visits/phone calls), used to proxy salience and spectacle.

Coding proceeded in two passes: an initial calibration on a small subset to refine operational definitions, then full coding of in-scope articles. Ambiguous items were assigned a neutral stance by default and flagged for cross-checking against the documentary timeline. The interpretive synthesis juxtaposed early-phase media frames (March–April) with the later EU policy ramp-up to assess whether initial “aid optics” had enduring geopolitical effects.

EU-level acts (export controls, Temporary Framework on state aid, SURE, and NextGenerationEU) were read for problem framing, instrument choice, and timing relative to Italy’s peak needs to understand why short-term sentiment could diverge from long-term alignment. These materials anchor the claim that institutional gravity re-asserted itself once EU responses scaled.

6.2.4 Limitations and Validation

Early-pandemic reporting sometimes contained incomplete or shifting figures on caseloads and shipment contents. The event log therefore prioritized cross-checked entries (see inclusion rule above) and updated items where official corrections emerged.

Focusing on seven leading dailies risks over-weighting agenda-setting outlets. Diversity of editorial lines was used as a partial countermeasure; still, media frames are not treated

as public opinion, only as inputs to it. Where polls existed, they were used for context—not as causal proof.

Coding was conducted by the author; without a second coder, inter-coder reliability cannot be reported. To mitigate bias, the codebook defined decision rules (default-to-neutral if ambiguous; explicit language required for positive/negative stance), and borderline items were revisited after timeline triangulation.

The focus is Italy; EU actions are used where they shape Italy's context. Findings are analytically transferable but not statistically generalizable without further comparative work.

6.2.5 Ethics and Data Availability

All sources used in this chapter are publicly accessible government/organization documents, media articles, and publicly reported polls; no human subjects were interviewed, and no personal data were processed, meaning ethics approval and informed consent are not applicable.

6.3 Geopolitical Context of the COVID-19 Crisis in Italy

6.3.1 Italy's Geopolitical Positioning Pre-COVID-19

Geopolitically, Italy has been a member of the American-led 'Western camp' since 1948, when American aid delivered under the European Recovery Plan (the ERP; more commonly referred to as the "Marshall Plan") created enough goodwill among the Italian population to preclude the pro-Soviet Popular Democratic Front (Fronte Democratico Popolare), made up of the Italian Communist Party (Partito Comunista Italiano) and the Italian Socialist Party (Partito Socialista Italiano), from winning the 1948 Italian general election. The following year, led by a pro-American government led by the center-right Christian Democracy (Democrazia Cristiana) party, Italy became a founding member of the American-led military alliance, the North Atlantic Treaty Organization (NATO), which the Italian government at the time (correctly) perceived as the "fulcrum" of future Western political and military cooperation. Furthermore, Italy took a leading role in the first intergovernmental, pan-European institutions created by ERP recipients—the Council of Europe (1949), the European Payments Union (1950) and the European Coal and Steel Community (1950; the precursor to the EU). Italy's center-right government understood that Italy had more to win than to lose from looser trade barriers and free movement of people in Western Europe. Gilbert (2024) argues that pursuing the pan-European project became an essential part of post-WWII Italian identity (Gilbert 2024).

As a result, Italy's relationship with both China and Russia—the other protagonists of this story—was viewed with a degree of suspicion by the bulk of Italy's politicians and print media from 1948 up to the start of the COVID-19 pandemic. Italy did not recognize the People's Republic of China until 1970 (*Storia and Diplomazia: Rassegna Dell'Archivio Storico Del Ministero Degli Affari Esteri* 2013). In 2019, the Italian parliamentary security committee described fears of Chinese state actors penetrating Italy's planned 5G networks as “well-founded” and suggested excluding Chinese companies from public tenders for the supply of 5G technology to Italy (Fortuna 2019). Nevertheless, in March 2019, Italy signed a memorandum of understanding with China on cooperation within the framework of China's 21st Century Maritime Silk Road Initiative (more commonly referred to as the “Belt and Road Initiative”). The memorandum outlined cooperation between China and Italy in policy, infrastructure development, trade and investment, financial matters and green development via high-level visits, information sharing and joint research (Baldassarre 2019). The memorandum was signed by an Italian government made up of two parties, which had not existed during the Cold War—the left-wing populist Five Star Movement (Movimento 5 Stelle) and the right-wing populist League (Lega)—and were thus not party to the post-WWII, pro-U.S. and pro-EU consensus that had formed among Italian parties that had existed during the Cold War (including the Italian Communist and Socialist Parties that had both adopted pro-NATO and pro-EU positions by the 1980s) (Cristiani 2019). As a result, the decision to sign the memorandum by the government was criticized by Italy's opposition politicians and major newspapers, with nefarious connections suggested between certain government officials and China (Pompili 2019).

While the powerful Italian Communist Party provided a conduit between the Soviet Union and Italy after WWII, its absence from every Cold War-era Italian national government meant that Italy remained solidly anchored in the U.S.-led “Western camp” during the Cold War. Soviet–Italian relations were characterized by mutual economic interest in the Cold War era—the Italian state oil company ENI became the first oil company in a NATO country to purchase crude oil from the Soviet Union during the Cold War in the 1960s, and the Italian automobile company FIAT set up a factory in the USSR in the 1970s. Russo–Italian relations in the post-Cold War era were colored by the strong personal relationship between Russia's president Vladimir Putin (in office: 2000–08; since 2012) and Italy's Prime Minister Silvio Berlusconi (in office: 1994–95; 2001–06; 2008–11), which led, among all else, to the establishment of a NATO–Russia Council in Pratica di Mare, Italy, in 2002. After Berlusconi's ouster in 2011, bilateral relations between Italy and Russia cooled somewhat, with Italy's first post-Berlusconi prime minister, Mario Monti, deferring to policies toward Russia agreed on the EU level. Nevertheless, legacies of the Cold War and Berlusconi eras kept Italy as one of the closest Western countries to Russia after 2011: in 2012, ENI, with the Italian government's support, partook in the building of a gas pipeline (South Stream) opposed by the EU (Siddi 2012).

Nevertheless, the support of close relations with Russia in Italy remained the remit of the business community and politicians whose parties that had originated after the Cold War (Berlusconi's Forza Italia, the Five Star Movement, and Lega). Italian politicians and media that had their legacies in the Cold War era remained skeptical of close relations with Russia. In 2016, *La Stampa* (founded in the nineteenth century), the fourth-largest Italian newspaper by circulation at the time, with a socially liberal outlook, accused Russia of being behind a campaign to discredit a constitutional referendum (ultimately defeated) called by Matteo Renzi, Italy's prime minister between 2014 and 2016, who had gotten a start in an outgrowth of the Christian Democracy Party (the party, as well as the Italian Communist and Socialist Parties, had dissolved in the early 1990s, with their former members establishing dozens of new political parties) (Iacoboni 2016).

6.3.2 Initial Impact of the COVID-19 Pandemic

Late February and early March of 2020 saw the Italian healthcare system buckle under the pressure of the COVID-19 pandemic. Despite introducing Europe's first nationwide restriction on movement and public gatherings on March 9, 2020 (Horowitz 2020a), Italian hospitals experienced an acute shortage of both personnel (as doctors and nurses became ill with COVID) and equipment (respirators, ventilators, and face shields) (Horowitz 2020b). The shortages in equipment became severe enough to prompt private enterprises in the Italian textile, printing, beverage, chemical and engineering sectors to start producing facial masks. However, as most of these products were produced without the proper certification, they rarely made it to hospitals and were mostly sold or donated to private consumers instead. The crisis became so dire as to prompt the Italian military and gendarmerie to deploy their doctors and nurses to public hospitals, as well as to deploy military engineers to a factory that produced ventilators (Busto Arsizio, in ospedale mascherine con la stampante 3D 2020; Easy Covid 19, la maschera da sub si trasforma in respiratore 2020; Le valvole per la rianimazione scarseggiano 2020; L'Istituto Poligrafico contro il Coronavirus 2020; Cupelli 2020; De Stefani 2020; Giacomino and Scaparone 2020; Bergamini and Bucci 2020; Patucchi 2020; Pelosi 2020; Pietrobelli 2020).

6.3.3 The EU's Lack of Coordinated Response

On March 11, 2020, Italy's ambassador to the EU accused the other member states of a "lack of solidarity," pointing out how the EU institutions were engaging in mere "consultations" and not devising "emergency actions that are quick, concrete and effective." The statement came in the context of a refusal of EU members to answer Italy's call for extra supplies of medical equipment. Instead, both Germany and France imposed restrictions on

the export of medical equipment (Boffey 2020), with Germany further prohibiting international corporations, such as the U.S.'s 3 M, from exporting surgical gloves, respirators, masks, protective goggles, vizors, and other protective equipment from their German factories on March 12 (Coronavirus, La Germania Strozza l'Italia Sulle Mascherine 2020). This led to accusations of Germany "suffocating Italy" in the Italian media. In the words of the Italian ambassador to the EU, Italy "asked to activate the European Union mechanism of civil protection for the supply of medical equipment for individual protection. But unfortunately, not a single EU country responded to the commission's call. Only China responded bilaterally. Certainly, this is not a good sign of European solidarity" (Boffey 2020). The inaction of the EU was in sharp contrast to the immediate measures taken by China and Russia, which started shipping equipment and medical professionals to Italy in the first few months of the pandemic (Chazan et al. 2020).

6.4 Key Third-Country Interventions

In the Italian context, the term "third countries" (*paesi terzi*) generally refers to countries that are not part of the EU (Glossario 2020).

On March 11, 2020, the Chinese embassy in Italy announced the sending of a million masks, 1000 ventilators, and 9 specialized doctors from China to Italy. The 30-ton shipment, which arrived on March 13, was organized by the Chinese Red Cross. Afterward, the Chinese government promised to deliver 100 million masks to Italy from March 25 onwards, with 20 million masks delivered each week (China Sends Medical Supplies, Experts to Help Italy Battle Coronavirus 2020; Dalla Russia con amore, in arrivo gli aiuti di Putin 2020; Pelosi 2020).

After a phone call between Italy's then prime minister, Giuseppe Conte, and the Russian president, Vladimir Putin, on March 22, Russia dispatched nine 45-ton Ilyushin Il-76 cargo planes to Italy in a 24-h period to deliver 10 million masks, 600 ventilators, hazmat suits, swabs for COVID tests, 13 military-grade sanitation vehicles (with "From Russia with Love" painted on them in Russian, English, and Italian), as well as 122 doctors, 66 of them specialists in bacteriological warfare from the Russian military (Dalla Russia con amore, in arrivo gli aiuti di Putin 2020; Dalla Russia con amore 2020).

6.5 Impact of Third-Country Involvement

On March 11, 2020, after news of the Chinese shipment of masks, ventilators and doctors had been declared on the Facebook page of the Chinese embassy in Italy, posts such as "thank you," "you are great," and "unlike Europe, you are showing solidarity," appeared under the post from Italian Facebook users. Luigi di Maio, Italy's foreign minister at the

time, attributed the successful acquisition of masks and pulmonary respirators to having “called China” on the “La Vita in Diretta” television show (broadcast on the Italian state-owned public broadcaster’s flagship television channel, Rai 1) on March 10, and proceeded to emphasize how Italy’s role as the only large Western country that had signed a memorandum of understanding on China’s Belt and Road initiative had enabled the Chinese help to arrive quickly (Pompili 2020). Italy’s decision to sign the memorandum of understanding in March 2019 had received negative backlash from both the EU and the U.S. (Ghiretti 2021; Yang and Gattolin 2023). As the Chinese aid planes arrived on March 13, Di Maio described the event as “what we call solidarity” in a live transmission on Facebook (Jakhnagiev 2020). As Chen (2021) has demonstrated, Chinese aid was not viewed negatively by any of Italy’s seven largest newspapers by circulation, regardless of their ideological alignment, in March–April 2020 (Chen 2021). On April 7, 2020, 36% of Italians polled believed that Italy should look more to China to develop its alliances outside Europe. Only 30% supported maintaining Italy’s traditional, post-WWII geopolitical stance (Palo 2020).

On the other hand, prominent Italian politicians who had started their careers during the Cold War downplayed or even attacked the Chinese aid shipments. Senator and former speaker of the Italian lower parliamentary chamber from 2001 to 2006, Pier Ferdinando Casini, commented on April 7, 2020, how the April 2020 survey, which showed more Italians favoring a geopolitical alliance with China than with the U.S., demonstrated “that the level of geopolitical awareness in Italy is very low. ... Even in a completely transformed world, believing that our new strategic partners are China and Russia means being very superficial” (Palo 2020). Maurizio Gasparri, a senator and the Italian minister of communications between 2001 and 2005, accused the then Italian foreign minister, Luigi di Maio, of being an “incapable, incompetent and inadequate person,” for only such a person could praise “a country [China] that represents the biggest problem on the planet from the point of view of unfair competition, pollution, denial of freedoms and the spread of epidemics” (Bracalini 2020).

Russian aid received an even less hospitable reception from Italian media and politicians than that offered by China: La Stampa, the fourth-largest Italian newspaper by circulation at the time, with a socially liberal outlook, quoted a nameless Italian political source who claimed that “80 percent of [Russian] supplies ... [were] useless, just a pretext [for spying by the Russian military]” on March 24 (Jacoboni 2020). On the same day, the head of Più Europa (a European federalist political party and an outgrowth of the Cold War-era Radical Party), Simona Viola, called the Russian military-medical mission an “act of political subordination of Italy by Russia.” The party Italian Radicals (Radicali Italiani; it shares its outlook and historical legacy with Più Europa) was similarly critical, asking if Russia’s “gifted horse” was not a “Trojan horse” in actuality (Dalla Russia con amore 2020).

6.6 Geopolitical Implications of Third-Country Involvement

6.6.1 Italy's Geopolitical Alignment

Even in early 2020, prominent Italian politicians who had started their careers during the Cold War dismissed the then-popular idea of Italy fundamentally changing its geopolitical position. Senator and former speaker of the Italian lower parliamentary chamber from 2001 to 2006, Pier Ferdinando Casini, commented on April 7, 2020, how Italy showed “such a strong interconnection in the economic system and in values,” with the U.S., that “thinking ... a historic pillar like the U.S. can be replaced overnight is completely wrong. I believe that the concept of “the west” is in crisis and that the relationship with the U.S. needs to be re-built but that is where we need to start. Considering all this, there is no doubt that China and Russia have a consolidated relationship with Italy that needs to be strengthened. But friendship or collaboration is one thing, and a strategic and geopolitical alliance is another” (Palo 2020).

