



Governing Cross-Infrastructure Digital Resilience in European Ports: A Feasibility Study in the Port of Rotterdam

By:

Lorenzo Bettin

6132928

*Engineering and Policy Analysis
Technology, Policy and Management*



Graduation Committee:

Tamara Metze – Multi Actor Systems

Nazli Aydin – System Engineering

Bernd Kasperek – Organization and Governance



Abstract

Nowadays, modern infrastructure systems are becoming more connected, more advanced, more digital, and more exposed to disruption. Events such as climate change, extreme weather, cyberattacks, geopolitical instability, energy stress, supply-chain shocks, and technological dependence increasingly show how fragile essential systems can become when one failure moves across different sectors. European ports are located at the center of this fragility. More specifically, they are not only defined as maritime gateways, but as dense operational environments where sectors of logistics, energy, transport, water, ICT systems, industrial activity, cyber-security arrangements, and public crisis management all depend on each other. In such a setting, port resilience now becomes a cross-infrastructure governance problem.

This thesis therefore examines this problem through the case of the Port of Rotterdam. As Europe's largest seaport and a strategic node for trade, energy, industry, and hinterland logistics, Rotterdam provides a highly relevant case for studying how cross-infrastructure disruption management is organized in practice. This research asks how existing disruption-management practices, information flows, and governance arrangements in and around the Port of Rotterdam shape the feasibility and potential added value of a cross-infrastructure digital resilience platform.

The study uses the "European Union Infrastructure Digital Resilience Platform (EU-IDRP)" as a conceptual object of analysis. EU-IDRP is a researcher-developed, non-operational platform concept. It was conceived as a federated coordination platform through which infrastructure actors could retain control over their own systems while sharing selected disruption-relevant information for dependency mapping, scenario analysis, and human-in-the-loop decision support.

The research combines literature reviews with ten semi-structured expert interviews involving different actors from infrastructure operation, public crisis management, port innovation, cyber resilience, terminal operations, digital modelling, and interoperability. Through this qualitative approach, the thesis then explores how different actors understand cascading disruptions, how information is currently shared, what coordination gaps exist, and under which governance conditions a shared digital platform could be trusted, used, and embedded.

The research findings show that a cross-infrastructure digital resilience platform could be in principle valuable, but its feasibility is presented as conditional. That is, existing systems and coordination practices already support parts of disruption management, yet they mainly produce partial visibility leaving aside shared system-level awareness. The research also identifies a grey space between routine operational incidents and formal crisis escalation, where cross-infrastructure coordination may already be needed before a formal crisis structure is activated. In this study, interoperability is presented as a socio-technical issue involving shared meanings, routines, responsibilities, legal arrangements, and operational fit. Finally, as it emerged from the analysis, the most useful information for resilience is also often the one that is the most sensitive to share.

The thesis concludes that the added value of a platform like EU-IDRP would especially lie in governed shared situational awareness and cross-infrastructure sense-making. The findings suggest that such a platform would most plausibly operate as a federated, role-based, and institutionally embedded coordination layer. Its purpose should therefore be to support existing responsibilities, provide controlled visibility, reduce coordination burden, and help actors recognize potential cascading effects earlier. The study contributes to port-resilience and critical-infrastructure governance literature by shifting attention from interdependence as an actual problem to governed coordination as a condition for resilience.

To my family, for their infinite love and support.

To all my close friends, for the encouragements, strenght, drive and motivation.

To my supervisors, for the care, passion and contribution they brought.

To TU DELFT, for all the times, the amazing journey, and the valuable experiences.

To me, for all the hard work and growth.

Table of Contents

<i>Abstract</i>	2
<i>1. Introduction, Case Context and Platform Concept</i>	7
1.1 Critical infrastructure disruption in European ports.....	7
1.2 The Port of Rotterdam as a cross-infrastructure ecosystem	8
1.3 The EU-IDRP platform concept and its role in the study	10
1.4 Problem statement, Research aim and Research Question.....	10
1.5 Scope, boundaries and contribution of the study	12
1.6 Thesis structure.....	13
<i>2. Methodology</i>	14
2.1 Research approach: qualitative single-case study	14
2.2 Case selection: the Port of Rotterdam	14
2.3 Platform description: the EU-IDRP concept as methodological entry point	15
2.4 Literature review and source selection	16
2.5 Infrastructure and actor identification	18
2.6 Semi-structured expert interviews	20
2.7 Data analysis: inductive coding and thematic interpretation	23
2.8 AI Statement	25
2.9 Research quality & Ethics	26
<i>3. Literature Review and Conceptual Framework</i>	28
3.1 Introduction.....	28
3.2 Cross-infrastructure disruptions and port resilience.....	28
3.3 Digital resilience platforms and shared situational awareness.....	33
3.4 Data sharing, trust, ownership, and information governance.....	35
3.5 Interoperability as a socio-technical governance condition.....	36
3.6 Governance and coordination of cross-infrastructure disruption management.....	37
<i>4. Findings</i>	40
4.1 From literature to interview findings.....	40
4.2 Literature based case context	41
4.2.1 The Port of Rotterdam as a cross-infrastructure resilience setting.....	41
4.2.2 A distributed actor landscape shapes platform feasibility	42
4.2.3 Rotterdam's coordination and digital environment is already populated.....	43
4.2.4 NIS2 and CER create pressure but not a complete governance model.....	45
4.2.5 Implication for the interview findings	45
4.3 Introduction to the interview findings	46
4.3.1 The grey space between routine operational incidents and formal crisis escalation	47

4.3.2 Existing systems produce partial visibility, but not shared system-level awareness.....	48
4.3.3 Interoperability as socio-technical alignment, not only technical integration.....	51
4.3.4 The most valuable information to share is often also the most sensitive	53
4.4 Rotterdam-specific manifestations of cross-infrastructure disruption.....	55
5. <i>Discussion</i>	56
5.1 Introduction to the discussion	56
5.2 Synthesis of the findings: platform feasibility as a governance problem.....	57
5.3 Contribution to the literature: from interdependence to governed coordination	59
5.4 Answering the research questions.....	61
5.5 Governance and organizational considerations for platform adoption	65
5.6 Design and staged implementation considerations for the Port of Rotterdam	67
5.7 Methodological reflection, limitations and future research.....	68
6. <i>Conclusion</i>	71
<i>References</i>	74
<i>Appendix</i>	79
<i>Appendix 1. Inductive codebook</i>	79
<i>Appendix 2. Semi-structured interview protocol</i>	85
<i>Appendix 3. Common oral EU-IDRP introduction used before the platform-related questions</i>	89
<i>Appendix 4. Informed consent</i>	89
<i>Appendix 5. Interview question example</i>	91

Abbreviations and Full term or meaning

ADA	Adaptive Data Adaptor
AI	Artificial intelligence
API	Application programming interface
C40	C40 Cities Climate Leadership Group
CER	Critical Entities Resilience Directive, Directive (EU) 2022/2557
CIA	Confidentiality, integrity, and availability
CISE	Common Information Sharing Environment
COP	Common operational picture
DMP	Data Management Plan
ECT	Hutchison Ports ECT Rotterdam
eFTI	electronic Freight Transport Information
EMSWe	European Maritime Single Window environment
ENISA	European Union Agency for Cybersecurity
EU	European Union
EU-IDRP	European Union Infrastructure Digital Resilience Platform — researcher-developed, non-operational platform concept used in this thesis
FTE	Full-time equivalent
GDPR	General Data Protection Regulation
GRIP	<i>Gecoördineerde Regionale Incidentbestrijdingsprocedure</i> — Coordinated Regional Incident Response Procedure
HREC	Human Research Ethics Committee
ICT	Information and communication technology
IP	Internet Protocol
IT	Information technology
ITSM	Information technology service management
LCMS	<i>Landelijk Crisis Management Systeem</i> — National Crisis Management System
MOU	Memorandum of understanding
MOVICI	Modeling and Visualization of Critical Infrastructures
NIPV	<i>Nederlands Instituut Publieke Veiligheid</i> — Netherlands Institute for Public Safety
NIS2	NIS 2 Directive, Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union
NS	<i>Nederlandse Spoorwegen</i> — Dutch Railways
OECD	Organization for Economic Co-operation and Development
OT	Operational technology
PCS	Port Community System
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
RWS	Rijkswaterstaat
SCADA	Supervisory control and data acquisition
UNCTAD	United Nations Conference on Trade and Development

1. Introduction, Case Context and Platform Concept

This chapter introduces the research problem, the Port of Rotterdam as the empirical case, and the EU-IDRP concept used to examine platform feasibility. It first explains why disruption in European ports must be understood across interconnected infrastructures and organizations. It then situates the Port of Rotterdam case, defines the platform concept, and specifies the research problem, scope, and contribution of the study.

1.1 Critical infrastructure disruption in European ports

European ports are more than sites of maritime cargo handling. They are interfaces linking maritime transport with hinterland logistics, industrial production, energy flows, digital communication, and public crisis-management systems. Their strategic value therefore depends on infrastructures and organizations that extend beyond the geographical and administrative boundaries of the port. The same connectivity that enables port operations also creates vulnerability. Consequently, essential functions may be interrupted even when individual port assets remain physically intact, for example when electricity, ICT, transport access, water-related infrastructure, or coordinated information exchange is disrupted (Huck et al., 2021; Punt et al., 2023a, 2023b; Tsoulfas, 2026).