Casini's view crystallized that of the Italian political and media establishment. In the months and years following the pandemic, several articles critical of Chinese and Russian aid (mostly accusing China and Russia of ulterior motives) appeared in the largest Italian newspapers by circulation (Cassati and Muglia 2020; Sarzanini 2022). In the first Italian national elections since the pandemic in 2022, both the League and the Five Star Movement lost seats in Italy's lower chamber of parliament (59 and 58, respectively). Brothers of Italy (Fratelli d'Italia)—an outgrowth of the Cold War-era neo-fascist and strongly anti-communist Italian Social Movement (Movimento Sociale Italiano) (Spotts and Wieser 1986; Ciucci 2022), which continues its predecessor's Atlanticist (pro-NATO, pro-American-troops-in-Italy) course (Vitale 2022)—went on to become the largest party in the Italian lower house (with 26% of the vote) and form the new government, which is in place until this day. While the current government includes the League and Berlusconi's Forza Italia as minor partners, it has taken a clearly anti-Russian and pro-NATO stance in foreign policy, as well as renounced the 2019 memorandum of understanding with China (Il senso del viaggio di Giorgia Meloni in Cina 2024; L'atlantismo di Giorgia Meloni è un fatto piuttosto recente 2022).

6.6.2 Impact on EU Unity

The initial reluctance—or inability—of key EU members to supply medical equipment to Italy in early 2020 shook many Italians' faith in European solidarity, amplifying Eurosceptic narratives. Italian media outlets repeatedly highlighted how countries like Germany and France imposed export restrictions on protective gear instead of coming to Italy's aid (Boffey 2020). Meanwhile, the swift arrival of medical equipment from China and Russia contrasted with the slow decision-making process within the EU, contributing to

the perception that the Union was either unwilling or unable to act in a crisis (Chazan et al. 2020).

However, later EU actions—such as the redirection of the EU’s cohesion policy funds to help member states strengthen their health systems and preserve jobs in March 2020 (Inforegio—Cohesion Policy Action against Coronavirus 2020); a temporary framework for state aid to allow governments to provide liquidity to businesses facing economic hardship due to COVID-19 in March 2020 (Temporary Framework—European Commission 2020); a temporary instrument to help member states cover the costs of national short-time work schemes designed to protect employees in April 2020 (SURE—European Commission 2023); and ultimately the creation of the “Next Generation EU” recovery plan in May 2020 (Recovery Plan for Europe—European Commission 2020)—helped repair some of the damage to the EU’s image in Italy. Eurosceptic feeling in Italy had cooled to such an extent by 2022 that the Brothers of Italy party—which had formerly supported the idea of Italy withdrawing from the Eurozone—abandoned the idea in the run-up to the elections (De Romanis 2022).

6.7 Critical Analysis of Disaster Diplomacy

“Disaster diplomacy” posits that crises can serve as catalysts for improved international cooperation or, conversely, highlight and exacerbate existing geopolitical divides. Italy’s COVID-19 experience quickly became a stage for outside actors to project influence through high-profile aid shipments. China’s and Russia’s interventions were not simply humanitarian gestures but strategic moves to showcase their global stature and cultivate goodwill—especially at a moment when Italy’s traditional partners seemed slow to help.

However, short-term perceptions and longer-term policy choices often diverge. In the immediate phase of the crisis (March–April 2020), visible, fast aid deliveries from China and Russia generated positive public sentiment and a fleeting sense among some Italians that the country might “pivot” geopolitically. The large-scale medical missions, replete with media coverage of planes touching down with supplies and specialized teams, underscored a level of responsiveness that the EU initially struggled to match. This was particularly salient in the face of Italy’s acute shortages in personal protective equipment and ventilators.

Over time, however, Italy’s deep-rooted alignments reasserted themselves. Establishment figures were quick to caution against drawing sweeping conclusions from the early pandemic period. Senator Pier Ferdinando Casini and others stressed the economic interconnection and shared values between Italy and the U.S., making a complete shift away from the Euro-Atlantic sphere unlikely. Moreover, the eventual ramp-up of EU assistance—ranging from the Temporary Framework for state aid to the landmark “Next Generation EU” funds—helped counter the narrative that Brussels was indifferent to

Italy's plight. This more robust European response, combined with concerns over Chinese and Russian motives, tempered any serious talk of a fundamental realignment.

In geopolitical terms, therefore, third-country aid to Italy functioned as both a life-line and a leverage point. It momentarily shook Italy's confidence in the EU but did not fundamentally alter Rome's longstanding alliances. The 2022 elections reaffirmed this continuity, as parties with Cold War-era roots—or those staunchly committed to NATO—consolidated power, while the initially enthusiastic, populist forces that had courted closer ties with China and Russia lost ground. Indeed, after the immediate emergency waned, skepticism toward the motives behind “gifted” aid resurfaced, with major newspapers critiquing both Beijing and Moscow. Overall, Italy's case illustrates how “disaster diplomacy” often achieves more symbolic wins than structural shifts in foreign policy—especially when the country receiving aid has established alliances, institutional ties and political legacies that guide its strategic direction.

6.8 Lessons Learned and Recommendations

6.8.1 Lessons

Timely and Visible Responses Matter: Major crises often amplify how quickly and visibly aid is delivered. In Italy's early COVID-19 experience, immediate and large-scale shipments from non-EU countries gained outsized public attention, temporarily reshaping perceptions of allied support. This underscores the high stakes of speed and symbolism in disaster relief: states or institutions that fail to act swiftly risk ceding both humanitarian and diplomatic ground.

Domestic and External Pressures Intersect: Global emergencies invite domestic political scrutiny over how international aid is procured and allocated. In Italy, public frustration with delayed EU assistance contrasted sharply with gratitude for prompt outside aid, complicating the foreign ministry's balancing act. This suggests that effective geopolitical risk assessment must account for domestic sentiment as much as external relationships, ensuring that internal and external priorities align.

Coordinated Mechanisms are Key: Fragmented responses—from the EU and individual member states—initially eroded trust in established alliances. Italy's requests for medical equipment went unanswered at first, prompting a spike in Eurosceptic narratives. This dynamic highlights the broader lesson that robust, pre-established crisis management structures can mitigate negative perceptions and prevent opportunistic external actors from filling aid gaps.

6.8.2 Recommendations

Enhance EU-level Crisis Coordination: Strengthening joint frameworks for emergency stockpiling and rapid response is critical for maintaining unity and credibility. If Italy, or any other EU member, perceives inertia from Brussels, it may again pivot—or at least appear to pivot—toward non-EU partners. A more cohesive EU crisis mechanism would streamline access to shared medical resources, preventing the early-stage inconsistencies seen in 2020.

Diversify Supply Chains: Limiting reliance on a single provider for critical equipment can reduce vulnerability to geopolitical pressures. In Italy's case, heavy dependence on external suppliers for masks and ventilators allowed countries like China and Russia to project influence. Going forward, more diverse sourcing—combined with internal EU production capacity—would bolster strategic autonomy and reduce potential leverage by outside actors.

Develop Clear Communication Strategies: Transparent information about aid procurement and distribution can shape domestic and international narratives. In the spring of 2020, sporadic messaging left many Italians concluding that outside help was more effective than European solidarity. By crafting unified communication plans, policymakers can pre-empt confusion, safeguard public trust, and minimize any geopolitical fallout arising from perceptions of inaction or disorganization.

6.9 Conclusion

6.9.1 Summary of Findings

The analysis presented throughout this chapter shows that Italy's severe health emergency during the early months of COVID-19 rapidly became a stage for foreign aid interventions, most notably from China and Russia. In immediate terms, these high-profile aid deliveries filled a critical gap in protective equipment, ventilators, and medical personnel. Italian public perception briefly tilted in favor of non-EU actors whose swift assistance stood in contrast to the initial inertia of Europe's Civil Protection Mechanism.

Yet, as demonstrated in previous sections, short-term impacts did not definitively alter Italy's longstanding geopolitical commitments. The political establishment's deep-rooted affiliations with the EU and the U.S.—as well as the eventual establishment of large-scale European support packages—ultimately reinforced Italy's traditional orientation. From this vantage point, the overall effectiveness of third-country interventions was partially overshadowed by the EU's more cohesive, longer-term recovery measures. The case thus underscores how initial, visible aid can influence public opinion, but longstanding alliances and economic interdependencies often drive a return to established geopolitical pathways.

6.9.2 Final Reflections

Italy's COVID-19 experience highlights a fundamental tension between urgent humanitarian responses and geopolitical maneuvering. Aid from China and Russia was undeniably effective in addressing immediate resource shortages, but it also served as a conduit for both countries to strengthen their soft-power foothold. Meanwhile, the EU's initially slow and fragmented crisis coordination exacerbated Italy's sense of vulnerability and fuelled skepticism about European solidarity.

Over time, however, more comprehensive European initiatives—ranging from shared stockpiles to financial recovery packages—helped restore faith in the EU's capacity to handle large-scale crises. This dual dynamic illustrates the complexities of disaster risk management: even when urgent humanitarian needs are at stake, major powers weigh strategic, reputational, and economic interests. For Italy, managing these competing pressures required careful navigation of its existing Euro-Atlantic commitments and an increasingly multipolar world order.

6.10 Perspectives

6.10.1 Outlook for International Cooperation in Health Emergencies

As with any highly publicized crisis, Italy's pandemic experience offers instructive lessons for future international health emergencies. First, rapid and visible assistance can shift public sentiment, at least temporarily, indicating the powerful influence of timely aid on political narratives. Second, the resurgence of Italy's traditional alliances and the bolstering of EU-wide support mechanisms reveal that longstanding institutional frameworks generally maintain their gravitational pull, even when new actors enter the scene.

Crucially, this interplay of immediate needs versus enduring alignments suggests that sustained coordination—rather than ad hoc or unilateral interventions—delivers the most robust and lasting solutions. In moving beyond a zero-sum approach, global and regional bodies alike must streamline crisis management protocols, diversify supply chains, and ensure transparent communication. By doing so, international cooperation in health emergencies can become a platform for meaningful multilateral engagement, rather than a mere bidding ground for geopolitical influence.

References

- Baldassarre R (2019) Via della Seta, il testo dell'intesa tra l'Italia e la Cina: La versione inglese e la traduzione in italiano. Corriere Della Sera. https://www.corriere.it/economia/19_marzo_12/via-seta-testo-dell-intesa-l-italia-cina-versione-inglese-traduzione-italiano-9ea09020-44c2-11e9-b3b0-2162e8762643.shtml

- Barnett M (2005) Humanitarianism transformed. *Perspect Polit* 3(04):723–740. <https://doi.org/10.1017/S1537592705050401>
- Barnett M, Weiss, TG (2011) *Humanitarianism contested: where angels fear to tread*. Routledge
- Boffey D (2020) Italy criticises EU for being slow to help over coronavirus epidemic. *The Guardian*. <https://www.theguardian.com/world/2020/mar/11/italy-criticises-eu-being-slow-help-coronavirus-epidemic>
- Bracalini P (2020) Di Maio, il ministro “cinese” che fa infuriare gli italiani. *ilGiornale.it*. <https://www.ilgiornale.it/news/politica/maio-ministro-cinese-che-fa-infuriare-italiani-1840090.html>
- Busto Arsizio, in ospedale mascherine con la stampante 3D (2020) *Il Giorno*. <https://www.ilgiorno.it/varese/cronaca/coronavirus-mascherine-3d-3d0c8bfb>
- Cassati D, Muglia A (2020) Coronavirus, i documenti segreti dell’Oms: «La Cina ha nascosto i dati». *Corriere Della Sera*. https://www.corriere.it/esteri/20_giugno_02/coronavirus-documenti-segreti-dell-oms-la-cina-ha-nascosto-dati-b2327048-a4c2-11ea-8ef6-a417ca68eeb2.shtml
- Chazan G, Johnson M, Fleming S (2020) Coronavirus: is Europe losing Italy? *Financial times*. <https://www.ft.com/content/f21cf708-759e-11ea-ad98-044200cb277f>
- Chen WA (2021) COVID-19 and China’s changing soft power in Italy. *Chin Polit Sci Rev* 8:440–460. <https://doi.org/10.1007/s41111-021-00184-3>
- China Sends Medical Supplies, Experts to Help Italy Battle Coronavirus (2020) *Reuters*. <https://www.reuters.com/article/world/china-sends-medical-supplies-experts-to-help-italy-battle-coronavirus-idUSKBN2101ZV/>
- Ciucci C (2022) Dall’Msi a Fratelli d’Italia, passando per An e la svolta di Fiuggi: Storia della fiamma tricolore nata con Almirante e arrivata fino a Meloni—*Il Fatto Quotidiano*. *Il Fatto Quotidiano*. <https://www.ilfattoquotidiano.it/2022/08/13/dallmsi-a-fratelli-ditalia-passando-per-an-e-la-svolta-di-fiuggi-storia-della-fiamma-tricolore-nata-con-almirante-e-arrivata-fino-a-meloni/6762009/>
- Coronavirus, la Germania strozza l’Italia sulle mascherine? Il caso dei «limiti alle esportazioni» (2020) *Il Messaggero*. https://www.ilmessaggero.it/italia/coronavirus_mascherine_germania_italia_esportazioni_3m_lettera-5108989.html
- Coronavirus, l’Italia supera la Cina: Primo Paese al mondo per numero di morti: 3.405. Impennata di guariti (2020) *La Stampa*. <https://www.lastampa.it/cronaca/2020/03/19/news/coronavirus-l-italia-supera-la-cina-primo-paese-al-mondo-per-numero-di-morti-3-405-impennata-di-guariti-1.38613038/>
- Cristiani D (2019) Italy joins the belt and road initiative: context, interests, and drivers. *China Brief* 19(8). <https://jamestown.org/program/italy-joins-the-belt-and-road-initiative-context-interests-and-drivers/>
- Cupelli C (2020) Canelli, la fabbrica dell’amaro Ramazzotti si mette a produrre l’igienizzante per le mani. *la Repubblica*. https://torino.repubblica.it/cronaca/2020/03/28/news/canelli_la_fabbrica_dell_amaro_ramazzotti_si_mette_a_producere_igienizzanti_per_le_mani-252550031/
- Dalla Russia con amore, in arrivo gli aiuti di Putin (2020) *la Repubblica*. https://www.repubblica.it/cronaca/2020/03/22/news/dalla_russia_con_amore_in_arrivo_gli_aiuti_di_putin-252006026/
- “Dalla Russia con amore”(2020) Nel team di medici destinato a Bergamo anche militari russi esperti in guerra batteriologica. https://www.tgcom24.mediaset.it/cronaca/dalla-russia-con-amore-nel-team-di-medici-destinato-a-bergamo-anche-militari-russi-esperti-in-guerra-batteriologica_16573710-202002a.shtml
- De Romanis V (2022) Le giravolte di Meloni sull’euro e il sogno impossibile di un’altra Ue. *La Stampa*. https://www.lastampa.it/politica/2022/07/27/news/le_giravolte_di_meloni_sulleuro_e_il_sogno_impossibile_di_unaltra_ue-5479947/

- De Stefani G (2020) La grande corsa alla riconversione: Chi creava vestiti ora fa mascherine. *La Stampa*. <https://www.lastampa.it/economia/2020/03/18/news/la-grande-corsa-alla-riconversione-chi-creava-vestiti-ora-fa-mascherine-1.38605102/>
- Drury AC, Olson RS, Van Belle DA (2005) The politics of humanitarian aid: U.S. foreign disaster assistance, 1964–1995. *J Politics* 67(2):454–473. <https://doi.org/10.1111/j.1468-2508.2005.00324.x>
- Easy Covid 19, la maschera da sub si trasforma in respiratore (2020) *Giornale di Brescia*. <https://www.giornaledibrescia.it/brescia-e-hinterland/easy-covid-19-la-maschera-da-sub-si-trasforma-in-respiratore-kef8poyy>
- Fortuna G (2019) ROME—parliamentary report casts a shadow over China’s 5G supply in Italy. *Euractiv*. https://www.euractiv.com/section/politics/short_news/rome-parliamentary-report-casts-a-shadow-over-chinas-5g-supply-in-italy/
- Ghiretti F (2021) The belt and road initiative in Italy: the ports of genoa and Trieste. *IAI Papers* 17:1–20
- Giacomino G, Scaparone S (2020) Coronavirus, la fabbrica dei cocktail ora fa i disinfettanti. *La Stampa*. <https://www.lastampa.it/topnews/edizioni-locali/torino/2020/03/27/news/coronavirus-la-fabbrica-dei-cocktail-ora-fa-i-disinfettanti-1.38644037/>
- Gilbert M (2024). *Italy reborn: from fascism to democracy*. Allen Lane, an imprint of Penguin Books
- Glossario (2020) Ministero del Lavoro e delle Politiche Sociali. <https://www.lavoro.gov.it/temi-e-priorita/immigrazione/focus-on/Cooperazione-internazionale/Documents/Glossario-04082020.pdf>
- Horowitz J (2020a) Message received: Italians are staying home. *The New York Times*. <https://www.nytimes.com/2020/03/10/world/europe/italy-coronavirus-movement-restrictions.html>
- Horowitz J (2020b) Italy’s Health care system groans under coronavirus—a warning to the world. *The New York Times*. <https://www.nytimes.com/2020/03/12/world/europe/12italy-coronavirus-health-care.html>
- Iacoboni J (2016) La propaganda russa all’offensiva anti-Renzi. E il web grillino rilancia. *La Stampa*. <https://www.lastampa.it/politica/2016/11/02/news/la-propaganda-russa-all-offensiva-anti-renzi-e-il-web-grillino-rilancia-1.34764558/>
- Iacoboni J (2020) Coronavirus, la telefonata Conte-Putin agita il governo: “Più che aiuti arrivano militari russi in Italia.” *La Stampa*. <https://www.lastampa.it/topnews/primo-piano/2020/03/25/news/coronavirus-la-telefonata-conte-putin-agita-il-governo-piu-che-aiuti-arrivano-militari-russi-in-italia-1.38633327/>
- Il senso del viaggio di Giorgia Meloni in Cina (2024) *Il Post*. <https://www.ilpost.it/2024/07/28/meloni-visita-cina-xi-jinping/>
- Inforegio—Cohesion policy action against coronavirus (2020). https://ec.europa.eu/regional_policy/funding/coronavirus-response_en
- Jakhnagiev A (2020) Di Maio: «Aiuti dalla Cina per fronteggiare il coronavirus, non siamo soli». *Il Messaggero*. https://www.ilmessaggero.it/video/politica/di_maio_coronavirus_aiuti_cina_13_marzo_2020-5108887.html
- L’atlantismo di Giorgia Meloni è un fatto piuttosto recente (2022) *Il Post*. <https://www.ilpost.it/2022/09/05/giorgia-meloni-atlantismo/>
- Le valvole per la rianimazione scarseggiano: Si stampano in 3D (2020) *Giornale di Brescia*. <https://www.giornaledibrescia.it/brescia-e-hinterland/le-valvole-per-la-rianimazione-scareggiano-si-stampano-in-3d-nd40ccxj>
- L’Istituto Poligrafico contro il Coronavirus: “Con la plastica delle carte di identità creiamo visiere sanitarie.” (2020) *la Repubblica*. https://www.repubblica.it/dossier/cronaca/italia-riparte/2020/04/26/video/listituto_poligrafico_contro_il_coronavirus_con_la_plastica_delle_carte_di_identita_creiamo_visiere_sanitarie-422724417/

- Mathieu E, Ritchie H, Rod  s-Guirao L et al (2020) COVID-19 pandemic. Our world in data. <https://ourworldindata.org/coronavirus>
- Bergamini N, Bucci A (2020) Coronavirus, l'azienda si converte: Dai tessuti per gli hotel alle mascherine distribuite gratis. La Stampa. <https://www.lastampa.it/torino/2020/03/20/news/coronavirus-l-azienda-si-converte-dai-tessuti-per-gli-hotel-alle-mascherine-distribuite-gratis-1.38617334/>
- Palo F (2020) W la Cina! Il sondaggio Swg che non ti aspetti. Parla Pier Ferdinando Casini. Formiche.net. <https://formiche.net/2020/04/cina-usa-sondaggio-swg-casini-ventura/>
- Patucchi M (2020) Dai body sportivi alle mascherine la fabbrica che reagisce all'emergenza. la Repubblica. https://www.repubblica.it/cronaca/2020/03/23/news/dai_body_sportivi_alle_mascherine_la_fabbrica_che_reagisce_all_emergenza-301114272/
- Pelosi G (2020) Coronavirus, attese per oggi un milione di mascherine. Il Sole 24 ORE. <https://www.ilsole24ore.com/art/coronavirus-attese-oggi-milione-mascherine-ADTgUWC>
- Pietrobelli G (2020) Coronavirus, Grafica Veneta riconverte produzione: 1,5 milioni di mascherine al giorno "gratis alla popolazione." Il Fatto Quotidiano. <https://www.ilfattoquotidiano.it/2020/03/18/coronavirus-grafica-veneta-riconverte-produzione-4-milioni-di-mascherine-al-giorno-gratis-alla-popolazione/5740755/>
- Pompili G (2019) Chi Mise la Cina al governo. Il Foglio. <https://www.ilfoglio.it/esteri/2019/03/07/news/chi-mise-la-cina-al-governo-241742/>
- Pompili G (2020) Ma quali aiuti della Cina contro il virus,   tutta roba che compriamo. Il Foglio. <https://www.ilfoglio.it/cronache/2020/03/12/news/ma-quali-aiuti-della-cina-contro-il-virus-e-tutta-roba-che-compriamo-306324/>
- Recovery plan for Europe—European Commission (2020). https://commission.europa.eu/strategy-and-policy/recovery-plan-europe_en
- Sarzanini F (2022) Dietro le minacce della Russia all'Italia il ricatto sugli accordi siglati durante la pandemia di Covid. Corriere Della Sera. https://www.corriere.it/politica/22_marzo_20/minacce-russia-italia-ricatto-accordi-pandemia-covid-1a8dcf76-a844-11ec-9fb7-9b041ce9b963.shtml
- Siddi M (2012) Italy-Russia relations: energy, politics and other business. In: Zsuzsa L (ed) Eurasian challenges: partnerships with Russia and other issues of the post-soviet area. Hungarian Academy of Sciences, pp 73–92. https://www.researchgate.net/publication/303738148_Italy-Russia_relations_energy_politics_and_other_business
- skytg24 (2021) Istat, in Italia oltre 700mila morti nel 2020: Pesa la pandemia Covid. <https://tg24.sky.it/cronaca/2021/03/05/istat-morti-2020-italia>
- Spotts F, Wieser T (1986) Italy, a difficult democracy: a survey of Italian politics. Cambridge University Press
- Storia and Diplomazia: Rassegna dell'Archivio Storico del Ministero degli Affari Esteri (2013) Ministero degli Affari Esteri e della Cooperazione Internazionale
- SURE—European Commission (2023). https://economy-finance.ec.europa.eu/eu-financial-assistance/sure_en
- Temporary Framework—European Commission (2020). https://competition-policy.ec.europa.eu/state-aid/coronavirus/temporary-framework_en
- Vitale G (2022) FdI, Giorgia l'atlantista: Le metamorfosi di Meloni. la Repubblica. https://www.repubblica.it/politica/2022/03/26/news/giorgia_meloni_atlantista-342871365/
- Yang J, Gattolin A (2023) Italy's decision on China's belt and road initiative and beyond. POLITICO. <https://www.politico.eu/article/china-belt-and-road-italy-trade/>

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.





Resilience and Service Continuity for Vital Services Providers in Multimodal Crises

7

Jaanus Kaugerand , Taivo Kangilaski , and Raul Savimaa 

Abstract

This chapter focuses on ensuring service continuity of vital service providers in the case of multiple simultaneous crises. Traditional risk and crisis management approaches in general concentrate on a single event, its consequences and mitigation mechanisms. This chapter indicates that such an approach is not suitable in case of multiple critical events occurring at the same time, as often the same resources are planned and deployed for supporting for multiple potential threats. The integrated scenario-based approach for risk analysis and crisis management is described to handle multi-modal crises.

Keywords

Risk management • Crisis management • Vital services • Service continuity • Vital service providers

J. Kaugerand · T. Kangilaski · R. Savimaa (✉)

Laboratory for Proactive Technologies, Institute of Software Science, Tallinn University of Technology, Tallinn, Estonia
e-mail: raul@savimaa.eu

T. Kangilaski
Eesti Energia AS, Tallinn, Estonia

R. Savimaa
Research Centre of Internal Security Institute, Estonian Academy of Security Sciences, Tallinn, Estonia

7.1 Introduction

This chapter focuses on ensuring service continuity of vital service providers in the case of multiple simultaneous crises. Traditional risk and crisis management approaches focus on a single event at a time, its consequences and mitigation mechanisms. However, such an approach does not cover the cases of multiple critical events occurring at the same time, as often the same resources are planned and deployed for supporting service continuity in several critical points. For example, following the traditional crisis management analysis in an organization or company, electricity backup may be installed and available for critical points, usually for one or two at the same time, but not for all if multiple events occur at the same time.

Services are typically categorized as vital services (mandated by the state for societal functioning), business-critical services (essential for achieving strategic objectives), continuity-critical services (necessary for supporting vital or business-critical services), and non-critical services (services with minimal impact during disruptions).

Units managing vital or critical services must conduct continuity risk analyses, develop response plans, and maintain readiness. Plans typically include identifying critical functions, assessing vulnerabilities, defining minimum requirements, planning mitigation, assigning responsibilities, and testing the continuity system.

In the case of a vital service, the prioritization of critical threats is not always the option as any of such threats may still cause interruption of continuity of the vital service. It is important to understand the characteristics of multimodal crises and their influence on the resilience of organizations. Therefore, a scenario-based approach for risk analysis and management for organizations that provide vital services is introduced in the chapter in more detail.

Modern societies depend on the uninterrupted delivery of vital services such as energy, water, healthcare, and telecommunications. To ensure continuity of vital services, risk analysis and crisis mitigation plans are elaborated and established in service-providing organizations and enterprises. Those plans and risk and crisis management approaches usually concentrate on coping with a single event, its consequences and mitigation mechanisms.

However, the increased interconnections of different global processes and their influence on enterprises and organizations worldwide has brought to the situation where multiple, overlapping threats emerge simultaneously, compounding risks and straining response mechanisms for organizations. Processes of an organization and services that are provided by the organization, including vital services, are increasingly threatened by the complexity and unpredictability of such interconnected crises. Traditional risk and crisis management models, that focus on single-event scenarios, are often insufficient in these dynamic environments. As organizations seek to enhance their resilience, there is a growing need for IT supported, integrated, scenario-based approaches to crisis management that account for interconnected risks, temporal dynamics and cascading effects.

Traditional crisis management frameworks frequently fall short in addressing multimodal crises because they tend to focus on individual components of a crisis without accounting for broader systemic interactions. This fragmented approach often leads to resource conflicts, where the same assets are allocated to address multiple crises, thereby reducing overall resilience. Addressing multimodal crises necessitates a comprehensive perspective that understands and integrates the interdependencies between events and their cascading effects.

Multimodal crises that influence vital services may have simultaneous impacts in different potential points of failure and may have different implications, such as physical infrastructure, the cyber domain, and quality of service parameters. In such cases, conventional crisis response strategies that focus on a single point of failure each may fail to allocate resources effectively, as the same assets may be needed to address multiple threats at once. Decision-making frameworks must adapt to the fact that prioritizing one risk may leave other vulnerabilities exposed, potentially compromising service continuity.

Such crises may originate from natural disasters accidents or deliberated man-made actions. As the major contemporary societal risks currently implicate both safety and security, safety and security risks should be governed with an integrated approach (Hansen and Antonsen 2024, p. 2).

This chapter is structured according to the following: Risk management from the multimodal crisis perspective is analysed in the Sect. 7.2. Section 7.3 analyses the factors to consider when designing a crisis response system for an organization. A scenario-based risk and crisis management approach to handle multimodal crises is described in the fourth section, followed by the conclusions at the end of the chapter.

7.2 Risk Management of Multimodal Crises Perspective

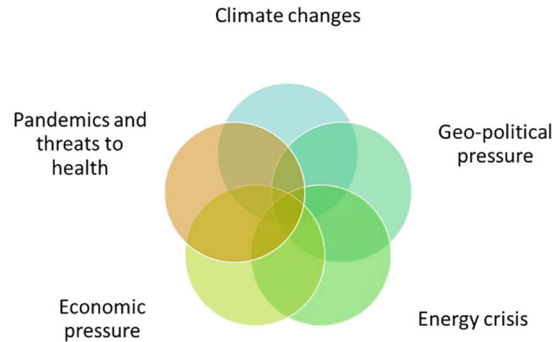
7.2.1 Systemic View of Multimodal Crises

A crisis, in scientific terms, is a complex and time-sensitive event characterized by a significant deviation from normal conditions, posing a threat to the stability, integrity or functionality of a system or organization (Bundy et al. 2017, p. 1662; Merriam-Webster 2024).

At their core, crises are characterized by heightened uncertainty, urgency, and the potential for adverse outcomes, necessitating prompt and decisive action to mitigate risks, manage consequences and restore stability (Lagadec 1993, p. 12; Moşteanu 2024, p. 445).