In this thesis, cross-infrastructure refers to dependencies and consequences that extend across these different infrastructure domains rather than remaining within one sector. Port continuity refers to the ability to maintain or rapidly restore essential functions such as cargo handling, terminal operations, hinterland access, energy-related flows, ICT-supported coordination, and crisis-response communication. Operational continuity is treated as one practical expression of port resilience, while resilience refers more broadly to the capacity to prepare for, absorb, respond to, and recover from disruption. This distinction shifts attention from protecting individual assets to sustaining the functioning of the port as an interdependent socio-technical system, whose performance depends on both technical infrastructures and organizational arrangements.

These dependencies have become more consequential within a risk environment shaped by extreme weather, flooding, energy-system stress, cyber incidents, geopolitical instability, and supply-chain shocks. Although these hazards differ in origin, they can produce cross-sector consequences because they act upon the same interconnected infrastructure and organizational systems. Their relevance therefore lies not only in the initial disruption they create, but also in the pathways through which their effects may spread across sectors, territories, and organizations.

Interdependence becomes a cross-infrastructure resilience problem when disruption in one domain alters the functioning of another. In this thesis, cascading disruption therefore refers to an initial disturbance in electricity, ICT, water-related infrastructure, transport, or another relevant domain that creates secondary operational consequences for other port functions or actors. These effects may propagate through service dependencies, digital connections, spatial proximity, and organizational or regulatory relationships (Little, 2002; Rinaldi et al., 2001). In a port setting, an energy or ICT disruption may consequently affect terminal operations, traffic management, industrial processes, logistics planning, and the communication required for coordinated response (Punt et al., 2023b; Tsoulfas, 2026).

Congestion or failure in hinterland transport corridors creates the same underlying problem by affecting cargo flows, supply-chain continuity, and the port's capacity to perform its strategic function. These examples show that

the central issue is not merely that infrastructures are connected, but that their cross-organizational consequences must be recognized, interpreted, and coordinated.

Digitalization intensifies this tension. In practice, automated terminal processes, sensor-based monitoring, data exchange, and digital logistics platforms can improve operational visibility and decision support, while also increasing dependence on ICT and introducing cyber, system-failure, and information-governance risks. Digital systems are therefore both part of the resilience problem and a possible part of the response (OECD, 2019; Punt et al., 2023b; Tsoulfas, 2026). For this thesis, the relevant question is not digitalization itself, but whether a shared digital tool could support cross-infrastructure disruption management when information, responsibilities, and operational decisions remain distributed across multiple public and private organizations.

Port continuity is produced collectively, but authority over the infrastructures that support it remains distributed. These systems are owned, operated, regulated, and monitored by different public and private organizations, each holding only part of the relevant information, responsibility, and decision authority. No single actor can therefore be assumed to possess a complete operational picture or a general mandate to direct all others. Cross-infrastructure resilience consequently becomes a multi-actor governance problem involving trust, role clarity, decision rights, information-sharing arrangements, and institutional fit, rather than a question of technical connectivity alone (Ansell & Gash, 2008; Huck et al., 2021; Provan & Kenis, 2008).

One possible response is a cross-infrastructure digital resilience platform intended to support shared situational awareness. The idea is to obtain a sufficiently common and role-relevant understanding of what is happening, how disruption in one domain may affect another, and what information different actors need for their own decisions. Its value cannot, however, be assumed. Assessing its feasibility requires examining how it would complement existing operational and crisis-management arrangements, how sensitive information would be protected, how access and ownership would be defined, and how the decision authority of participating organizations would be preserved.

The unresolved issue is therefore not simply whether such a platform can be technically built, but under which governance and organizational conditions it could be trusted, used, and institutionally embedded. The Port of Rotterdam provides the empirical setting through which this question is examined in the following sections.

1.2 The Port of Rotterdam as a cross-infrastructure ecosystem

In this study, the Port of Rotterdam represents the main area of analysis and is treated as a dense cross-infrastructure ecosystem and not exclusively as a maritime gateway. Its specific relevance for this study lies in the fact that the concept of port operational continuity mostly depends on the concentration and interaction between maritime transport, terminal operations, road and rail corridors, inland waterways, pipelines, energy systems, industrial production, ICT systems, cyber-security arrangements, water-related infrastructures, and public crisis-management structures. This concentration makes Rotterdam a particularly suitable and interesting setting for studying the governance and organizational feasibility of a cross-infrastructure digital resilience platform.

For the purposes of this study, the Port of Rotterdam is characterized not only as a transshipment location, but also as a strategic port-industrial and infrastructure node in which logistics, industrial activity, energy flows, digital systems, and hinterland connections are spatially and functionally concentrated (Punt et al., 2023a, 2023b; Van den Bosch et al., 2011). This characterization broadens the analytical scope beyond vessel movements and cargo handling to include interconnected infrastructures, port-city relations, public-private responsibilities, and digital coordination systems. An exclusively maritime framing would omit the port's connections with hinterland

logistics, industrial supply chains, energy production and distribution, and wider Dutch and European transport networks.

The port connects global shipping flows with hinterland logistics, industrial supply chains, energy production and distribution, and wider Dutch and European transport networks. Road, rail, inland waterway, and pipeline connections are not secondary features but integral parts of the port's core functioning. As a consequence of this interconnected design, disruptions affecting one infrastructure domain may become relevant for other domains, even when the original source of disruption lies outside the direct control of port actors.

The resilience of ports is therefore increasingly discussed in terms of their role within wider supply chains and infrastructure systems. United Nations Conference on Trade and Development (UNCTAD, 2022) frames port resilience as a matter of risk management, business continuity, crisis management, cyber-resilience, and preparedness across port functions. This is useful for Rotterdam because the port is here not only considered as an operational site, but also as a strategic node in wider energy, logistics, industrial, and transport networks. This framing directs attention to both internal port operations and the external infrastructure systems on which those operations rely

Rotterdam is also embedded in wider urban and regional infrastructure systems. Huck et al. (2021), in their study of networked infrastructure resilience in Rotterdam, show that urban infrastructure resilience depends on interactions between multiple public and private actors and between infrastructure systems such as water and energy. Huck et al. (2021) interpret infrastructure resilience in Rotterdam as involving institutional and organizational issues alongside technical ones, particularly because responsibilities are distributed across administrative levels, infrastructure sectors, and public-private relationships. Their analysis provides relevant case context for examining whether similar governance considerations arise in relation to a cross-infrastructure digital platform.

The digital and cyber dimension further strengthens the relevance of the case. Rotterdam's digital and cyber environment adds a further case-specific reason for its selection. Research on cyber resilience at the Port of Rotterdam shows that digital disruption can affect physical port operations, business continuity, and wider supply chains, while preparedness depends on coordination and information exchange among multiple port actors (Punt et al., 2023b). European Union Agency for Cybersecurity (ENISA, 2020) similarly frames port cyber risk as a multi-actor and socio-technical issue involving public authorities, port and terminal operators, transport companies, logistics firms, and service providers. Rotterdam is therefore relevant not simply because its operations are highly digitalized, but because digital dependence and cross-organizational coordination are already closely intertwined.

Taken together, these characteristics justify treating Rotterdam as a networked, multi-actor infrastructure setting for the purposes of this study. The case involves multiple infrastructure layers, multiple operators, multiple authorities, and multiple digital systems. The coexistence of multiple infrastructure layers, operators, authorities, and digital systems makes Rotterdam an information-rich case for examining how actors understand cross-infrastructure disruption and whether they perceive a role for a shared platform in situational awareness, interdependency mapping, or cross-actor coordination.

1.3 The EU-IDRP platform concept and its role in the study

The European Union Infrastructure Digital Resilience Platform (EU-IDRP) is a researcher-developed working concept used in this thesis. Despite its name, it does not refer to an existing European Union programme, operational platform, or technically validated prototype. It was developed as a concrete representation of a possible cross-infrastructure coordination platform through which the governance and organizational feasibility of shared digital resilience support could be examined.

At the conceptual level, EU-IDRP is imagined as a federated coordination and orchestration platform able to connect different existing systems used by infrastructure operators, port actors, and public crisis-management organizations. By conceptual design, the platform would not require participating organizations to transfer all of their operational data into one central repository. Instead, each organization would retain control over its own systems and determine which disruption-relevant outputs could be shared, at what level of detail, with which actors, and for how long.

This logic is supported conceptually by one central component of the platform, an Adaptive Data Adaptor (ADA) located within the digital boundary of each participating organization. The ADA would translate selected internal outputs into a common format, apply agreed filtering or aggregation rules, and expose only information approved by the relevant data owner. The central EU-IDRP layer could then combine these outputs to represent cross-infrastructure dependencies, examine possible cascading effects, support scenario analysis, and provide role-specific alerts or decision-support information. Raw operational data would therefore, by default, remain within the organization that controls it.