The threats that affect the continuity of providing the service by an organization can be divided into three groups: (1) natural disasters, (2) loss of performance due to long-term use of technical systems and (3) man-made actions. Examples of natural disasters are storms, heavy rain, flooding, forest wildfires, snowstorms and earthquakes. Due to the climate changes in the last decades, extreme weather conditions and natural disasters have

Fig. 7.1 Different threat domains in recent years for Europe



become more frequent. Yet the actual technical systems and built environments are not often modified to endure changes in heat, cold or flooding.

Loss of performance due to long-term use is more common in cases of economic pressure. In such situations the modifications are avoided until they are absolutely needed and therefore the number of cases of performance loss due to long-term use is increasing.

Besides human errors, man-made hostile actions vary depending on the purpose and means. In increasing age of digitalization, many man-made attacks and errors happen in the digital domain, but they have influence in the physical sphere.

Considering the external operating environment for an organization in Europe, various new events and increasing threats have come to the fore in last few years. Sources for those threats can be categorized into five main categories as indicated in Fig. 7.1: climate changes, pandemics and threats to health, geopolitical pressure, energy crisis and economic pressure.

Those threats may emerge simultaneously resulting in multiple potential critical events for the organization/company at the same time. Such threats may actuate multiple critical events that may be related with each other or independent from each other. As a result, a potential crisis or multiple crises may emerge that influence the organization/company multimodally.

Resulting from the previous, a multimodal crisis for an organization may be caused by a large single event or a set of multiple critical events. In both cases there is a cumulative effect to the organizational performance. Such a crisis that influences the organization/company multimodally can be defined as a multimodal crisis. In a multimodal crisis, the organization (its crisis response team or control room) must respond to multiple crises simultaneously and also share the resources to tackle with the event.

From a systems perspective, multimodal crises emerge simultaneously across processes and inter-process channels, disrupting organizational performance and service availability on multiple fronts. They are often triggered by a number of critical events occurring in quick succession, exert simultaneous pressures on different aspects of a system and producing a cumulative effect on organizational processes and outcomes, often resulting in greater damage than a single crisis scenario.

Hostile man-made attacks in the form of hybrid attacks often comprise direct attacks together with orchestrated indirect attacks to vital service providers and sometimes timed for the emergence of additional natural disasters (e.g. storms, flooding, etc.). Such multimodally emerging critical events put higher stress on the security systems of organizations and difficulty to continue providing the business continuity. Therefore, it is important that the risk and crisis management systems should be focussed also to handle multimodal crises and to tackle increased uncertainty.

Glette-Iversen and Flage (2024) point out five main lines of thinking concerning how unpredictable events can be delineated: unpredictability as the lack of ability to assign (meaningful) probabilities, unpredictability as the lack of ability to establish accurate models or cause-effect relationships, unpredictability as the lack of precursor signals and warnings, unpredictability as (irreducible) uncertainty, and unpredictability as lack of knowledge (Glette-Iversen and Flage 2024, pp. 2, 5). To reduce unpredictability, risk analysis for an organization should tackle to all those five types of unpredictability and develop relevant prevention strategies.

7.2.2 Risk and Crisis Management for Vital Service Providers

Risk and crisis management serve as vital frameworks for organizations to anticipate, mitigate and respond effectively to potential threats and disruptions. Central to these principles is the identification and assessment of risks across key domains, including financial, operational, reputational and strategic areas. Through systematic evaluation, organizations can prioritize risks based on their likelihood and potential impact, enabling the strategic allocation of resources and the development of proactive mitigation strategies. Cultivating a culture of risk awareness and transparency is equally crucial, fostering employee participation in risk identification and reporting to enhance organizational resilience.

Crisis preparedness involves a range of activities, including risk assessment, planning, training, simulation exercises and resource stockpiling. However, preparedness begins with a foundational awareness of risks within and around the organization. With this, organizations should overcome the gap on how to translate theoretical models of crisis management into real activity (Aven 2023, pp. 3–5), or how to use risk and vulnerability analyses in organizational learning for crisis prevention and preparedness (Eriksson 2023).

Organizations providing vital services, such as energy supply, water systems, healthcare and communication networks play a critical role in societal stability. The definition of vital services varies by country (e.g. Herrera and Maennel 2019; Mehvar et al. 2021; Santos et al. 2014.), reflecting differences in critical infrastructure durability, resource availability and external threats. The common characteristics are that these services are essential for maintaining societal functionality, and any interruption due to crises can have widespread consequences or even danger to life and health.

In case of threat to disruption of a vital service, rapid and decisive action is imperative to safeguard organizational continuity. Effective crisis management involves clear communication channels, swift decision-making protocols, and resource mobilization. Predefined crisis response plans tailored to specific scenarios streamline coordination efforts, ensuring cohesive and systemic responses. Partnerships with external stakeholders, including government agencies and community groups, strengthen collective capacity to manage crises collaboratively.

In addition, effective risk and crisis management require a commitment to continuous learning and adaptation. Post-crisis debriefings and comprehensive reviews provide opportunities for introspection, enabling organizations to identify gaps, refine strategies, and bolster preparedness for future contingencies. A dynamic and iterative approach fosters a resilient organizational culture capable of navigating uncertainty with agility and confidence.

There are different organizational and coverage levels of the crisis management. At the state, country, or national level, risk and crisis management entail sophisticated strategies and intergovernmental cooperation to address multifaceted challenges. Similar applies at municipality level where risk and crisis management are vital for ensuring the safety, security and resilience of local communities.

Crisis preparedness at enterprise, company and organizational level requires the main commitment from the respective organization. It is a critical function that ensures an entity's resilience and ability to respond effectively to emergencies. Organizations need to establish structured crisis management frameworks to mitigate risks, maintain operations, and safeguard stakeholders. This level of crisis management operates between broader national or local authority responses and the immediate on-site incident response, bridging strategic decision-making with operational execution to minimize the disruption of a critical service.

Key crisis management activities at the organizational level include risk assessment, systematic risk analysis, contingency planning, training and continuous improvement. Organizations bear the primary responsibility for developing and implementing crisis management policies tailored to their specific risks and operational environments. This includes ensuring compliance with legal and regulatory requirements, establishing crisis response teams and fostering a culture of preparedness. Transparency and accountability are essential in maintaining stakeholder trust and ensuring effective crisis resolution.

At the lowest operational level, crisis management at the site of an event entails a structured and dynamic approach aimed at mitigating immediate risks, ensuring the safety of personnel and facilitating the rapid restoration of normalcy. Crisis management teams at organizational/company level employ advanced technologies, such as real-time monitoring systems, geographical information systems (GIS), and remote sensing platforms, to enhance situational awareness assess the extent of damages, identify emerging hazards, mitigate the impact of events, optimize resource utilization, and expedite the recovery process.

7.3 Factors to Consider When Designing a Crisis Response System for an Organization

7.3.1 Integrated Management Systems for Organizations

The introduction of ISO-based management systems is always a strategic decision of the organization. Implementing an ISO-based management system can help improve the overall performance of the organization, as well as create a solid foundation for a sustainable development initiative.

To give a better focus to the functioning of the organization, many companies have brought their work organization into line with the requirements of the ISO 9001:2015 standard (Quality management systems - Requirements). ISO 9001:2015 promotes the adoption of process-oriented approaches in the development of the Quality Management System. Understanding and managing interrelated processes as a system contributes to the intended results of the effectiveness and efficiency of the organization. ISO 9001 implements the principles of continuous improvement, risk-based thinking which opens the possibility of dealing with both risks and opportunities. There are around 838,000 valid certificates of ISO 9001 for 1.25 million sites worldwide (ISO 2025).

There are two more standards that organizations also frequently implement. ISO 45001:2018 (Occupational health and safety management systems. Requirements with guidance for use) aims to create a framework for managing occupational safety and work environment risks and opportunities—which is expressed in the prevention of injuries and health damage to employees, ensuring safe and healthy workplaces. Therefore, it is extremely important for the organization to minimize hazards caused by occupational health and safety (OHS) risks through effective prevention and protection measures.

Since the company's activities inevitably affect the environment, it is frequently the case that, having implemented ISO 9001:2015, the activities of the organization are also applied to comply with ISO 14001:2015 (Environmental management systems, Requirements with guidance for use). ISO 14001:2015 seeks to strike a balance between society's expectations of sustainable development, organizational transparency and accountability, along with increasingly stringent legislation.

Having implemented more than one of these ISO standards, the management system of the organization can be called an integrated control system.

7.3.2 NIS 2 Directive

To ensure Europe's cybersecurity, the European Parliament adopted the NIS Directive on network and information systems in 2016 (Directive 2016/1148 of the European Parliament and the Council concerning measures for a high common level of security of network and information systems across the Union (the "NIS Directive")). When the

Directive entered into force, it was seen that its implementation by the Member States led to fluctuations in the content and quality of the requirements laid down.

In order to extend, harmonize and strengthen cybersecurity requirements, the NIS2 Directive, which is part of the EU's cybersecurity strategy, has now been adopted as of 2022 ((Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure a high common level of cybersecurity in the Union and amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing the Directive (EU) 2016/1148 (NIS 2 Directive)). While the NIS1 Directive categorized service providers as operators of essential services and digital service providers, the NIS2 Directive changed the classification of essential and important entities.

The NIS2 Directive aims to strengthen the cybersecurity of companies providing critical services. Continuity of services, cyber hygiene, access control, cryptography and secure authentication must be ensured. As an important change, the NIS2 Directive has introduced a move of cybersecurity issues beyond IT departments. This means that cybersecurity risk management measures must be approved at the level of the company's management—hence the requirement for board members to participate in industry-related training.

Thus, companies in EU Member States that are involved in providing vital services rights today have two options—either to certify themselves in accordance with the NIS2-based national legislation established on the part of the Member State, or to implement ISO 27001:2022 standard (Information security, cybersecurity and privacy protection. Information security management systems. Requirements) compliance. Companies operating in different markets predominantly choose ISO 27001 compliance because it reduces the complexity of the integrated management system.

Thus, in the coming years, the number of ISO 27001 certified companies in the EU will also increase significantly. For example, in Estonia, the established information security standard “E-ITS” (eits.ria.ee) is fully compliant with ISO 27001. The Estonian information security standard ensures comprehensive protection of business processes and information systems used to perform public tasks.

7.4 Scenario-Based Risk and Crisis Management for Multimodal Crises

7.4.1 Integrated Risk Management and the Need for Systemic Approaches

Risk management in an organization should correspond to the increasing likelihood of simultaneous and multimodal threats. The dynamic nature of risks should be considered (Glette-Iversen et al. 2023, p. 11) together with human factors in a socio-technical system that provides vital services (Nolan-McSweeney et al. 2023, pp. 10–13). ISO 31010:2010

presents 31 techniques for different contexts, thus the selection of methods depends on available expertise, resource constraints and organizational capacity. Low-ranked risks require monitoring but no immediate action, while moderate risks demand preventive measures to prevent escalation. High or very high risks necessitate recovery plans and prioritized mitigation, with strict timelines—within three to six months for significant risks, and immediate action for intolerable risks.

Bow tie diagrams are effective tools for visualizing threats, consequences, and controls. Preventive and mitigative actions, along with responsibilities and timelines, should be systematically documented. Biases in risk assessments, such as overconfidence or confirmation bias, must be addressed as well as cognitive pitfalls (Hunt and Naweed 2023, pp. 3–8).

For growing complexity of threats and potential multimodal appearance, the usual Excel-based methods should be extended with scenario-based risk modelling. Visualized scenarios help reveal interdependencies and cascading effects across organizational layers. ISO 31010:2018 provides relevant methods for scenario modelling, where risks at one level can trigger events at another. This chain-of-risk approach (Fig. 7.2) enables identification of critical risks and analysis gaps. The green circle indicates the event that starts the chain of multiple events possibly in different locations and channels.

Risks should be categorized by impact (e.g. financial, reputational, environmental) and type (e.g. compliance, security, third-party) to support cross-organizational generalization and prioritization. Risk categorization enables a consolidated overview, allowing senior management to focus on top risks across categories.

The interdependence between services and processes, service-based and cross-service risk analyses should be conducted. Scenario-based models provide early insight into

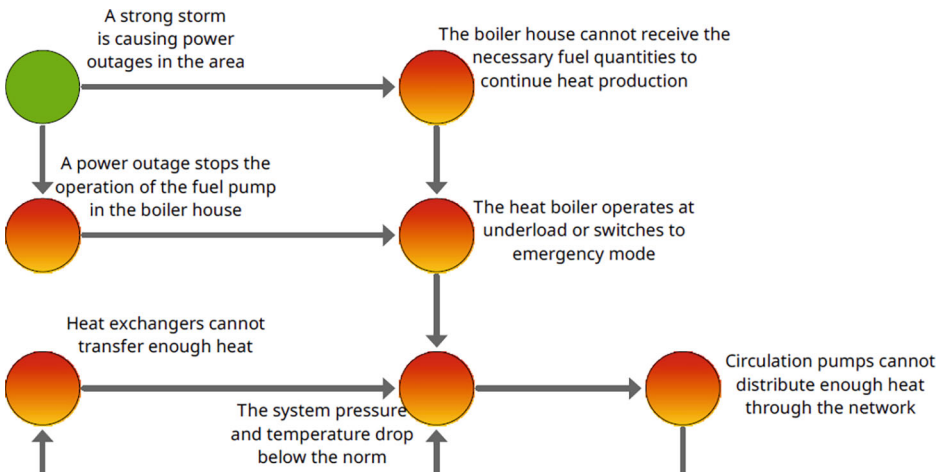


Fig. 7.2 The principle of risk chain formulation

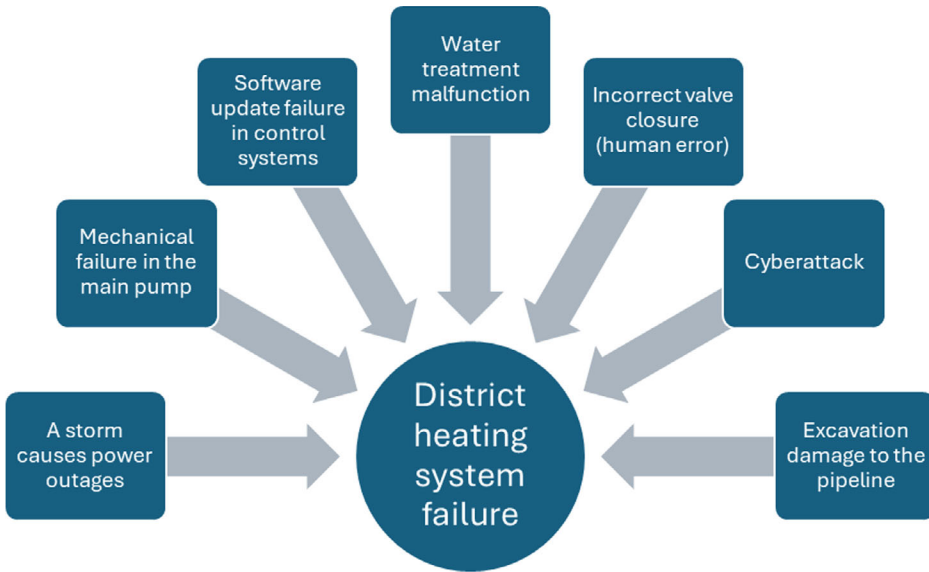


Fig. 7.3 Events that create cascading scenarios leading to failure of district heating system

risks arising from the interaction of causes and consequences. Risk assessment proceeds through scenario development, probability and impact evaluation, and bow-tie diagramming, with risk aggregation for upper management levels.

The actual risk picture is significantly more complex, consisting of a large number of risks and their interconnections as illustrated in Fig. 7.3. The overall integrated picture enables us to understand how a single event influences the outcome of providing services in an enterprise.

The scenario diagram depicted on Fig. 7.3 illustrates how multiple, interconnected failures, ranging from environmental conditions to technical and human errors, can cascade into a widespread multimodal crisis in a district heating network. This example demonstrates the importance of holistic crisis management and adaptive business continuity planning.

This diagram represents a failure cascade scenario in a district heating system. Several initial trigger events are visualized:

- A storm causes power outages,
- Mechanical failure in the main pump,
- Software update failure in control systems,
- Water treatment malfunction,
- Incorrect valve closure (human error),
- Cyberattack,

- Excavation damage to the pipeline.

Each initial trigger leads to progressive system degradation.

- Fuel supply interruptions → boiler underload → low pressure → reduced circulation → cooling of network → widespread heat disruption
- Sensor/control failure → over/under heating → pipeline or equipment damage
- Sediment build-up → clogging → pressure increases → leaks/failures
- Leaks → water loss → pressure drop → freezing → traffic accident → access disruption → delayed repair

The causal chains are interconnected, simulating a multimodal crisis scenario where one failure can interact with or amplify others. The overall picture supports understanding what are the critical chains that interrupt provision of critical services.

Based on the scenario-based approach it is possible to evaluate which chains and nodes should be strengthened to increase the resilience of a critical service.

7.4.2 Using a Scenario-Based Approach for Crisis Management

Unlike traditional crises triggered by singular events, multimodal crises arise from multiple concurrent events across domains, producing interdependent, cascading effects that intensify vulnerabilities. These crises challenge conventional crisis management due to their complexity and require integrated, adaptive responses.

Multimodal crises are defined by multidimensional impacts, often spanning geographical, sectoral, and organizational boundaries. For example, a natural disaster may coincide with a resource shortage, compounding disruptions. Such crises may result from interconnected or unrelated events, or from a single large-scale incident generating widespread effects. In all cases, the cumulative impact on organizational performance is significant.

Given this complexity, organizations must recognize how disruptions affect service delivery and implement robust business continuity strategies. Organizations should also prepare for crisis communication, which varies depending on the level of public interest. Crisis management must also integrate operational tools (continuity plans, communication protocols) with broader governance frameworks, balancing rules-based compliance with principles-based adaptability. This dual approach enhances organizational resilience under pressure.

An organization understands the critical paths to ensure resilience of a critical service. In case of the crisis event, scenario-based approach supports better situation awareness and understanding the extent of the crisis and potential recovery paths. There can be discussion whether a rule-based or principle-based approach is preferred to be more efficient in crisis management. However, both rules-based and principles-based approaches act as a duality,

to create an integrated whole, rather than as a dualism, where they are in opposition to each other (Pilbeam et al. 2025, p. 12).

The potential benefit of the scenario-based approach for crisis management and previous existence of scenario-based risk picture together with relations is more realistic mode-based situation awareness.

7.4.3 Implementation of the Integrated Approach

A core challenge in risk management is recognizing how interconnected events can trigger cascading effects. Seemingly minor issues may escalate into significant incidents, acting as catalysts for further disruptions. For instance, a supply chain delay may evolve into financial losses, reputational harm or regulatory consequences. Similarly, a small technical fault could cause broader system failures if not addressed promptly.

Focussing on event chains rather than isolated incidents reveals the dynamic nature of risk propagation. This perspective helps identify critical intervention points where early action can disrupt escalation pathways and prevent major crises.

Scenario-based risk analysis delivers actionable insights by evaluating both the likelihood and impact of potential events. This dual assessment enables categorization into small, medium, or large impacts, supporting prioritization and efficient resource allocation.

For example, a high-impact scenario like a cyberattack on critical infrastructure would involve detailed analysis of exploited vulnerabilities and potential systemic effects. In contrast, a minor disruption such as a short communication outage may require minimal intervention but should still be monitored.

Effective risk management hinges on distinguishing between risks of varying severity. Prioritizing high-impact scenarios ensures resources are directed where they matter most, avoiding diluted efforts. This prioritization also informs strategic planning by intervening early in high-risk event chains so minimizing both the likelihood and cost of adverse outcomes.

Proactive risk management emphasizes anticipation over reaction. Through comprehensive risk mapping and scenario analysis, organizations can identify and address threats before they materialize. These insights support broader initiatives such as business continuity and crisis planning. For example, anticipating supply chain risks might prompt supplier diversification and enhanced logistics visibility. Similarly, heightened cybersecurity concerns can drive investment in detection systems and employee training.

The introduced method represents a shift from traditional risk management towards a proactive, systems-based approach that enhances decision-making under uncertainty.

When implementing scenario-based risk and crisis management, there are a number of relevant aspects of modelling technologies that can be considered for analysis of inter-related, often simultaneous processes and in order to obtain a comprehensive situational

picture, as described by Hassel et al. (2022, p. 5), Colombo and Golzio (2016, pp. 48–55), Lorraine et al. (2025, p. 13), Tavana (2008), Chu et al. (2024), Qabaja et al. (2023), Cheminod et al. (2013), Phiri and Tembo (2022), Ingvarson and Hassel (2023, p. 11), Cedergren and Hassel (2022, pp. 1–5), Stefana and Paltrinieri (2021, p. 13) and Saghafian et al. (2025, p. 6).

7.5 Conclusions

Multimodal crises are quite common nowadays. The EU is seeking to strengthen the business environment of companies in its Member States in such a way as to increase the soundness of the functioning of companies providing essential services by putting in place its own measures. This article analysed the positive impact of the implementation of ISO standards in the implementation of the EU's efforts and showed how the organization of risk management and crisis management can be combined into a single logical whole through scenario-based analysis of risks.

The increasing prevalence of multimodal crises has highlighted the critical need for innovative approaches to risk and crisis management. These crises, characterized by their simultaneous and interconnected impacts across multiple domains, pose significant challenges to traditional management frameworks. As demonstrated throughout this article, conventional methods that address crises in isolation are insufficient in navigating the complexities of modern, overlapping threats.

The research emphasizes the role of a scenario-based risk management approach in addressing the unique challenges posed by multimodal crises. Grounded in systems thinking and supported by ISO-based management standards, this method enables organizations to anticipate and mitigate the cascading effects of simultaneous crises. By fostering a holistic understanding of interdependencies and resource demands, organizations can enhance their resilience and adaptability, ensuring the continuity of vital services even under extreme conditions.

References

- Aven T (2023) On the gap between theory and practice in defining and understanding risk. *Saf Sci* 168:106325. <https://doi.org/10.1016/j.ssci.2023.106325>
- Bundy J, Pfarrer MD, Short CE et al (2017) Crises and crisis management: integration, interpretation, and research development. *J Manage* 43(6):1661–1692. <https://doi.org/10.1177/0149206316680030>
- Cedergren A, Hassel H (2022) Using action design research for developing and implementing a method for risk assessment and continuity management. *Saf Sci* 151:105727. <https://doi.org/10.1016/j.ssci.2022.105727>

- Cheminod M, Bertolotti IC, Durante L, Valenzano A (2013) Modeling emergency response plans with coloured petri nets. In: Hämmerli B, Kalstad Svendsen N, Lopez J (eds) CRITIS 2012, LNCS7722, pp 106–117
- Chu L, Ding J, Xie Y (2024) Modeling and analysis of petri nets for multimodal transport “single contract” systems based on blockchain. ASCE-ASME J Risk Uncertain Eng Syst Part A: Civ Eng-Ing 10(1). <https://doi.org/10.1061/AJRUA6.RUENG-1094>
- Colombo S, Golzio L (2016) The Plant Simulator as viable means to prevent and manage risk through competencies management: experiment results. Saf Sci 84:46–56. <https://doi.org/10.1016/j.ssci.2015.11.021>
- Eriksson K (2023) Organisational learning without fire? Risk analyses as a basis for developing crisis management capabilities. Saf Sci 163:106144. <https://doi.org/10.1016/j.ssci.2023.106144>
- Glette-Iversen I, Flage R (2024) On unpredictable events in risk analysis. Saf Sci 180:106652. <https://doi.org/10.1016/j.ssci.2024.106652>
- Glette-Iversen I, Flage R, Aven T (2023) Extending and improving current frameworks for risk management and decision-making: a new approach for incorporating dynamic aspects of risk and uncertainty. Saf Sci 168:106317. <https://doi.org/10.1016/j.ssci.2023.106317>
- Hansen ST, Antonsen S (2024) Taking connectedness seriously. A research agenda for holistic safety and security risk governance. Saf Sci 173:106436. <https://doi.org/10.1016/j.ssci.2024.106436>
- Hassel H, Cedergren A, Tehler H (2022) Strategies for aggregating risk information in a societal safety context. Saf Sci 149:105691. <https://doi.org/10.1016/j.ssci.2022.105691>
- Herrera LC, Maennel O (2019) A comprehensive instrument for identifying critical information infrastructure services. Int J Crit Infrastruct Prot 25:50–61
- Hunt D, Naweed A (2023) The risk of risk assessments: investigating dangerous workshop biases through a socio-technical systems model. Saf Sci 157:105918. <https://doi.org/10.1016/j.ssci.2022.105918>
- Ingvarson J, Hassel H (2023) On the strength of arguments related to standardization in risk management regulations. Saf Sci 158:105998. <https://doi.org/10.1016/j.ssci.2022.105998>
- ISO (2025) The ISO survey. ISO. <https://www.iso.org/the-iso-survey.html>. Accessed 15 April 2025
- Lagadec P (1993) Preventing chaos in a crisis. In: Strategies for prevention, control and damage limitation. McGraw-Hill
- Lorraine I, Domgue KL, Paes D et al (2025) Video see-through augmented reality fire safety training: a comparison with virtual reality and video training. Saf Sci 184:106714. <https://doi.org/10.1016/j.ssci.2024.106714>
- Mehvar S, Wijnberg K, Borsje B et al (2021) Towards resilient vital infrastructure systems—challenges, opportunities, and future research agenda. Nat Hazards Earth Syst Sci 21(5):1383–1407
- Merriam-Webster (2024) Crisis. Merriam-Webster Online Dictionary. Merriam-Webster, Incorporated. <https://www.merriam-webster.com/dictionary/crisis>
- Moşteanu NR (2024) Adapting to the unpredictable: building resilience for business continuity in an ever-changing landscape. Eur J Theor Appl Sci 2(1):444–457. [https://doi.org/10.59324/ejtas.2024.2\(1\).37](https://doi.org/10.59324/ejtas.2024.2(1).37)
- Nolan-McSweeney M, Ryan B, Cobb S (2023) Interviews with rail industry leaders about systems thinking in the management of organisational change and risk management. Saf Sci 164:106168. <https://doi.org/10.1016/j.ssci.2023.106168>
- Phiri L, Tembo S (2022) Petri net-based (PN) cyber risk assessment and modeling for zambian smart grid (SG) ICS and SCADA systems. Comput Sci Eng 12(1):1–14. <https://doi.org/10.5923/j.computer.20221201.01>
- Pilbeam C, Denyer D, Sutliff M (2025) Guided by principles or rules: a Delphi study on how safety professionals frame safety practices. Saf Sci 184:106772. <https://doi.org/10.1016/j.ssci.2024.106772>

- Qabaja H, Ashqer MI, Bikdash M et al (2023) A meso-scale petri net model to simulate a massive evacuation along the highway system. *Futur Transp* 3:311–328. <https://doi.org/10.3390/futuretransp3010019>
- Saghafian M, Vatn DMK, Thordarson Moltubakk S, Bertheussen LE et al (2025) Understanding automation transparency and its adaptive design implications in safety-critical systems. *Saf Sci* 184:106730. <https://doi.org/10.1016/j.ssci.2024.106730>
- Santos JR, Herrera LC, Yu KDS et al (2014) State of the art in risk analysis of workforce criticality influencing disaster preparedness for interdependent systems. *Risk Anal* 34(6):1056–1068
- Stefana E, Paltrinieri N (2021) ProMetaUS: a proactive meta-learning uncertainty-based framework to select models for dynamic risk management. *Saf Sci* 138:105238. <https://doi.org/10.1016/j.ssci.2021.105238>
- Tavana M (2008) Dynamic process modelling using petri nets with applications to nuclear power plant emergency management. *Int J Simul Process Model* 4(2):130–138

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.





Disaster and Crisis Preparedness of Communities

8

Raul Savimaa 

Abstract

Polycrises are characterized by the simultaneous occurrence of multiple, interconnected crises of different natures, some of them short-term, some long-term. The changed global security environment, the COVID-19 pandemic, ongoing climate change and potential security threats have created conditions for long-term polycrises. They pose a significant challenge to the disaster and crisis preparedness of communities worldwide. As they may impact the continuity of several critical services, readiness of individuals and communities to cope with disasters and crises needs to be adjusted to cope with the current threats. Better resilience enables communities to effectively manage and recover from unexpected disruptions, thereby safeguarding lives, infrastructure, and the economy. This chapter examines how the communities and residents in Estonia are prepared for short- and long-term crises and for their potential cumulative influence regarding internal security and public safety. A set of surveys and case studies from the period 2023–2024 is presented and analysed in the paper. Estonia is taken as an example of a country on the Eastern border of the EU where the natural, health (COVID-19) and geo-political threats in last few years have been combined. This chapter identifies key factors that influence the preparedness and resilience of communities during polycrises. Based on the research results and the theoretical and background materials discussed in the paper, suggestions are made on policy development on how to increase crisis preparedness of the residents and the communities.