EU-IDRP is conceived as a human-in-the-loop decision-support tool, not as an autonomous command or control system. Meaning that in principle, it could provide information, warnings, dependency visualizations, or scenario outputs, but the interpretation of those outputs and all operational decisions would remain with the actors holding the relevant legal and organizational responsibilities.

Within this thesis, EU-IDRP serves two related purposes. Substantively, it is the platform concept whose possible value and feasibility are examined in the Port of Rotterdam. Methodologically, it functions as a common point of reference through which interviewees could discuss existing coordination gaps, cross-infrastructure information needs, data sensitivity, interoperability, ownership, trust, and institutional embedding.

1.4 Problem statement, Research aim and Research Question

The previous sections characterize the Port of Rotterdam as a dense cross-infrastructure ecosystem involving a distributed public-private actor landscape. Against this background, the study examines how existing coordination and digital arrangements shape the possible role and feasibility of a cross-infrastructure digital resilience platform.

The research does not assume that coordination mechanisms are absent. Instead, it investigates what existing systems and arrangements already support and where cross-infrastructure coordination gaps may remain. Because cross-infrastructure disruptions may extend beyond the organizational or sectoral boundaries in which they originate, it remains uncertain whether existing arrangements provide sufficient support for actors to interpret and coordinate their wider consequences. A disruption affecting electricity, ICT, water systems, transport corridors, terminal operations, or industrial processes may require actors to consider not only conditions within their own domain, but also possible consequences for other domains and the implications for coordinated response.

The study therefore examines whether coordination needs arise in situations that do not fit neatly within routine operational handling or formal crisis escalation. On the one hand, individual operators and public authorities retain their own responsibilities, mandates, systems, and decision rights. On the other hand, cascading disruptions may require a shared understanding of interdependencies, impacts, timing, and possible mitigation options across organizations.

Accordingly, the study treats platform feasibility as an open socio-technical question and examines how technical possibilities interact with governance and organizational arrangements. The analysis therefore considers both technical and governance dimensions of feasibility, including how different architectural choices may interact with data control, trust, and institutional arrangements. A technically plausible platform may nevertheless raise questions concerning adoption, trust, authority, ownership, and institutional fit.

The empirical analysis therefore considers questions of platform ownership, operation, funding, data-sharing safeguards, access to outputs, interpretation of recommendations, and the platform's relationship with crisis-management escalation and operator-specific decision-making.

NIS2 and CER form part of the regulatory context because they strengthen requirements concerning resilience, cybersecurity, and cooperation. The thesis examines which governance questions relevant to a shared platform remain unresolved. While these directives increase the policy relevance of resilience, cybersecurity, and cooperation, they leave open how a shared platform would be owned, governed, accessed, and integrated within local operational and crisis-management arrangements. Accordingly, the thesis does not ask solely whether a platform could be technically imagined, but under what governance and organizational conditions it could realistically be feasible.

The central research problem is therefore how existing governance and organizational arrangements shape whether a cross-infrastructure digital resilience platform could be considered feasible and potentially valuable in a complex, multi-actor port ecosystem.

The aim of this thesis is consequently to examine how existing disruption-management practices, information flows, and governance arrangements in and around the Port of Rotterdam structure the feasibility and potential added value of a cross-infrastructure digital resilience platform.

More specifically, the research examines how stakeholders understand the platform's possible roles in shared situational awareness, interdependency mapping, and cross-actor coordination, and how those possible roles would relate to existing arrangements and distributed responsibilities.

The study does not aim to technically validate EU-IDRP as a completed digital system, test a prototype, or measure operational effectiveness during real disruptions. Instead, it uses the platform concept as an analytical object through which relevant stakeholders can reflect on cross-infrastructure disruption management, platform feasibility, perceived value, risks, and governance requirements.

In this way, the thesis aims to contribute both to academic debates on port resilience and interdependent critical infrastructure governance, and to practical discussions about the possible role of digital resilience tools in complex public-private infrastructure settings.

The main research question guiding this thesis is:

“How do existing disruption-management practices, information flows, and governance arrangements in and around the Port of Rotterdam shape the feasibility and potential added value of a cross-infrastructure digital resilience platform?”

To answer this main question, the thesis addresses the following sub-questions:

- 1. How are cross-infrastructure disruptions and cascading effects currently understood in and around the Port of Rotterdam?*
- 2. How are disruption management, coordination practices, information flows, responsibilities, and decision rights currently organized across relevant actors?*
- 3. What barriers and enabling conditions do stakeholders identify for the adoption and use of a cross-infrastructure digital resilience platform?*
- 4. What governance and organizational conditions would need to be in place for such a platform to be trusted, used, and institutionally embedded in the Port of Rotterdam context?*

1.5 Scope, boundaries and contribution of the study

This thesis focuses on how existing disruption-management practices, information flows, and governance arrangements in and around the Port of Rotterdam shape the feasibility and potential added value of a cross-infrastructure digital resilience platform. The study examines this question from a governance and organizational perspective. It therefore focuses on actor roles, coordination practices, responsibilities, decision rights, information-sharing conditions, trust, interoperability, operational use, and institutional embedding.

In this thesis, the Port of Rotterdam refers primarily to the port-industrial and logistics ecosystem in and around the port area, including relevant infrastructure dependencies and public crisis-management actors. Where the municipality, safety region, Port Authority, or other specific organizations are meant, they are named explicitly. The empirical focus is therefore not the Port Authority alone, nor the municipality of Rotterdam alone, but the wider port ecosystem in which disruption management depends on multiple public and private actors.

The platform is studied as a conceptual object of analysis and not as an implemented technical system. The study does not technically validate the platform, test a prototype, or assess operational performance during real disruptions. Instead, it examines how relevant actors perceive cross-infrastructure disruption management, data sharing, coordination, decision rights, trust, interoperability, and institutional embedding, and how these perceptions shape the possible role of a digital resilience platform.

The Port of Rotterdam is not used as a statistically representative case. It is treated as an information-rich case of a large European landlord port with dense infrastructure interdependencies, a complex public-private actor landscape, and strong relevance under emerging EU resilience and cybersecurity regulation. The study is therefore not intended to produce statistical generalization or a comparative assessment of other ports. Instead, the study aims for analytical transferability: insights from the Rotterdam case may be relevant for other large port and infrastructure settings that face similar cross-infrastructure disruption and governance challenges, while still requiring adaptation to their own institutional contexts. The study also has several clear boundaries. It does not fully assess all possible risks affecting the Port of Rotterdam, nor does it quantitatively model cascading disruptions. It does not propose a detailed technical system architecture beyond the conceptual description of EU-IDRP and ADA used during the interviews. It also does not evaluate the legal implementation of NIS2 and CER

in detail. These directives are treated as regulatory context that increases the relevance of resilience, cooperation, cybersecurity, and cross-sector risk management, but they are not the primary object of legal analysis.

The scientific contribution of the thesis lies in combining conceptual and empirical insights on cross-infrastructure digital resilience. Conceptually, the thesis connects literature on port resilience, interdependent critical infrastructures, crisis coordination, data governance, digital resilience platforms, interoperability, and institutional embedding. Empirically, it uses interview-based evidence from the Port of Rotterdam to examine how relevant actors understand current disruption-management practices, information flows, barriers, enabling conditions, and governance requirements for a possible cross-infrastructure digital resilience platform.

The thesis also seeks to provide a practical contribution by structuring the governance and organizational issues that relevant actors consider when assessing whether a platform should be explored further. The analysis considers issues such as technical integration, information safeguards, actor responsibilities, institutional legitimacy, operational usability, and alignment with existing crisis-management and infrastructure-governance arrangements. It does not assume in advance which of these issues will prove decisive or how they should be configured.

1.6 Thesis structure

The remainder of the thesis is structured as shown by the following table.

Table 1: Thesis overview

<i>Chapter 2</i>	Explains the research design and methodology, including the qualitative single-case approach, data collection and literature review, interview sample, coding process, and research quality considerations.
<i>Chapter 3</i>	Develops the literature review, focusing on port resilience, cross-infrastructure disruption, digital resilience platforms, shared situational awareness, data sharing, interoperability, and governance conditions.
<i>Chapter 4</i>	Presents the literature-based case context and empirical findings from the interviews
<i>Chapter 5</i>	Discusses the interview findings in relation to the literature and derives governance, organizational, and staged implementation considerations for cross-infrastructure digital resilience platform adoption. Answers the main research question and sub-questions. Translates the findings into platform-related and Rotterdam-specific implementation considerations. Outlines the theoretical contribution, practical recommendations, limitations, and future research directions.
<i>Chapter 6</i>	Concludes the thesis.

2. Methodology

2.1 Research approach: qualitative single-case study

This thesis uses a qualitative single-case study design because the research question concerns how governance and organizational feasibility are understood within a specific, multi-actor port context. The research examines how relevant actors perceive cross-infrastructure disruption management, which coordination problems they do identify, and under what conditions they might trust, use, and institutionally embed a shared digital coordination platform.

For this logic, a qualitative design is here appropriated because platform feasibility is defined as an organizational and institutional element and not solely defined as purely technical. For this reason, it depends on roles, responsibilities, trust, decision rights, data-sharing arrangements, operational routines, security concerns and regulatory pressures, as well as on the meanings, expectations and practical experiences of actors working in different infrastructure, crisis management, cybersecurity, logistics, digital modelling and public coordination.