R. Savimaa (✉)

Research Centre of Internal Security Institute, Estonian Academy of Security Sciences, Tallinn, Estonia

e-mail: raul@savimaa.eu

Keywords

Community preparedness • Crisis preparedness • Civil protection • Community resilience • Civil defence

8.1 Introduction

A crisis, in scientific terms, is a complex and time-sensitive event marked by a significant deviation from normal conditions, threatening the stability, integrity, or functionality of a system or organization (Bundy et al. 2017, p. 1662; Merriam-Webster 2024). Crises manifest across various domains, including natural disasters, technological failures, socio-political unrest, economic downturns and public health emergencies. At their core, crises are characterized by heightened uncertainty, urgency and the potential for adverse outcomes, necessitating prompt and decisive action to mitigate risks, manage consequences and restore stability (Lagadec 1993, p. 12; Mostenau 2024, p. 445).

Historically, crisis preparedness has primarily focussed on local industrial or natural disasters. The changed global security environment, the COVID-19 pandemic, ongoing climate change, and potential security threats have created conditions for long-term polycrises. Preparedness for disruptions to critical services and emergencies is now essential for municipalities and residents alike. Communities and their respective NGOs play a vital role in improving resilience and managing crises effectively, as outlined in this paper.

However, in recent years, threats and potential crises emerge from several societal domains. Climate changes directly influence the everyday activities of people: in some European countries there are more intense heat waves, in others more storms or flooding or more volatile weather. Severe weather such as heavy storms may also cause interruptions of different services, including vital services like electricity or water supply. Absence of electricity in turn may cause interruptions of transportation services, availability of liquid fuel for motor vehicles as well as disruption of banking services and operation of grocery stores. There can be also other reasons, natural or man-made threats and events that may lead to crises in society or community. Such threats may emerge from different, apparently independent sources such as climate change, pandemics, geopolitical tensions or hybrid attacks, but still influence society and/or communities simultaneously and in a multi modal way (e.g. as described earlier, absence of electricity, transportation availabilities and lack of food). Such simultaneous occurrence of multiple, interconnected crises from different domains is defined here as polycrises.

Polycrises differ from singular events as they involve a complex interplay of systemic vulnerabilities, cascading effects, and interconnected risks, which amplify their collective impact. For example, a natural disaster such as a hurricane may trigger secondary crises like infrastructure failures, power outages and supply chain disruptions. These challenges can then be compounded by socio-economic or public health crises. Consequences continue much longer than the temporal span of the initial triggering event. Long-term consequences of a large natural disaster, pandemic or a hybrid attack can

be shortages of essential goods, economic instability and social unrest. Disruptions in one domain can precipitate cascading effects across interconnected systems. Furthermore, these crises often span geographical regions, sectors and organizational hierarchies, complicating response coordination and resource allocation. This “domino effect” underscores the need to address complex risk interactions and foster resilience through integrated crisis management approaches.

Polycrises are characterized by high uncertainty and unpredictability arising from multiple factors, feedback loops and emergent dynamics. Their simultaneous occurrence challenges communities and governments by exposing the limitations of traditional crisis management that focuses on isolated events. As conventional risk assessment and preparedness methods fall short, adaptive strategies are needed to address evolving risks. This shift calls for holistic approaches integrating cross-sectoral perspectives and fostering collaboration among diverse stakeholders. Key components include robust risk assessments, scenario planning and contingency measures to mitigate systemic vulnerabilities, enhance community resilience and ensure effective responses to interconnected crises.

The convergence of multiple crises demands a rethinking of how to manage security at local, national and international levels. Communities, governments, and NGOs must work collaboratively to build resilience and address systemic vulnerabilities. Recommendations include enhancing risk awareness and public education to prepare residents for complex crises, building local partnerships to foster coordinated response efforts, conducting regular risk assessments and scenario planning to adapt to evolving threats, and shifting from reactive crisis management to proactive preparedness strategies.

A core element of effective management of large-scale crises is community preparedness. The degree to which communities are involved in crisis response depends on the nature and scale of the event. Whether addressing natural disasters, socio-political unrest or technological disruptions, communities’ ability to prepare for, respond to and recover from crises is critical for maintaining societal stability and reducing the human, economic, and environmental toll of such events.

Prepared communities are better equipped to safeguard lives, infrastructure, and the economy. They can mobilize resources, implement emergency plans and coordinate response efforts swiftly, reducing the impact of crises. To enhance preparedness, communities and NGOs can conduct regular risk assessments, establish clear communication channels, promote public education on disaster awareness and response strategies, and build strong local networks and partnerships to ensure a coordinated and inclusive approach to crisis management.

This chapter examines the pivotal role of disaster and crisis preparedness in communities facing polycrises. It advocates for a multidisciplinary approach to crisis management, emphasizing the contributions of governance, communication, technology and community engagement. Decentralized governance and public–private partnerships are highlighted as key to effective resource mobilization and risk management. The study outlined underscores the importance of risk awareness, resource allocation, social cohesion and

collaborative response strategies, arguing that strong community-level preparedness is essential for managing complex crises.

The rest of the chapter is organized as follows. Section 8.2 reviews essence of crisis management levels from national level down to local level and explains the role of municipalities in the crisis management. The role of communities in crisis preparedness is reviewed in Sect. 8.3. Section 8.4 presents and analyses five case studies on crisis preparedness of communities in Estonia. The conclusions and recommendations are presented at the end of the chapter.

8.2 Crisis Management with Communities

Preparedness for crises and the mitigation of potential risks form the cornerstone of effective risk and crisis management. The overall process is essential for authorities, service providers and organizations to anticipate, mitigate and respond effectively to potential threats and disruptions while working towards the restoration of normal operations. Similarly, this is also important on a residential level, although not always handled by a systematic approach.

8.2.1 Levels of Crisis Management

Three temporal and logical stages in crisis management can be distinguished (Lettieri et al. 2009, p. 125): pre-crisis (the period before the disaster occurs), crisis (the actual occurrence of the event) and post-crisis (the period from the crisis subsiding to the return to normal conditions). The integrated process of crisis management consists of prevention, planning, response, recovery and learning (Coombs 1999; Pearson and Clair 1998).

Traditional crisis management systems predominantly rely on top-down planning approaches, implemented at national, regional, municipal and incident-specific levels. These systems emphasize immediate and professional responses to disasters, requiring detailed and structured plans at each administrative level. While this approach has proven effective in managing discrete crisis events such as natural disasters or industrial accidents, it often struggles to address the prolonged and multifaceted nature of certain crises, particularly those involving cascading or systemic impacts.

At the national level, risk and crisis management employ sophisticated strategies and intergovernmental cooperation to address complex challenges. Government agencies conduct comprehensive assessments across economic, environmental, political, and societal dimensions to guide strategic planning and policy development, aiming to prevent, mitigate, and respond to crises such as natural disasters, public health emergencies, terrorism and geopolitical conflicts (Björck et al. 2024). Coordinated response frameworks facilitate

information sharing, resource mobilization and decisive action, while transparent public communication fosters trust and community resilience.

At the municipal level, risk and crisis management are essential for ensuring local safety, security and resilience. Municipal governments identify and address risks (such as natural disasters, infrastructure failures, public health emergencies and social unrest) by collaborating with businesses, community organisations and emergency responders to leverage local expertise and resources.

Dedicated emergency management agencies are established to develop and implement crisis response plans, coordinate emergency operations, and disseminate critical information. These agencies also foster trust and resilience through proactive community engagement, enabling local authorities to better anticipate and manage crises.

The interplay between nationwide and municipal crisis management and organizational preparedness is symbiotic. While governmental and local authorities provide regulatory frameworks, infrastructure support and coordinated emergency response, businesses contribute by investing in local infrastructure, forming public–private partnerships and adhering to safety standards. This collaboration enhances information sharing, resource allocation and coordinated responses, with insights from corporate practices informing more adaptive governmental strategies for emerging threats.

At the event site, crisis management requires a structured yet adaptable approach. When an emergency occurs (be it a natural disaster, industrial accident, or other incident) multidisciplinary teams are swiftly mobilized to assess the situation, establish command centres, and activate response protocols. These teams include emergency responders, medical personnel, engineers and communication specialists.

However, there remains a gap between planned crisis management strategies and actual situational awareness, which limits support in scenarios where multiple crises occur concurrently.

8.2.2 Municipalities in Emergency Management

Crisis management, including emergency preparedness, response and the continuity of vital services, is governed by the Emergency Act (2017). This legislation outlines the responsibilities of state and municipal authorities in organizing crisis management and ensuring societal resilience. A business continuity strategy for vital service providers should be developed while local authorities are mandated to prepare a risk analysis of the local authority, considering the national risk analysis.

Organizations providing vital services play a pivotal role in societal stability. Vital services, ranging from energy and water supply to healthcare and communication networks, are essential for maintaining functionality during crises. A local authority organizes in its administrative territory the continuity of some vital services like district heating, ensuring the operability of local roads, and water supply and sewerage.

Subsection 2¹ of Section 6 of the Local Government Organisation Act (1993) stipulates, in relation to crises, that a local government shall contribute to the evacuation of persons and the accommodation, catering and medical care of evacuees. Pursuant to Subsection 1 of the same section, a local government shall organize the provision of social services, housing and communal services, water supply and sanitation, waste management and the construction and maintenance of rural municipality or city roads in its administrative area, unless these tasks have been assigned to someone else by law. Subsection 3 also stipulates that a local government shall also decide and organize those local life issues that have been assigned to it by other laws or that have not been assigned to someone else by law to decide and organize.

However, how is it determined how exactly a local government ensures crisis management capacity is managed by the authority itself? Predefined crisis response plans and partnerships with external stakeholders strengthen the collective capacity to manage crises collaboratively (Whitacre 2021). Although the implementation of uniform crisis management methods throughout the country is important, to improve the resilience of the local area, it is important that preparedness for dealing with crises is sufficiently provided at the level of local governments (Tej et al. 2014, p. 4). Therefore, crisis management practices and effectiveness may also vary (Hede 2018, p. 33).

When dealing with crises, local governments may encounter different situations within their administrative area (natural disasters, man-made disasters), but they may also be affected by disasters that occur elsewhere, but to which the local government population is involved (e.g. major natural disasters in other regions, etc.) (Hede 2018, pp. 5–7). Crisis exercises and constant maintenance of preparedness help local governments ensure resilience in, among other aspects, the following aspects: adaptability (ability to learn, acquire new solutions), adaptation and redundancy (ability to replace components if one of them fails), and better capacity for resource mobilization (Steen and Morsut 2019, pp. 4–5).

8.3 The Role of Communities in Crisis Preparedness

8.3.1 The Importance of Communities

There is no single definition for communities, it varies depending on context. Clark (2007, pp. 4–5) draws from multiple perspectives to suggest that the concept of community includes identity and belonging, inclusion and exclusion, as well as dimensions of place, time, and social interaction. Most often, communities are characterized by geographical and/or social belonging (Clark 2007, p. 5). Still, both residents and community associations often have differing understandings of what constitutes a community. Recognizing these differences is essential to fostering a shared understanding (Vihma and Lippus 2014, p. 8).

In traditional emergency management research, communities are typically viewed as groups of people living in the same area or near common risks (McAslan 2011, p. 6). However, this location-based definition overlooks other key dimensions, such as shared interests, values, activities, and social structures. Understanding community behaviour requires recognizing that communities are rarely uniform and that the roles and relationships among their members are complex. One community (e.g. residents of a specific region) may encompass multiple sub-communities, such as cultural associations, interest groups, or hobby clubs. Individuals often belong to several communities simultaneously, connected by factors such as location, occupation, economic status, gender, religion, or recreational interests (Turner 2010, p. 281).

Communities are also dynamic, forming around shared goals and disbanding once those goals are achieved (McAslan 2011, p. 6). Interest- and principle-based communities can significantly influence the functioning of location-based communities. For this reason, it is important to consider these dynamics when evaluating the performance of community associations, particularly in the context of crisis management.

One defining feature of a community is social capital—the informal norms that foster cooperation among individuals, citing honesty, commitment and trustworthiness as key examples (Fukuyama 2001, pp. 7–8). Social capital underpins community inclusion, or community participation, which ensures that all individuals, regardless of abilities, education, socioeconomic status or other factors are valued and respected members of the community (Fieldhouse and Donskoy 2013). In countries where local communities actively participate in local government and national decision-making, community participation has long been a key component of social capital (Roseland and Spiliotopoulou 2017).

There are a number of factors that determine community resilience (Patel et al. 2017, pp. 21–23): local knowledge, community networks and relationships, communication, healthcare, governance and management, resources, economic support, readiness and mental outlook.

Community participation involves people addressing issues that matter to them, shaping policies, and contributing to service planning, development and delivery (Adema et al. 2016). However, participation is ineffective if it only involves superficial consultation or fails to address the core concerns of the target group (Bishoge et al. 2019). In the context of crisis preparedness, members of community associations may be interested in contributing to preparedness efforts, even if these activities are not explicitly outlined in their association's general objectives.

Community associations embody the collective civic activity within a society. They unite neighbours or individuals with shared interests, enabling them to plan, organize and collaborate with local governments and provide a platform for citizens to voice opinions and collectively improve their quality of life (Sarbanes and Skullney 1995). A substantial body of research supports the benefits of a bottom-up approach, where active local community involvement helps achieve regional and national goals more effectively (Koontz

and Newig 2014; Meslin 2010; Russell 2015). However, combining bottom-up and top-down approaches creates a hybrid model in which both central and local factors contribute to effective policy implementation (Khan and Khandaker 2016) as top-down approaches alone are insufficient for sustainable development (Ulate et al. 2018).

In Estonia, community societies and NGOs largely depend on active, enterprising individuals with strong communication skills. The “anchor community” is defined by the presence of a central strong institution or facility, such as a school, library or company. These institutions often serve as focal points for the surrounding region, attracting residents and people with shared interests (Paas and Pegolainen-Saar 2022; Taylor and Luter 2013). The strategic documents also highlight the need to enhance crisis preparedness and post-crisis damage mitigation through the collaboration of state institutions, local governments and communities (Siseministeerium 2020, p. 32).

8.3.2 Community Associations as Supporters of Crisis Management

As a rule, the initial basis for the emergence of community associations has been the desire to promote cultural life, get along with each other or to solve an existing problem (Vihma and Lippus 2014, p. 24). Supporting residents’ crisis preparedness could be one (additional) area of community association activity, if it is a sufficiently important common problem for the residents of the region.