The single-case approach is then justified because the Port of Rotterdam is here defined as a dense and strategically important infrastructure ecosystem in which the research problem can be especially visible. Case study research is especially suitable when a real-life phenomenon must be studied and addressed within its environmental context. On this theme, Ridder (2017) describes case study research as the in-depth investigation of a real-life phenomenon within its setting, using interviews, archives and other sources to build detailed case understanding. For this specific reason, the study does not seek statistical generalizability as it mainly aims for analytical transferability. Following Flyvbjerg (2006), the Port of Rotterdam is here treated as a strategically relevant and information-rich case from which governance conditions can be analytically derived and discussed in relation to comparable European port and infrastructure hubs, by taking respect to each core difference that any European ports might have.

2.2 Case selection: the Port of Rotterdam

During this thesis research, the Port of Rotterdam was selected because it is both a strategically significant European port and a highly interdependent infrastructure ecosystem. That is, the Port of Rotterdam connects maritime transport, hinterland logistics, road and rail corridors, pipelines, energy systems, industrial clusters, digital infrastructures, water management and public crisis-management arrangements. With that taken into account and by considering the design of such network, disruptions in electricity, ICT, transport, cyber systems, water infrastructure or port logistics can in principle directly generate impactful cascading effects beyond their initial incident area.

This research frames the Port of Rotterdam as Europe's largest seaport and a key gateway for trade and energy, directly affected by evolving EU resilience and cybersecurity regulation. It also identifies the port as a setting where digital and physical critical infrastructures are tightly intertwined, making it a relevant case for studying cross-infrastructure risks and platform feasibility. The specific case contains the actor diversity that is required for such a platform to function, including port-related actors, public authorities, transport and infrastructure operators, energy actors, cyber-security organizations, terminal/logistics actors and digital/modelling experts.

Rotterdam becomes also relevant under the NIS2 Directive and the Critical Entities Resilience Directive, which are published with the broader aim to increase attention to resilience, cybersecurity, incident reporting, risk management and cross-sector cooperation (European Parliament & Council of the European Union, 2022a, 2022b). Nevertheless, regulation does not necessarily determine who should own, govern, fund, operate or use a platform. The case is therefore appropriate for examining how regulatory pressure directly interacts with local governance feasibility.

The case is constrained to the Port of Rotterdam ecosystem and its surrounding infrastructure dependencies, it focuses on governance and organizational feasibility and do not take into analysis technical engineering. It treats the platform as a conceptual object of analysis rather than as a finished and detailed functional prototype

2.3 Platform description: the EU-IDRP concept as methodological entry point

As previously described in Section 1.3, the EU-IDRP platform concept preceded the empirical phase of this study and was therefore not developed from the results of the interview findings. It was initially originated in exploratory research and concept-development work undertaken before the start of the thesis research. This earlier work was based on the idea of developing a digital resilience platform that could support coordination among interdependent critical infrastructures. When the thesis research officially began, the emphasis therefore shifted from proposing the development of such a platform to examining whether the concept would be feasible and potentially valuable within the governance and organizational environment of the Port of Rotterdam. EU-IDRP was therefore used as a prior conceptual research object and as a methodological entry point for the interviews.

Before the interview process started, the principal functional and architectural features of the concept had already been conceptually formulated. These features included a federated arrangement in which participating organizations would retain control over their own systems and data. That is, the possible use of a local filtering and translation component referred to as the Adaptive Data Adaptor, the selective exchange of disruption-relevant information, the representation of cross-infrastructure dependencies and possible cascading effects, support for scenario analysis, alerts, and decision-support outputs, and a human-in-the-loop approach in which existing actors would retain their legal, operational, and crisis-management responsibilities. These features provided a sufficiently stable common reference for the interviews. However, they were treated as pre-existing design assumptions and not as empirically established requirements or validated technical solutions.

The interviews were structured in two broad stages. In the first stage, after an introduction of the research, participants were asked about existing practices without initially being directed toward the proposed platform. Questions addressed the disruptions and infrastructure dependencies relevant to their field, current coordination arrangements, information flows, existing systems, escalation procedures, organizational responsibilities, decision rights, data-sharing practices, and perceived coordination gaps. Only after these existing practices had been discussed was EU-IDRP introduced as a hypothetical shared-platform concept. This sequencing was used so that participants could first describe the current disruption-management environment in their own terms, rather than interpreting current problems immediately through the lens of a proposed technological intervention.

The same general sequence was followed across all the interviews, although the wording and follow-up questions were adapted to the expertise and institutional position of each respondent. Operational and infrastructure actors were asked more about disruption consequences, information needs, recovery timing, and the practical usability of a platform. Crisis-management actors were asked more about escalation, shared operational pictures, mandates, and decision authority. Cyber-resilience, modelling, and interoperability actors received more detailed follow-up questions about sensitive information, technical and semantic integration, local data control, and institutional safeguards. The platform's common functional core nevertheless remained consistent across the interviews.

EU-IDRP was introduced orally. No slide, diagram, concept note, interface mock-up, prototype, or other visual or technical material was shown to the participants. The common oral description can be found in Appendix 3

The platform description was intended to make the hypothetical scenario sufficiently concrete for meaningful discussion while avoiding the presentation of EU-IDRP as an already developed or officially adopted platform. Considering no prototype or interface was shown, participants assessed the platform primarily as a functional, organizational, and governance proposition. The interviews therefore provide evidence about perceived need, added value, institutional fit, information-sharing conditions, trust, ownership, interoperability, and operational relevance. They do not provide evidence about actual interface usability, software performance, model accuracy, cybersecurity performance, or user behavior in an implemented system.

Although the platform had a predefined conceptual core, all its elements remained completely open to empirical evaluation. Participants could question whether an additional platform was needed at all, whether its proposed functions would provide operational value, whether existing systems or coordination arrangements would be preferable, and whether the federated logic or the Adaptive Data Adaptor would be workable in practice. They could also evaluate which actors should participate, what information could realistically be shared, which level of detail would be appropriate, how access should be controlled, who should own and operate the platform, how it should be funded and maintained, and how it should relate to existing operational and crisis-management arrangements. The concept was therefore bounded enough to create a common discussion object but open enough to be challenged, modified, or rejected.

Methodologically, this distinction is important for interpreting the findings. Features that existed before the interviews, such as federated data control, local filtering, and human-in-the-loop decision support, should not be presented as having emerged entirely inductively from the interview material. Interview evidence concerning these features instead represents participants' evaluation, support, criticism, or refinement of the prior concept. By contrast, the specific coordination problems, information needs, governance barriers, institutional tensions, and implementation conditions identified by participants form the empirical contribution of the study.

EU-IDRP consequently served both as the object whose feasibility was examined and as an interview stimulus through which different actor groups could discuss a common hypothetical situation. This made it possible to compare different perspectives across diversified infrastructure operators, public crisis-management actors, port-related actors, cyber-resilience actors, and digital and interoperability experts, while still allowing each participant to relate the platform to the systems, responsibilities, constraints, and routines of their own institutional setting. The following section explains how academic, regulatory, and policy sources were selected to develop the conceptual and contextual basis for this empirical examination.

2.4 Literature review and source selection

After defining the EU-IDRP platform concept, the literature review was used to place the research problem within existing academic and policy debates. The platform idea raised questions about interdependencies, data sharing, interoperability, shared situational awareness, cyber resilience, institutional embedding and cross-sector governance. Accordingly, the review helped build the conceptual language of the thesis and supported the later empirical work. The literature review followed a purposive and iterative logic. Sources were selected because they were directly relevant to the research question and to the Port of Rotterdam case. This approach was appropriate because the thesis connects different research areas that are often discussed separately, such as critical infrastructure resilience, port resilience, cyber resilience, crisis coordination, digital platforms, interoperability and EU regulation. The aim was to develop a focused conceptual basis for a qualitative feasibility study.

The literature base was first developed through keyword searches in academic databases such as Web of Science and ScienceDirect. Search terms combined port, infrastructure, resilience, digital and governance-related

concepts. Examples of search terms included critical infrastructure interdependencies, cascading failures, port resilience, maritime resilience, cyber resilience in seaports, digital resilience platforms, digital twins, interoperability, data sharing, shared situational awareness, NIS2, CER Directive and Port of Rotterdam. These searches were then complemented through reference tracing from key papers, suggestions from supervisors and sources that became relevant during the empirical phase.

The selection of sources was therefore developed step by step and resulted in a final academic literature base of 42 scholarly sources. These were complemented by 19 legal, policy, institutional, and practice-oriented sources used to establish the regulatory, methodological, and case-specific context of the study. Initial sources helped clarify the general research problem, while later sources helped refine specific parts of the thesis, such as data-sharing safeguards, interoperability, public-private coordination, cyber resilience and platform governance. This was useful because the thesis does not belong to one single literature stream. Papers on maritime and port resilience helped explain disruptions and cascading effects in port systems. Critical infrastructure literature helped frame interdependencies and cross-sector risk. Governance literature helped interpret questions of ownership, mandate, trust and institutional embedding. Digital and modelling literature helped clarify what kind of coordination and information integration a platform could support.

Priority was additionally given to peer-reviewed academic literature, EU regulatory documents and selected policy-oriented sources. Academic papers were used to define and connect the main concepts of the study, including infrastructure interdependencies, cascading disruption, resilience, shared situational awareness, interoperability, data governance and networked crisis coordination. Port-specific papers were used to contextualize Rotterdam as a complex infrastructure and logistics ecosystem. Cyber and digital resilience sources were used to understand how digitalization creates both new coordination possibilities and new vulnerabilities.

More technical sources on digital twins, infrastructure modelling and simulation were included when they helped explain the platform concept or the type of information integration that could be relevant for cross-infrastructure coordination. These sources were used at a conceptual level. Technical model testing, software validation and digital-twin validation remained outside the methodological scope of the thesis.

EU regulatory documents, especially the NIS2 Directive and the Critical Entities Resilience Directive, were included because they form part of the institutional context in which platform feasibility is discussed. These documents helped clarify the regulatory pressure around risk management, cyber resilience, incident reporting, essential services and cross-sector cooperation. In the methodology, these documents function as legal and policy context. The empirical evidence base remains the interview material, while the regulatory sources help situate interview accounts within the wider European resilience framework.

Selected policy-oriented and practice-oriented sources were also used where they were directly relevant to the problem. These sources helped connect academic concepts to practical governance issues, such as public-private cooperation, information sharing, cascading risk, safe spaces for data exchange and critical infrastructure coordination. This was important because the thesis studies a platform concept in a real port ecosystem, where governance practice, regulation and organizational routines are part of feasibility.

The sources were examined through close reading and thematic notetaking. During the review, attention was given to how each source described cross-infrastructure risk, which actors or systems were involved, which coordination problems were identified and what this implied for a shared digital resilience platform. In this way, the review helped develop sensitizing concepts for the empirical research. These concepts were later translated into interview

themes concerning disruption management, information flows, responsibilities, decision rights, data-sharing conditions, trust, confidentiality, interoperability, platform value and institutional embedding.

The literature review also supported the contextualization of the Port of Rotterdam case. It helped position the port within wider debates on port resilience, critical infrastructure governance and European resilience regulation. This was relevant because the thesis aims for analytical transferability. By connecting the Rotterdam case to broader discussions on ports, infrastructures and regulation, the review made it possible to interpret the case as an information-rich setting that may offer insights for comparable European port and infrastructure hubs.

The literature and documentary sources served two roles in this study. First, the broader academic literature was used to develop the conceptual framework and the sensitizing concepts that informed the interview protocol, the interpretation of the case, and the discussion of the findings. Second, a narrower body of Rotterdam-specific academic studies, Dutch crisis-management documentation, institutional sources, policy documents, and European regulatory instruments was used as secondary documentary evidence about the case environment.

This second documentary layer was synthesized to identify the principal contextual conditions within which EU-IDRP would have to operate. These conditions were the cross-infrastructure character of the Port of Rotterdam, the distribution of authority and operational responsibility across multiple actors, the presence of existing coordination and digital arrangements, and the regulatory pressure associated with NIS2 and CER. These conclusions are presented in Section 4.2 as literature-based contextual findings.

The term *literature-based contextual findings* does not mean that these conclusions were generated through the same inductive coding procedure as the interview findings. They were developed through close reading and thematic synthesis of secondary sources rather than through the ATLAS.ti codebook. The evidence base of the case study is therefore layered. Section 4.2 draws on secondary documentary evidence to establish the case context, while Section 4.3 draws on primary interview evidence to develop the four empirical themes. The documentary context supports the interpretation of the interview material but does not replace or independently validate it.

The next section explains how the relevant actors and infrastructure domains in and around the Port of Rotterdam were mapped before and during the empirical research.

2.5 Infrastructure and actor identification

Literature was first used to identify the relevant infrastructure domains and to understand the problem as a cross-infrastructure governance issue. Studies on port resilience, critical infrastructure interdependencies, flood resilience, cyber resilience and infrastructure governance helped describe the Port of Rotterdam as an ecosystem where several infrastructure domains are connected. These domains include maritime transport, hinterland logistics, rail and road transport, energy, ICT and digital systems, water management, terminal operations and public crisis-management arrangements.

This literature gave the first understanding of how the ecosystem is organized and why disruptions can move across sectors. A problem in electricity, cyber systems, transport infrastructure, water infrastructure or terminal operations can affect other actors because many port processes depend on shared systems, shared corridors, shared information flows and coordinated decision-making. Accordingly, the actor mapping started from the idea that platform feasibility had to be studied across different domains and institutional positions.

The first actor categories were therefore derived from the literature and from the case description of the Port of Rotterdam. Previous research on Rotterdam and port resilience pointed to port authorities, infrastructure operators, public crisis-management actors, water and flood-related actors, cyber-security actors, logistics and terminal actors, transport operators, digital experts and interoperability experts as relevant groups for the research. EU resilience and cybersecurity regulation also helped define the wider institutional setting, because NIS2 and CER increase attention to risk management, incident reporting, resilience planning and cooperation across sectors.

After this first mapping, it was necessary to reach out to actors who could provide information-rich perspectives on these domains. Participants were selected because they could explain one or more parts of the problem: infrastructure operation, disruption management, cyber resilience, public crisis coordination, port innovation, terminal IT, digital modelling or interoperability. The sample was therefore built from the relevance of each actor to the research question. An initial set of actors was contacted using web search and LinkedIn. Due to the criticality of infrastructure nature and sensitivity of current processes or information, a major part of reached actors rejected the invitation to be part of the research.

The mapping was then refined during recruitment and during the first interviews. Some actors helped clarify which other perspectives were relevant, and in a few cases, this led to additional outreach. This snowball element was useful because the Port of Rotterdam ecosystem is distributed across many organizations, and some relevant connections are easier to identify through practitioners who work inside the field. Snowballing was therefore used as a minor and complementary recruitment strategy, while the main selection logic remained purposive and based on relevance to the research question.

The final actor mapping included operational, public, cyber, digital and governance-oriented perspectives. Transport infrastructure actors were relevant because they could explain operational continuity, rail disruption, control-center coordination and escalation. Public crisis-management actors were relevant because they could explain formal coordination structures, shared operational pictures and net-centric working. Energy and infrastructure actors were relevant because electricity dependence is central to cascading disruption and critical service continuity. Port innovation and terminal IT actors were relevant because they could explain digitalization, platform adoption, operational dependencies and the practical value of resilience tools. Cyber-resilience actors were relevant because they could explain information-sharing constraints, threat intelligence, security maturity and data sensitivity. Digital modelling and interoperability experts were relevant because EU-IDRP depends on data integration, semantic alignment, model coupling and socio-technical interoperability.

Table 2.1 presents the interview actor categories and organizational affiliations used in the thesis and explains how each actor type is relevant to the research question.

Table 2.1. Interview actor categories and organizational affiliations

Interview group	Actor-type category used in the thesis	Infrastructure name	Relevance to the research question
Transport infrastructure and rail continuity actors	Transport infrastructure operator / crisis-management actor	ProRail	Provided insight into 24/7 operational continuity, rail disruption, escalation, netcentric working and cross-modal coordination

Interview group	Actor-type category used in the thesis	Infrastructure name	Relevance to the research question
Public infrastructure and water/crisis-management actors	Public authority / crisis-management actor	Rijkswaterstaat	Provided insight into public crisis structures, water-safety risks, LCMS/netcentric coordination and multi-actor crisis governance
Energy infrastructure risk actor	Infrastructure operator / energy actor	Stedin	Provided insight into electricity dependence, enterprise risk management, cascading disruption, public-private responsibilities and critical service continuity
Port innovation actor	Port authority / innovation actor	Port of Rotterdam	Provided insight into port digitalization, internal/external platform feasibility, stakeholder management and resilience initiatives
Port cyber-resilience actor	Cyber/security actor	FERM	Provided insight into port cyber resilience, information-sharing arrangements, NIS2-related incentives, threat intelligence and security maturity
Terminal and logistics IT actor	Logistics/terminal actor / IT-operations actor	ECT Rotterdam	Provided insight into terminal operations, IT disruption, automated container handling, cyber incidents and operational dependencies
Digital infrastructure modelling actor	Digital/modelling expert	MOVICI	Provided insight into cross-sector modelling, data integration, model interoperability and infrastructure dependency representation
Digital governance and interoperability actor	Interoperability expert	TU DELFT	Provided insight into technical, semantic, organizational, legal and relational interoperability in digital public infrastructure contexts

2.6 Semi-structured expert interviews

The main empirical material consisted of ten semi-structured expert interviews. This format was selected because the research required a common direction across interviews, while still leaving space for participants to explain their own role, experience and institutional context (Ahlin, 2019). The interviews were used to understand how actors perceive cross-infrastructure disruptions, how coordination currently works, what information is shared, and under which conditions a shared digital resilience platform could be feasible.