Community crisis preparedness has been studied from various different viewpoints: Martin et al. (2023) analyse the decision-making process and community involvement in improving the living environment. Cass et al. (2022) analyse community expectations to reduce regional flood risks, while Khan et al. (2022) and Chen et al. (2020) analyse crisis communication and community involvement during the COVID-19 pandemic, and Nahkur et al. (2022) analyse the involvement of volunteers in crisis management activities in Europe.

Still, no voluminous literature exists on the role of community associations in supporting residents’ crisis preparedness. The involvement of the community and community associations could be useful not only in an actual crisis, but also in emergency preparedness and response planning, including considering the consequences. The opinion of local communities is expected to be the basis for implementing better quality plans and policies based on local realities (DCAH 2021, p. 3). Linnell (2013) has described ways to involve communities in crisis management. Based on his observations, volunteers and communities are mainly involved not so much in crisis preparedness planning, but as supporters of crisis and natural disaster mitigation, e.g. as providers of shelter, distributors of food and essential goods, or as performers of essential recovery work Linnell (2013, pp. 22–23).

8.3.3 The Potential of Prepared Communities

Organized and prepared communities can contribute to the crisis preparedness of citizens and support local authorities in different stages of crisis management. Involvement of communities in risk reduction analysis enables them to exhibit and use their competence regarding local conditions, environment, potential vulnerabilities and early response to potential threats. For example, in areas prone to natural disasters such as floods, earthquakes, or wildfires, community members can provide valuable insights into high-risk zones, evacuation routes and early warning signs. This localized knowledge is vital for authorities when developing risk assessments and crisis management plans tailored to the specific needs of a community.

To enhance preparedness, communities or respective NGOs can conduct regular risk assessments, establish clear communication channels and engage in public education on disaster awareness and response strategies. Also, building strong local networks and partnerships ensures a more coordinated and inclusive approach to crisis management. Community-based organizations can support public security efforts by engaging in awareness campaigns, educational programmes, and training sessions focussed on risk prevention. By promoting hazard awareness and preparedness measures, communities can reduce their vulnerability to crises. For instance, in areas vulnerable to hurricanes, community-led workshops on disaster preparedness, covering topics such as emergency kit assembly, first aid, and evacuation procedures can save lives and reduce property damage when a disaster strikes.

Prepared communities can provide enhanced crisis response. The capacity of a community to mobilize quickly and efficiently can be critical to the overall effectiveness of response efforts. Public security agencies rely on community members to provide timely information about local conditions, which can help in making informed decisions about resource allocation, emergency response routes, and communication strategies. Community members often act as first responders, providing initial care and assistance to affected individuals before professional emergency services arrive.

Fostering strong communication channels between local authorities and community leaders can streamline crisis response operations. Trusted community figures, such as religious leaders, school administrators, or neighbourhood association heads, can act as intermediaries, facilitating the dissemination of accurate information and helping to quell panic. In this way, community networks can serve as force multipliers, extending the reach and effectiveness of official response efforts in the crucial early hours of a crisis.

Prepared communities and their organisations in a region enable effective management and recovery from unexpected disruptions, thereby safeguarding lives, infrastructure and the economy. Prepared communities can swiftly mobilize resources, implement emergency plans and coordinate response efforts, reducing the impact of crises.

Beyond immediate response, long-term resilience-building within communities is essential for public security and crisis management. Resilient communities are better

equipped to handle future crises, whether they be natural disasters, economic shocks, or public health emergencies. Resilience can be fostered through infrastructure improvements, social programmes, and continuous community education. Community-driven initiatives that focus on sustainability, such as strengthening local economies, investing in climate-resilient infrastructure, and supporting public health initiatives, all contribute to long-term stability. A resilient community is one that is not only prepared for crises but also able to recover quickly, reducing the long-term social and economic impacts of disasters.

8.4 Case Study on Crisis Preparedness of Communities

There has been increasing interest in understanding the potential preparedness of the population and communities and therefore in recent years there has also been several surveys conducted to analyse the preparedness of citizens and communities.

For the whole of Estonia, Kantar Emor conducted an index survey of the population's awareness of emergency preparedness in 2019, 2021 and 2023 (Kantar 2023) at the request of the Estonian Rescue Board. According to this, the proportion of those who have never thought that their family or home could be in a serious emergency in the two years preceding the survey has dropped from 46% in 2019 to 23% in 2023. The main likely emergencies in their area were an interruption of vital services for more than 48 h and exceptional weather conditions. 59% of respondents indicated that they had purchased supplies to cope with an emergency. The survey (Kantar 2023, p. 26) concluded that the potential resilience of houses from an emergency perspective and familiarization of residents with the emergency code of conduct has increased. The study also drew attention to the fact that the level of provision of homes with what is necessary for a crisis is still low and that information from the local government reaches only less than half of the residents, and the level of satisfaction with it is also low.

There have also been more detailed studies focussing on municipalities, community organisations or on residents of specific communities. Some of these are reviewed hereunder.

8.4.1 Readiness for Crisis Management in Municipalities

The tabletop exercise on crisis preparation of municipalities was conducted in 2023 to evaluate the crisis preparedness of all 79 Estonian local governments in the event of a nationwide power outage. Organized by the Estonian Rescue Board, the exercise involved 926 participants from municipal crisis teams and their collaboration partners, using the Board's virtual crisis training platform (Savimaa and Vernik 2023, p. 42). Observers from various institutions also participated.

The exercise simulated a winter power outage, initially planned for four hours, with scenarios escalating to a long-term outage. Exercise covered four stages: planning activities during a 24-h advance warning; managing the immediate effects of the outage; escalating to a prolonged outage; and conducting a post-exercise resource analysis.

This exercise demonstrated that local authorities possess a strong overall readiness for crisis situations. Municipalities were mostly prepared for short-term crisis management, with crisis teams convened and roles clearly defined. However, gaps in detailed advance planning were noted, suggesting that some responses were guided more by the exercise questions than pre-existing strategies. In terms of risk communication, authorities expressed competence in providing timely information during short outages. Yet, concerns emerged regarding the sustainability of proposed solutions for longer-term scenarios. For example, the use of physical messengers to deliver information in communication blackouts was often suggested but lacked sufficient resource planning. The study emphasized the importance of predefined information boards and schedules to ensure consistent updates.

During prolonged outages, municipalities demonstrated a capacity to adapt initial four-hour outage plans to 48-h scenarios. While this adaptability was a positive outcome, weaknesses were apparent in anticipating secondary challenges, such as heating outages in apartment buildings, food supply chain disruptions, and operational continuity of stores without functioning cash registers. Resource estimates for these challenges were insufficient.

Responses also highlighted concerns about post-crisis recovery, particularly the restoration of critical infrastructure, such as heating, water systems, and wastewater treatment, which could take weeks in some cases. Additionally, the dependency on individual leaders, such as mayors, for communication and coordination raised sustainability concerns in prolonged crises (unlikely for municipalities, for larger authorities, there are several spokespersons who can fulfil the communication tasks during long crises).

Despite these challenges, the municipalities demonstrated a strong capacity for critical analysis during the exercise. Many acknowledged their limitations and proposed actionable steps to address shortcomings.

Based on the findings, several proposals were developed to enhance municipal crisis preparedness (Savimaa and Vernik 2023, p. 62):

- Detailed continuity planning: municipalities should conduct thorough analyses of business continuity, including resource availability for prolonged power, communication, and heating outages, while addressing food and fuel supply issues.
- Community engagement: local governments could involve additional volunteers in delivering messages and gathering situational updates during crises.
- Scheduled information updates: it is suggested to establish fixed times and locations for disseminating updates, ensuring residents know where and when to access crucial information.

- Tailored public guidance: municipalities should adjust preparedness communication to reflect specific local vulnerabilities, ensuring that residents and communities understand how to respond effectively.
- Inter-municipal learning: municipalities should share insights from exercises like this to improve collective readiness across regions.

8.4.2 Crisis Preparedness Studies in Muuga and Harku

Crisis preparedness studies in Muuga and Harku communities were conducted in 2023 (Savimaa 2024a, p. 11) and 2024 (Savimaa 2024b, p. 11), respectively. The studies employed a mixed-methods research design, integrating quantitative survey analysis with qualitative case studies. The surveys aimed to quantify awareness levels, preparedness measures, risk perceptions, and community engagement in crisis management. To enhance the reliability and validity of the findings, the study employed triangulation by comparing survey results with qualitative insights. The combined methodological approach allows for a holistic understanding of community crisis preparedness, offering data-driven insights that inform policy recommendations for enhancing resilience at the local and national levels.

The study consisted of five sections (perception of threat, awareness of local problems and resources, preparation for crises, assessment of crisis capacity of a community association, and sociodemographic aspects). The Study of the Muuga community consisted of a total of 57 questions and sub-questions, while the study on Harku community consisted of 31 questions.

Muuga is located near industrial zones and the largest port in Estonia. The residents reported heightened awareness of industrial accidents and related risks. A majority had considered potential threats such as armed conflict, extended service outages and chemical leaks. 65% of respondents had prepared for a potential crisis, mainly focussing on essential services like water, power and healthcare. Two-thirds had emergency supplies, while 50% periodically checked their stockpiles. Only 7% had practiced emergency procedures at home. Communication was limited, with only 12% discussing preparedness with neighbours. Knowledge of local emergency plans was inconsistent. The study highlighted the need for enhanced local awareness campaigns, focussing on practical guidance rather than amplifying risk perception.

Harku is a suburban area with fewer industrial risks. The respondents exhibited different patterns of preparedness. Residents were more concerned about natural disasters, such as storms and extended power outages. Residents identified water supply, electricity, and healthcare as critical services. Many considered storms as the most likely crisis. Two-thirds of respondents had emergency supplies, and nearly all had first aid kits. However, less than half had stored adequate water supplies. Financial and storage limitations

hindered some residents' preparedness. Many respondents sought additional training and clearer communication from local authorities.

These findings correlate with public opinion surveys on internal security carried out in 2022 for the whole of Estonia. Respondents have crisis-preparedness supplies mainly in the form of first aid supplies, hygiene products, food and cash, while less than half of respondents have an independent heating device, a battery-powered radio and sufficient drinking water at home (Turu-uuringute 2022, pp. 47–49).

The surveys indicated three main differences between crisis preparedness of Muuga and Harku residents: risk context due to the geographical situation; difference in preparedness levels; and difference in community engagement. Muuga faces industrial and port-related risks, reflected in residents' focus on chemical leaks and accidents. Harku's concerns revolve around natural disasters due to its suburban and coastal setting. Awareness of industrial risks was higher in Muuga, whereas Harku residents prioritized weather-related crises.

Residents of Muuga demonstrated slightly higher engagement in emergency planning, such as evaluating resource accessibility and checking stockpile quality. Harku residents had better access to basic first aid supplies but lacked adequate water reserves. Respondents from Harku reported stronger interest in community training and workshops, while Muuga's findings revealed limited neighbour-to-neighbour communication on preparedness. Harku showed greater reliance on local government for crisis management, compared to Muuga's self-reliant approach.

There were detected also six similarities between the crisis preparedness of residents of Muuga and Harku:

- In both areas, electricity, water, and healthcare were deemed the most critical services during a crisis.
- Approximately two-thirds of residents in both regions had emergency supplies, emphasizing food and first aid kits.
- Common obstacles included financial limitations, lack of storage, and perceived low likelihood of crises.
- Both studies identified a gap in crisis communication channels and public awareness of local resources.
- Respondents in both areas expressed interest in improving community resilience through training and collaborative efforts.
- Both studies emphasized the need for clear, localized crisis response plans.

The results are similar in the survey by Paadik (2024) on residents' preparedness for long-term crises in Estonia, highlighting that around 80% of the respondents believe that they are more likely to recognize a long-term crisis. Still, the result also points to a certain uncertainty or lack of awareness regarding the primary signs of a crisis. The survey results also indicated that people feel least prepared for persistent terrorist threat, cyberattack,

CBRNE (Chemical, Biological, Radiological, Nuclear and/or Explosives) incident, foreign attack/war, and industrial accident/leak. The highest rated self-awareness is preparedness for a pandemic. This can be attributed to the recent COVID-19 pandemic, which has increased awareness and preparedness for such situations. (Paadik 2024, p. 63).

While a significant portion of respondents had considered crisis preparedness, their practical readiness varied widely, therefore the survey on long-term crises presented the following recommendations: expand community education, strengthen local collaboration, enhance resource accessibility, and improve crisis communication (Paadik 2024, p. 63). Similarly, in another survey conducted by Saar Poll OÜ in 2020, 23% of respondents strongly believed that, in addition to the police and rescue services, businesses and communities should participate in ensuring security, and additionally 58% of the respondents agreed with this (Saar Poll 2020, p. 26).

8.4.3 Crisis Readiness of Estonian Community Associations

Here are summarized two studies that assessed the crisis readiness of Estonian community associations, focussing on their awareness of local threats, available resources, and capacity for crisis management. The research aimed to determine the roles community associations play in preparing for crises, ensuring community resilience and fostering sustainability. Data in the first study was collected in 2023 via an online survey targeting all community associations in Estonia, excluding apartment associations due to differing operational objectives. A total of 395 invitations were distributed, yielding 104 responses from active associations (Savimaa and Kont 2023, p. 80). The second study in 2025, the sample consisted of representatives of Estonian regional community associations that have applied for support from the Civil Society Foundation for the development of civil protection capabilities and crisis preparedness (Jõgi 2025, p. 35). There responded 46 regional community associations out of 104 potential respondents.

The first survey revealed that community associations have a good understanding of their operational areas, particularly physical conditions like road networks (61% reported a thorough understanding). However, systematic awareness of potential hazards remains inconsistent, with many associations lacking structured threat mapping or risk analysis. Cooperation with external organizations was identified as another area for improvement; only half of the respondents reported working with the Rescue Board, and just a quarter collaborated on crisis preparedness initiatives.

Approximately 50% of respondents expressed readiness to assist their communities during crises, with many already contributing to daily safety measures and providing advisory support. Collaboration with local governments was deemed adequate, and associations frequently participated in resolving crisis events. Respondents shared numerous insights and experiences, including the need for greater local government initiatives, better leadership, and increased access to training on crisis planning.

The second study analysed knowledge of community associations about potential crises in their region. Most associations assessed their understanding of the crises as good. Community associations have received several information leaflets and appreciated also practical trainings. The knowledge of residents developed through training is one of the elements of community resilience (Jōgi 2025, p. 55).

Also, most community associations assessed their readiness for a crisis as at least satisfactory in terms of knowledge and skills, as well as supplies and services necessary for life. However, less than half of the societies have a gathering place with heating, electricity and a water supply, meaning that less than half of the societies can speak of the existence of a local resilience centre. Local crisis preparedness would benefit if there were more community societies with the possibility of a resilience centre. Still, most of the community associations studied can provide residents with such modest physical amenities as a warm space with electricity and water supply for some hours or days (Jōgi 2025, pp. 56–57).