Participants were selected purposively on the basis of the actor mapping described in the previous section. The aim was to include actors with practical, institutional or technical knowledge of the problem. The sample therefore included participants connected to infrastructure operation, disruption management, public crisis coordination, port innovation, cyber resilience, terminal and logistics IT, digital modelling and interoperability. Recruitment relied on professional and academic networks, targeted outreach and a small snowball element.

Individual-level pseudonymization was used because the research concerns critical infrastructure, cyber resilience, operational disruption, and governance arrangements. Personal names and direct personal identifiers were removed from the thesis. Organizational affiliations are retained because they are analytically relevant to the multi-actor governance analysis. Participants are therefore described through interview IDs, actor types, institution types, expertise areas and, where analytically relevant, organizational affiliations. Role descriptions and contextual details are generalized where their combination with an organization and quotation could make an individual readily identifiable. Table 2.2 provides a pseudonymized overview of the interview material used in the study.

Table 2.2. Pseudonymized interview overview

Interview ID	Interview period	Mode and language	Actor-type	Institution type	Main expertise / relevance to the research question
I1	May 2026	Online / English	National crisis-management and net-centric working expert	Water National infrastructure / public crisis-management network	Net-centric working, national crisis coordination, shared operational pictures, and crisis-information exchange
I2	May 2026	Online / English	Rail infrastructure operator – operational IT and control-center perspective	Rail infrastructure operator	Operational IT, control-centre coordination, rail disruption management, and infrastructure continuity
I3	April 2026	Online / English	Rail infrastructure operator – business continuity and resilience perspective	Rail infrastructure operator	Business continuity, resilience planning, rail infrastructure dependencies, and disruption preparedness
I4	April 2026	Online / English	Port terminal / automated container operations and IT-continuity expert	Port logistics / terminal operations	Automated terminal operations, IT continuity, container handling,

					operational disruption, and port logistics dependencies
I5	May 2026	Online / English	Cross-sector infrastructure modelling and digital-twin/simulation expert	Academic / infrastructure modelling platform	Cross-sector modelling, digital-twin logic, simulation, dependency representation, and data integration
I6	May 2026	Online / English	Electricity distribution operator – corporate risk management perspective	Energy / electricity distribution operator	Electricity distribution, corporate risk management, critical service continuity, and infrastructure interdependencies
I7	April 2026	Online / English	Port authority innovation and emerging-technologies perspective	Port authority	Port innovation, emerging technologies, digitalization, platform feasibility, and stakeholder coordination
I8	April 2026	Online / English	Rail infrastructure operator – crisis-management and network-governance perspective	Rail infrastructure operator / crisis-management network	Crisis management, network governance, rail disruption coordination, escalation, and multi-actor response
I9	April 2026	Online / English	Academic / research expert on interoperability and digital public infrastructure	Academic / interoperability research	Technical, semantic, organizational, legal, and governance dimensions of interoperability
I10	April 2026	Online / English	Port cyber-resilience intermediary / port-sector	Port cyber-resilience intermediary	Cyber resilience, port-sector information sharing, threat

			information-sharing actor		intelligence, NIS2-related incentives, and security maturity
--	--	--	---------------------------	--	--

This table reports the interview ID, interview period, mode, language, actor type, institution type and main expertise area. This table shows how the final empirical material relates to the actor categories identified in Table 2.1.

The interviews were conducted as semi-structured expert interviews. The interview guide was used flexibly and was adapted to the role, expertise and institutional position of each participant. The interviews therefore followed the same general direction, but the emphasis changed depending on what each actor could meaningfully explain.

Across the interviews, the questions focused on current disruption-management practices, information flows, coordination arrangements, responsibilities, decision rights, data-sharing conditions, trust, interoperability and the possible value of EU-IDRP. For example, crisis-management actors were asked more about escalation, coordination and information needs during disruptions, while digital and interoperability experts were asked more about data integration, model alignment and platform feasibility. Cyber-resilience and port-related actors were asked more about sensitive information sharing, threat intelligence, security maturity, platform adoption and institutional trust.

This flexible structure made it possible to keep the interviews comparable while still allowing each participant to speak from their own practical experience. The protocol therefore worked as a guiding structure rather than as a fixed questionnaire. Follow-up questions were used when participants introduced relevant examples, uncertainties or actor-specific concerns. An example of the interview questions is included in the appendix.

All interviews were conducted in English and online. The recordings and transcripts were used for coding, quotation selection and evidence validation. The full transcripts are not reproduced in the thesis because they may contain identifiable or operationally sensitive information. Instead, quotations and summarized evidence are presented without personal-name attribution. Interview IDs, broad actor categories and, where analytically relevant and consistent with the consent arrangements, organizational affiliations are used to indicate the institutional perspective behind the evidence. After the interviews were completed and the transcripts were prepared, the material was analyzed through a two-stage inductive coding process. The next section explains how this coding process was conducted and how the final empirical findings were developed.

2.7 Data analysis: inductive coding and thematic interpretation

The purpose of the analysis was to move from interview accounts to empirical findings that could answer the research question. The analysis therefore focused on recurring patterns across actor types, while still keeping the meaning of each quotation connected to its interview context.

The analysis followed a two-stage coding process. In the first stage, the interview transcripts were coded using ATLAS.ti in an open yet descriptive way. This first-cycle coding generated a large number of detailed codes connected to specific quotation fragments. These codes captured what interviewees said about disruptions, coordination, information sharing, crisis escalation, interoperability, data sensitivity, trust, governance, platform adoption and operational constraints. At this stage, coding stayed close to the words and concerns of participants.

Because the first-cycle codes were highly detailed, a second-cycle coding step was then conducted. In this step, the original codes were reviewed together with the full interview transcripts. The aim was to understand what each quotation meant in its interview context. Where necessary, short quotation fragments were expanded into larger transcript segments, so that the final code reflected the full point made by the interviewee. This was important because several interview statements only became analytically meaningful when read together with the surrounding explanation.

During second-cycle coding, related first-cycle codes were consolidated into broader analytical codes. Similar codes were merged, overlapping codes were clarified, and weak or purely contextual quotation fragments were separated from stronger evidence. Some transcript segments were assigned to more than one code when they supported multiple analytical points. This was especially relevant for segments that connected information sharing to trust, interoperability to governance, or crisis coordination to data sensitivity. The broader analytical logic was informed by methodological guidance on thematic analysis, while the coding stages were adapted to the specific empirical and research context of this thesis (Ahmed et al., 2025).

The final codebook was then developed as a formal version of this coding process. Each final analytical code was defined through a code name, description, quotation, actor coverage and evidence strength. This made the analysis more transparent because the codebook showed how quotation-level material was translated into broader empirical claims.

Table 2.3 presents the data-analysis workflow. It shows how the analysis moved from transcript preparation to initial coding, code consolidation, theme development, cross-actor comparison, evidence validation and chapter synthesis.

Table 2.3. Data-analysis workflow

Step	Analytical activity	Output
1. Transcript preparation	Organizing recordings, meeting notes and automatic transcripts into readable interview transcripts	Cleaned and structured transcript set
2. Initial coding	Coding relevant transcript segments in ATLAS.ti	Initial code list and quotation base
3. Code consolidation	Reviewing fragmented codes and merging overlapping ones	Consolidated codebook
4. Theme development	Grouping codes into higher-order thematic categories	Candidate themes
5. Cross-actor comparison	Comparing evidence across actor types and identifying convergences/tensions	Actor-type theme matrix
6. Chapter synthesis	Translating validated themes into empirical findings and governance implications	Chapter 4 findings and Chapter 5 discussion

The final analytical codes were grouped into four empirical findings. These findings were developed inductively from recurring patterns in the interview material and then checked against the transcripts and the earlier coding files.

Cross-actor comparison was used throughout the analysis. This comparison examined which issues appeared across several actor types and which issues were more specific to particular institutional positions. For example, crisis-management actors were especially important for understanding escalation, authority and coordination structures. Operational and terminal-related actors were important for understanding disruption consequences, workload and practical information needs. Cyber-resilience actors were important for understanding sensitive information sharing, threat intelligence and trust. Digital modelling and interoperability experts were important for understanding data integration, model coupling and socio-technical alignment. This comparison helped identify findings that cut across actor types rather than depending on one organizational viewpoint.

Analytical refinement was then used to keep the findings connected to the empirical material. Quotations were checked against the original transcripts to avoid decontextualization. Short fragments were expanded when the surrounding text was needed to understand the participant's point. Claims that were weakly supported were removed, softened or treated as contextual evidence. Quotations that could not be confidently linked to a final analytical code were kept outside the main evidence base.

The final findings chapter was then written from this validated evidence base. Direct quotations were selected because they clearly represented an analytical point and because they could be connected to broader patterns across the material. In this way, the analysis remained inductive and empirical, while still being structured enough to support the later discussion of governance and organizational feasibility for EU-IDRP.

2.8 AI Statement

A generative AI tool, ChatGPT 5.5, was used as a limited supporting tool at specific stages of the organization, refinement, and presentation of the research. Its use did not alter the data-analysis workflow presented in Table 2.3. The interview transcripts were first reviewed and coded by the researcher in ATLAS.ti through open and descriptive first-cycle coding. This initial stage produced a relatively granular set of researcher-generated codes connected to specific quotation segments. The first-cycle codes, their definitions, and their links to the interview material were therefore established before generative AI was introduced into the analytical process.

Generative AI was subsequently used during parts of code consolidation and, more specifically, during Step 4: theme development. At this stage, the tool assisted in comparing the more granular researcher-generated codes, identifying possible conceptual overlaps or redundancies, and suggesting candidate groupings through which related codes might be organized into broader analytical categories. For example, codes concerning separate operational systems, role-based access, fragmented communication channels, and the absence of a common operational picture could be compared as possible components of a broader theme concerning partial visibility and shared system-level awareness. These suggestions were treated as analytical prompts rather than as final coding decisions. The researcher reviewed each proposed grouping against the complete interview context, the original coded quotations, the developing codebook, and the research question. Suggested groupings could therefore be retained, modified, separated, or rejected through manual interpretation.

Generative AI did not independently assign codes to the interview material, determine the meaning of quotations, select the final themes, or establish the strength of the empirical evidence. Theme development remained an interpretive and iterative process led by the researcher. After candidate themes had been developed, the researcher manually compared them across actor types, checked the supporting quotations against the original transcripts, distinguished core from supporting evidence, and removed or softened claims that were insufficiently supported. The final four findings were therefore based on the researcher-led coding process, cross-actor comparison, the finalized codebook, and manual quotation validation.

AI was also used in a limited editorial capacity during the writing process. It supported the refinement of sentence structure, paragraph organization, transitions between sections, and the overall linearity of the thesis. This included helping identify repetition, improve the sequence in which arguments and findings were presented, and make the relationship between paragraphs more explicit. Such assistance concerned the presentation of researcher-developed content rather than the generation of substantive findings. All AI-assisted wording was reviewed and revised by the researcher to ensure that it remained consistent with the interview evidence, the conceptual framework, and the intended analytical meaning.

Additionally, AI supported administrative aspects of reference-list organization. It was used to help alphabetize entries, identify apparent inconsistencies in formatting, and suggest a more uniform presentation of author names, publication years, titles, journal information, and in-text citation forms. The researcher remained responsible for checking the bibliographic details against the original sources and for confirming the accuracy of author lists, publication years, titles, digital object identifiers, and the selected citation style. AI assistance with the reference list was therefore limited to ordering and formatting support and was not treated as source verification.

Final interpretation, code selection, theme definition, quotation validation, evidence assessment, written claims, and conclusions remained the responsibility of the researcher. The analytical authority of the study rests on the interview transcripts, the researcher-led coding process, the final codebook, the cross-actor comparison, and manual validation. Generative AI therefore functioned only as a secondary organizational and editorial aid.

2.9 Research quality & Ethics

The quality strategy adopted during this research focused on trustworthiness, transparency and analytical traceability, reflecting the qualitative and interpretive nature of the study. The aim was therefore to develop a credible and well-documented interpretation of the governance and organizational conditions shaping the feasibility of a cross-infrastructure digital resilience platform in the Port of Rotterdam case and not to produce statistically generalizable findings.

Credibility was supported mainly through comparison of evidence across different interviews and actor categories. Secondary academic, institutional, policy, and regulatory sources were also used to establish the case context and to position the interview accounts within wider debates on infrastructure resilience, coordination, digital systems, and regulation. Such sources were not used to mechanically verify the interview themes, nor to increase the apparent strength of weak interview evidence. Where documentary and interview evidence converged, this was treated as contextual consistency while where different perspectives or tensions appeared, the interview evidence was retained and interpreted on its own terms.

In the findings chapter, direct quotations are used to show how interpretations are grounded in the empirical material. Quotations were also checked against the original transcripts to reduce the risk of misinterpretation or decontextualization.

Transferability was then addressed by providing contextual detail on the Port of Rotterdam case, the actor categories involved, the proposed platform concept and the governance conditions under analysis. Rather than claiming direct generalizability, the research provides sufficient case-specific detail for readers to judge whether the findings may be relevant to other landlord ports, infrastructure hubs or multi-actor resilience settings.

Following, dependability was supported by documenting the research design, data sources, actor-type categories, coding process, thematic development, validation procedure and limitations. ATLAS.ti exports, thematic workbooks and evidence matrices provided a structured audit trail from transcripts and coded quotations to the

final analytical themes. This audit trail helped make the interpretive process more transparent, even though theme development remained an analytical judgement rather than a mechanical aggregation of codes.

Confirmability was then supported by linking interpretations to coded evidence, direct quotations and cross-actor patterns. Reflexivity was particularly important because the research examines the feasibility of a digital resilience platform, a concept that could otherwise lead to overly solution-oriented interpretations. To address this risk, the analysis explicitly included skepticism, barriers, informal workarounds, operational constraints, data-sharing concerns, institutional tensions and limits to platform feasibility. All these elements were treated as central empirical evidence for assessing the governance conditions under which such a platform could or could not be developed.

Because the study involved human participants and addressed critical infrastructure, cybersecurity, operational disruption and organizational responsibilities, the ethical strategy focused on informed consent, confidentiality, individual-level pseudonymization, secure storage, participant rights and the avoidance of operationally sensitive disclosure.

This study was conducted in accordance with the approved TU Delft human-research ethics procedure. Before participants were approached, the HREC documentation was completed and approved, following the TU Delft requirement that research involving human participants should receive HREC approval before recruitment begins and that MSc thesis research should be approved by the responsible researcher. The approved HREC checklist identifies this project as a TU Delft MSc thesis on cross-infrastructure digital resilience in the Port of Rotterdam, with a research period from February to June 2026, with later refinements to July 2026. It also records the corresponding researcher, the responsible researcher, the faculty and the department involved in the study (Delft University of Technology, 2022).

Over the interview process, participants were informed about the study purpose and intended use of interview material. The informed consent form which is present in Appendix 4 states that participants were invited to discuss cross-infrastructure disruption management in and around the Port of Rotterdam, including governance arrangements, coordination practices, information sharing and shared digital resilience tools or platforms. It also states that interviews would be recorded and supported by note-taking. Participation was completely voluntary, that is, participants could refuse questions and withdraw without any consequences, personal information would not be shared beyond the study team, and responses could be quoted anonymously if preferred.

Data management followed the DMP (Data Management Plan). That is, such form identifies informed consent as the legal ground for personal-data processing and records personal data such as contact details, audio recordings, proof of consent, job title and employer, and names used for administrative purposes. It states that no personal data would be transferred to third parties and that anonymized or aggregated data may be shared. Because of clear security sensitivity, the research deliberately avoided requesting any detailed system schematics, operational vulnerabilities, confidential incident plans or sensitive cyber-security procedures. Interviews could remain at a high governance level, and participants could decline sensitive questions.

3. Literature Review and Conceptual Framework

3.1 Introduction

Chapter 3 sets out the literature and concepts used to study the feasibility of EU-IDRP in the Port of Rotterdam. It begins with cross-infrastructure disruption and port resilience. It then addresses digital resilience platforms, shared situational awareness, data governance, interoperability, and cross-actor coordination. This progression connects cascading disruption with the governance and organizational conditions surrounding a shared digital platform. Within the thesis, Chapter 3 provides the conceptual basis for the empirical analysis. Its concepts guide the presentation of the findings in Chapter 4 and support their interpretation in Chapter 5. The chapter therefore creates a clear link between the research problem, the interview material, and the later discussion.

The actual starting point of the chapter is that ports are not isolated transport nodes. They are complex socio-technical systems that depend on energy, ICT, transport, water, logistics, industrial activity, public safety, and digital coordination infrastructures. Disruptions in one of these systems can propagate across others, creating cascading effects that exceed the control of any single organization. This makes port resilience not only a matter of physical robustness or technical preparedness, but as well as a governance challenge involving distributed responsibilities, fragmented information, public-private interdependence, and contested decision authority.

The literature review follows a funnel-shaped logic. Section 3.2 establishes the problem foundation by examining critical-infrastructure interdependencies, cascading disruption, and port resilience. Sections 3.3 to 3.5 progressively narrow the analysis toward shared situational awareness, information governance, and interoperability. Section 3.6 then examines the collaborative, network, and crisis-governance conditions under which cross-infrastructure coordination can take place. Within each section, the review distinguishes what previous research establishes, what remains unresolved, and which issue is subsequently examined through the interviews.

This structure avoids a technology-deterministic framing. EU-IDRP is not treated as a self-evident solution to port disruption management, but as a possible coordination and sensemaking layer whose feasibility depends on governance and organizational conditions. The literature is therefore used to define the analytical problem and identify relevant questions without predetermining the empirical findings presented in Chapter 4.

3.2 Cross-infrastructure disruptions and port resilience

The first valid area of research was based on critical infrastructure interdependencies and cascading disruptions. The literature on such theme starts from the observation that different infrastructures such as energy, transport, water, telecommunications, logistics, and emergency services cannot nowadays, be understood as just separate systems. Instead, they are interdependent socio-technical systems whose functioning depends on physical assets, digital control systems, organizational routines, institutional responsibilities, and user practices. Rinaldi et al. (2001) provide a foundational contribution by distinguishing between physical, cyber, geographic, and logical interdependencies. Physical interdependencies arise when the output of one infrastructure is required for another to function. Cyber interdependencies arise through information and communication systems. Geographic interdependencies occur when infrastructures are co-located and exposed to the same hazard. Logical interdependencies refer to less direct relationships, such as financial, regulatory, market, or organizational links.