The research results of the second survey also show that community associations need practical training and exercises, especially in first aid, general crisis preparedness, evacuation and sheltering, and cooperation with other organizations. Of the material resources, community associations need the most generators, rooms for storing and gathering supplies, fuel and drinking water supplies. Comparing the size of the community society's area of operation, it turned out that societies with a smaller area of operation consider their activities to be more active. Societies with a smaller area of operation are better aware of the vulnerable people living in the area. Community societies with a smaller area of operation rated their readiness for crisis situations higher in terms of knowledge and skills and higher in terms of supplies and services necessary for life. In addition, community societies with a smaller area of operation rated their contacts and cooperation with the local government as closer (Jōgi 2025, pp. 57–58).

As a result of both surveys, community associations can be advised to be active in communicating with municipalities. The survey results show that in several cases community associations have been the initiator and more active party in cooperation with local governments (Jōgi 2025, p. 58). Local governments could have a better understanding of the crisis preparedness of communities (Jōgi 2025, p. 58).

Based on the studies, there can be outlined six key suggestions for community associations (Savimaa and Kont 2023, pp. 102–103; Jōgi 2025, pp. 58–60):

1. Conduct systematic mapping of regional threats and risks.
2. Update business continuity plans annually.
3. Strengthen crisis communication strategies and diversify communication channels, especially online as this requires less effort to reach more people. Focus also on younger residents who it may be are not interested in participating in the physical events of the community association.
4. Practical crisis and first aid training would be necessary to increase resilience.

5. Foster community mental health to build resilience.
6. Enhance collaboration with local, national, and international organizations, including municipality, the Rescue Board, the Defence League, the Red Cross and the Women's Shelter.

For municipalities there can be outlined the following suggestions:

1. Increase cooperation with community associations on crisis preparedness.
2. Provide training on crisis planning and evaluate the quality of completed plans.
3. Establish and communicate the locations of emergency centres, if possible.

Community associations play a crucial role in local crisis management but face challenges such as limited systematic awareness and insufficient collaboration with external entities (Savimaa and Kont 2023, pp. 103–104). The proposals outlined aim to strengthen their capacity to support local governments and residents during crises, enhancing overall community resilience. By addressing these gaps, community associations can be better equipped to mitigate risks and respond effectively to emergencies.

8.5 Conclusions

The evolving nature of polycrises necessitates a fundamental shift in crisis management towards community-centred preparedness. This research underscores the critical role of local communities in responding to and recovering from such complex disruptions, emphasizing the importance of tailored, inclusive and collaborative strategies.

Findings from studies conducted in Estonia, particularly in Muuga and Harku, reveal shared vulnerabilities and opportunities for enhancing community resilience. Key themes include the necessity of localized training programmes, inclusive crisis education for vulnerable populations, and simulations to raise public awareness. Clear and consistent communication channels are also vital; these must combine digital tools with traditional media and updated routines to maintain trust and enable timely coordination during emergencies.

Resource accessibility emerged as a universal concern. Ensuring households have emergency supplies and backup utilities is crucial, particularly during prolonged crises such as power outages. In tandem, community hubs and local associations should facilitate resource distribution, disseminate information, and support coordination. Inter-municipal knowledge exchange, including sharing best practices from tabletop exercises, also proves benefits for regional capacity building.

Given the compounding nature of polycrises, community preparedness must adopt a systems-based approach. This includes comprehensive risk education, which enables residents to understand interconnected hazards, such as how economic shocks might

exacerbate social unrest or health crises. Contingency planning at the community level is essential, involving residents in the co-creation of evacuation protocols, resource allocation strategies, communication plans and the identification of vulnerable individuals.

Social cohesion is a recurring determinant of resilience. Strong community ties foster rapid mobilization, effective resource sharing and mutual support. Programmes that promote trust (such as volunteer initiatives, local festivals and inclusive neighbourhood engagement) are integral to building these bonds. Equally important is access to both physical and informational resources, supported by training in first aid, disaster response and digital literacy.

Technology plays an increasingly central role. Innovations such as AI-based early warning systems, satellite imagery for damage assessment, and mobile apps for coordination offer new means to improve preparedness and response. However, such systems must prioritize transparency and cybersecurity to ensure reliability and trust during crises.

To institutionalize these practices, six policy recommendations are advanced:

- Allocate sustainable funding for community-level preparedness.
- Empower local leadership through training and peer exchange.
- Foster social cohesion and ensure inclusivity, especially for marginalized groups.
- Integrate community insights into national crisis strategies.
- Cultivate public–private partnerships to mobilize resources and innovation.
- Invest in technology adoption and infrastructure to enhance cooperation between municipalities and community associations and within communities.

Ultimately, resilient communities serve as the foundation of effective national crisis responses. By equipping local populations with the knowledge, tools and support they need, governments can create adaptive, responsive systems capable of managing the increasing complexity of global threats. Community resilience is not merely supportive of public security; it is essential to it.

References

- Adema CL, Muluka KO, Oteki EB (2016) Community participation in corporate social responsibility projects: the case of Mumias Sugar Company, Kenya. *IOSR J Bus Manage* 18(8):70–86
- Bishoge OK, Zhang L, Mushi WG, Matomela N (2019) A literature survey of community participation in the natural gas sector in developing countries. *Int J Energy Sect Manage* 13(4):765–786
- Björck A, Bläse R, Bastida P (2024) Becoming crisis-ready: a systematic literature review on corporate crisis readiness and the process to achieving it. *J Contingencies Cris Manage* 32:e12614. <https://doi.org/10.1111/1468-5973.12614>. Accessed 12 March 2025
- Bundy J, Pfarrer MD, Short CE, Coombs WT (2017) Crises and crisis management: integration, interpretation, and research development. *J Manage* 43(6):1661–1692. <https://doi.org/10.1177/0149206316680030>. Accessed 12 March 2025

- Cass E, Shao W, Smiley K (2022) Comparing public expectations with local planning efforts to mitigate coastal hazards: a case study in the city of New Orleans, USA. *Int J Disaster Risk Reduct* 74:102940
- Chen Q, Min C, Zhang W, Wang G, Ma X, Evans R (2020) Unpacking the black box: how to promote citizen engagement through government social media during the COVID-19 crisis. *Comput Hum Behav* 110:106380
- Clark A (2007) Understanding community: a review of networks, ties and contacts. NCRM Working Paper Series 9/07. ESRC National Centre for Research Methods, University of Leeds
- Coombs WT (1999) Ongoing crisis communication: planning, managing and responding. Sage, Thousand Oaks, CA
- DCAF (2021) Restrictions on civil society organizations: strengthening accountability and SDG16 amid the pandemic. Webinar Report of the Stockholm Forum 2021. Geneva Centre for Security Sector Governance, Geneva
- Emergency Act RT I (2017). <https://www.riigiteataja.ee/en/eli/ee/511122019004/consolide/current>. Accessed 12 March 2025
- Fieldhouse J, Donskoy A-L (2013) Community participation and social inclusion in Bristol. *Ment Health Soc Incl* 17(3):156–164
- Fukuyama F (2001) Social capital, civil society and development. *Third World Q* 22(1):7–20
- Hede S (2018) Crisis management: psychological challenges for leaders, p 38. Doctoral Thesis, Karlstad University Studies (2018)
- Jõgi J (2025) Kogukonnaseltside kriisivalmidus ning tugi kogukonnaliikmetele. Crisis preparedness of community associations and support for community members. Master Thesis. Sisekaitseakadeemia, Tallinn
- Kantar E (2023) Elanikkonna hädaolukorrale valmisoleku alase teadlikkuse indeksuuring 2023. Population emergency preparedness awareness index survey 2023. Tallinn
- Khan AR, Khandaker S (2016) A critical insight into policy implementation and implementation performance. *Public Policy Adm* 15(4):538–548
- Khan S, Mishra J, Ahmed N, Onyige CD, Lin KE, Siew R, Lim BH (2022) Risk communication and community engagement during COVID-19. *Int J Disaster Risk Reduct* 74:102903
- Koontz TM, Newig J (2014) From planning to implementation: top-down and bottom-up approaches for collaborative watershed management. *Policy Stud J* 42(3):416–442
- Lagadec P (1993) Preventing chaos in a crisis. In: *Strategies for prevention, control and damage limitation*. McGraw-Hill
- Lettieri E, Masella C, Radaelli G (2009) Disaster management: findings from a systematic review. *Disaster Prev Manage* 1(2):117–136
- Linnell M (2013) Community approaches involving the public in crisis management: a literature review. Risk and Crisis Research Centre Working Paper Series
- Local Government Organisation Act RT I 1993, 37, 558. As of 01.07.2023. <https://www.riigiteataja.ee/en/eli/ee/501072023003/consolide/current>. Accessed 12 March 2025
- Martin A, Fischer A, McMorran R (2023) Who decides? The governance of rewilding in Scotland ‘between the cracks’: community participation, public engagement, and partnerships. *J Rural Stud* 98:80–91
- McAslan A (2011) Community resilience. understanding the concept and its application. Torrens Resilience Institute, Adelaide
- Merriam-Webster (2024) Crisis. Merriam-Webster Online Dictionary. Merriam-Webster, Incorporated. <https://www.merriam-webster.com/dictionary/crisis>. Accessed 12 March 2025
- Meslin EM (2010) The value of using top-down and bottom-up approaches for building trust and transparency in biobanking. *Public Health Genomics* 13(4):207–214

- Mosteanu NR (2024) Adapting to the unpredictable: building resilience for business continuity in an ever-changing landscape. *Eur J Theor Appl Sci* 2(1):444–457. [https://doi.org/10.59324/ejtas.2024.2\(1\).37](https://doi.org/10.59324/ejtas.2024.2(1).37)
- Nahkur O, Orru K, Hansson S, Jukarainen P, Myllylä M, Krüger M, Max M, Savadori L, Nævestad T-O, Frislid Meyer S, Schieffellers A, Olson A, Lovasz G, Rhinard M (2022) The engagement of informal volunteers in disaster management in Europe. *Int J Disaster Risk Reduct* 83:103413
- Paadik I (2024) Eesti elanike teadlikkus ning valmisolek siseturvalisuse valdkonda puudutavate pikaajaliste kriisidega toimetulekuks. Awareness and readiness of Estonian residents to cope with long-term crises related to internal security. Master Thesis. Sisekaitseakadeemia, Tallinn
- Paas E, Pegolainen-Saar K (2022) Kogukondade arengufaasid. Development phases of communities. Estonian Village Movement “Kodukant”, Tallinn
- Patel SS, Rogers MB, Amlôt R, Rubin GJ (2017) What do we mean by ‘Community Resilience’? A systematic literature review of how it is defined in the literature. *PLOS Currents Disasters*. King’s Collage London. <https://currents.plos.org/disasters/article/what-do-we-mean-by-community-resilience-asystematic-literature-review-of-how-it-is-defined-in-the-literature/>. Accessed 12 March 2025
- Pearson CM, Clair JA (1998) Reframing crisis management. *Acad Manage Rev* 23(1):59–76
- Roseland M, Spiliotopoulou M (2017) Sustainable community planning and development. In: *Encyclopedia of sustainable technologies*, pp 53–61
- Russell HA (2015) Neo synthesis approach to policy implementation of social programs: an alternative approach to policy implementation. *J Sociol Soc Work* 3(1):17–26
- Saar Poll OÜ (2020) Siseturvalisuse avaliku arvamuse uuring 2020. Homeland security public opinion survey 2020. Report. Tallinn
- Sarbanes M, Skullney K (1995) Taking communities seriously: should community associations have standing in Maryland. *Maryland J Contemp Leg Issues* 6(2):283–316
- Savimaa R (2024a) Muuga elanike kriisivalmidus. Uuringuraport. Crisis preparedness of the residents of Muuga. CESERE SelgeSiht OÜ, Tallinn. <https://doi.org/10.5281/zenodo.13341130>. Accessed 12 March 2025
- Savimaa R (2024b) Harku valla elanike kriisivalmidus. Uuringuraport. Crisis preparedness of the residents of Harku municipality. CESERE SelgeSiht OÜ, Tallinn. <https://doi.org/10.5281/zenodo.12742427>. Accessed 12 March 2025
- Savimaa R, Kont K-R (2023) Kogukonnaseltside roll ja võimekus kogukondade kerksuse tagamisel kriisides. The role and capacity of community associations in ensuring the resilience of communities in crises. *Turvalisuskompass*, vol 4. Sisekaitseakadeemia, Tallinn, lk 69–108.
- Savimaa, R., Vernik, J. (2023) Lauaõppus „79 särtsu“—peegel kohalike omavalitsuste kriisivalmiduse enesehindamiseks. Table exercise “79 vibrancy”—a mirror for self-assessment of the crisis preparedness of local governments. *Turvalisuskompass*, vol 4. Sisekaitseakadeemia, Tallinn, lk 35–67
- Siseministeerium (2020) Siseturvalisuse Arengukava 2020–2030. Internal security development plan 2020–2030. Siseministeerium, Tallinn
- Steen R, Morsut C (2019) Resilience in crisis management at the municipal level: the Synne storm in Norway. *Risk Hazards Cris Public Policy* 11(1):35–60
- Taylor LH Jr, Luter G (2013) Anchor institutions: an interpretive review essay. University at Buffalo, Anchor Institutions Task Force
- Tej J, Živčák P, Ali Taha V, Sirkova M (2014) Crisis awareness of the municipal district residents: implication for crisis management at the local government level. *Qual Innov Prosper* 18(2)
- Turner JH (2010) The micro basis of the meso and macro social realms. *Theor Princ Sociol* 2:271–301

- Turu-uuringute AS (2022) Siseturvalisuse avaliku arvamuse uuring 2022. Homeland security public opinion survey 2022. Tallinn
- Ulate K, Alcoverro T, Arthur R, Aburto-Oropeza O, Sánchez C, Huato-Soberanis L (2018) Conventional MPAs are not as effective as community co-managed areas in conserving top-down control in the Gulf of California. *Biol Cons* 228:100–109
- Vihma P, Lippus M (2014) Eesti kogukondade hetkeseis. Current status of Estonian communities. Research report. Linnalabor and Estonian Village Movement Kodukant, Tallinn
- Whitacre P (2021) Learning from rapid response, innovation, and adaptation to the COVID-19 crisis: proceedings of a workshop—in brief. National Academies of Sciences, Engineering, and Medicine, 2021. The National Academies Press, Washington, DC. <https://doi.org/10.17226/26131>. Accessed 12 March 2025

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