Figure 3.1 visualizes this broader interdependency logic and shows visually why failures in one infrastructure domain can create consequences for others.

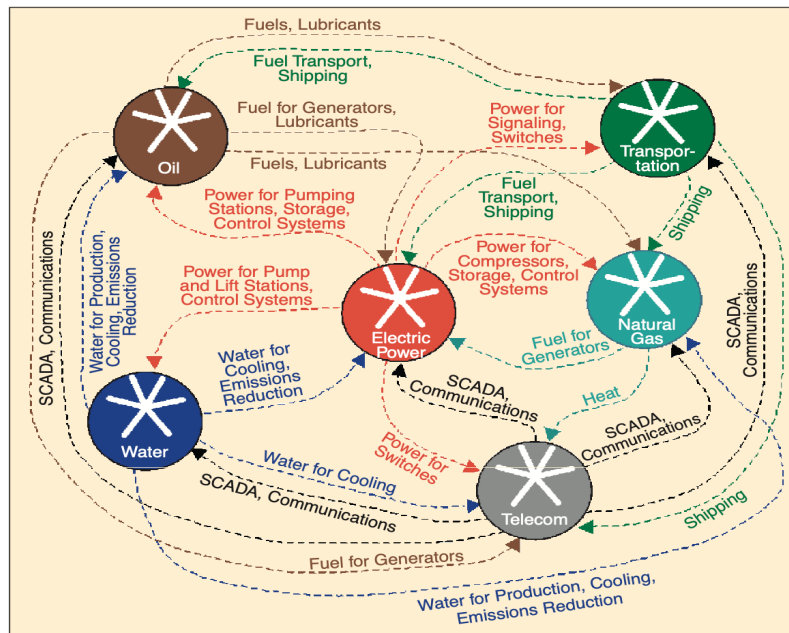


Figure 3.1 Examples of infrastructure interdependencies. Source: Rinaldi et al. (2001, Fig. 3).

In the Port of Rotterdam context, this logic is relevant because electricity, ICT, transport, water, logistics and crisis-management arrangements are not separate layers, but mutually dependent systems.

This presented typology is central because cascading disruption is rarely caused by just one type of interdependency. In practice, a disruption may begin as a physical failure, but its consequences can spread through digital systems, organizational dependencies, spatial proximity, and decision-making processes. Little (2002) argues that interconnected infrastructures create vulnerabilities that cannot be addressed only through the protection of isolated assets. The core problem is that failures can propagate through service dependencies, producing consequences that do extend beyond the initial disruption. Cascading disruption is therefore understood as both a technical and organizational phenomenon. Cascading disruptions also depends on how actors detect, interpret, communicate, and respond to emerging system stress and not only on the structure of infrastructure networks.

Research on interdependent infrastructure modelling has developed a wide range of approaches to capture these propagation mechanisms. Ouyang (2014) reviews modelling and simulation approaches for interdependent critical infrastructure systems, including empirical, agent-based, system dynamics, economic, and network-based approaches. Such approaches can in theory help identify critical nodes, dependency patterns, and possible failure pathways. Yet modelling interdependencies does not automatically solve the governance challenge. A model may in principle represent dependencies between electricity, water, transport, and ICT systems, but actors will still need to agree on what data can be shared, how outputs should be interpreted, who is responsible for acting, and how decisions are coordinated.

Balakrishnan et al. (2024) develop an integrated simulation and optimization framework for interdependent power, water, and transport networks in Shelby County, Tennessee. The framework compares alternative resilience investments by combining physical-damage and business-disruption losses with decision-makers' risk preferences. Their analysis shows that resilience-investment pathways change when decision-makers assign different weights to low-probability, high-impact events. The study therefore demonstrates that resilience planning

is shaped not only by technical system performance, but also by how risks, costs, and anticipated benefits are perceived by decision-makers.

Arvidsson et al. (2021), through a systematic cross-field review of critical-infrastructure, geographical-information-science, and risk-governance research, identify geo-visualization, spatial data management, hazard modelling, and network analysis as important opportunities for analyzing infrastructure interdependencies. At the same time, they find limited integration across the three research fields and identify continuing difficulties related to conceptual harmonization, confidential data, and the incorporation of socio-cultural dimensions. Taken together, these studies show that infrastructure dependencies can be represented analytically, but that the usefulness of such representations remains dependent on decision assumptions, access to suitable information, and alignment between different bodies of knowledge.

Practice-oriented leadership reaches a similar conclusion. For example, C40 Cities Climate Leadership Group (2019) presents infrastructure interdependencies especially as a cross-sector problem requiring mapping, collaboration, and attention to cascading effects across administrative and sectoral boundaries. This is useful because it translates the abstract concept of interdependency into a practical governance task. The point is that actors really need to identify shared failure points, discuss cascading consequences, and develop procedures for managing interconnected risks.

Following cross-infrastructure interdependencies and disruptions, it is relevant to now address the idea of port resilience and seaport disruption management. That is, ports are defined as a particularly consequential type of critical infrastructure because they combine logistics, industrial activity, transport connections, digital coordination, energy flows, and public authority functions. They represent the interfaces between maritime and hinterland networks and are embedded in wider supply chains. Their resilience therefore depends on more than the robustness of quays, terminals, access channels, or physical assets, it also depends on organizational preparedness, cyber resilience, information exchange, stakeholder coordination, and the actual ability to maintain essential functions under disruption.

Two recent reviews are especially important for positioning the development of port-resilience research. Mohsendokht et al. (2026) critically examine the development of seaport-resilience analysis across definitions, disruption types, assessment methods, limitations, and future research directions. Their review shows that the field remains conceptually and methodologically diverse. That is, resilience is operationalized through different capacities and analytical traditions, including robustness, recovery, adaptability, and learning. This makes seaport resilience a multidimensional concept but also complicates comparison and accumulation across studies.

Tsoulfas (2026) applies a Scopus search, bibliometric co-occurrence analysis, a PRISMA-guided systematic review, and qualitative content analysis to 41 journal articles. The review identifies a shift from a predominantly infrastructure-centered understanding of port resilience toward a more holistic view that includes organizational adaptation, governance, stakeholder collaboration, technology, and environmental pressures. It also finds that digital technologies can improve monitoring, forecasting, and operational decision support while simultaneously introducing cybersecurity vulnerabilities, system-failure risks, and new technological dependencies. Read together, these reviews establish that contemporary port resilience cannot be reduced to the physical resistance or recovery of port assets. That is, it also depends on organizational, technological, environmental, and governance capacities.

Network-based research further specifies how disruption can propagate through maritime and hinterland transport systems. Zhang et al. (2024) conduct a systematic review supported by science mapping to examine the

development of maritime transportation network resilience research. Their analysis organizes the literature around the construction and topological characterization of maritime networks, vulnerability-oriented and recovery-oriented resilience analysis, resilience-investment decisions, climate-change impacts, and pandemic-related disruption. The review therefore shows that maritime resilience has been examined through several different analytical perspectives, ranging from the identification of critical network structures to the assessment of disruption impacts and possible recovery strategies.

Cao et al. (2025) move from literature synthesis to a data-driven analysis of the global container-shipping network. Using liner-service data from 2020 to the second quarter of 2023, covering 686 ports, they model the network as a weighted and directed system and assess how port failures can trigger cascading load redistribution. The study compares a breadth-first redistribution rule, in which disrupted cargo is distributed across multiple ports, with a depth-first rule, in which the load is transferred toward a single preferred port. The results show that these choices create different resilience effects. That is, multi-target redistribution disperses risk but can involve more ports in the cascade, whereas single-target redistribution concentrates pressure on individual ports and may reduce the network's remaining safety redundancy. The authors also test their models against five historical port-disruption scenarios.

Lu and Qiu (2025) extend this network perspective to the relationship between seaports and dry ports. Using empirical data from China's coastal port system, they develop a multi-stage load-redistribution strategy in which disrupted loads can first be buffered by dry ports, then shared with neighbouring seaports, and finally managed through port skipping. Their results indicate that this staged strategy can contain cascading failures, reduce losses in network efficiency, and protect major seaports from mutual disruption. The study also finds that the number of operational dry ports has a stronger effect on network resilience than their individual capacity and identifies the importance of selecting an appropriate port-skipping probability. Together, these studies establish that the consequences of a port disruption depend not only on the initial failure, but also on network topology, port criticality, available capacity, and the rules used to redistribute disrupted flows. They consequently show how failures can extend across maritime routes, neighbouring ports, dry ports, and wider hinterland connections. Their primary focus, however, remains the quantitative behavior and performance of transport networks rather than the organizational arrangements through which relevant data would be shared, model outputs interpreted, and response decisions coordinated. Figure 3.2 provides a compact way to understand resilience as a process of disruption, performance loss, response, recovery and movement toward a new stability.

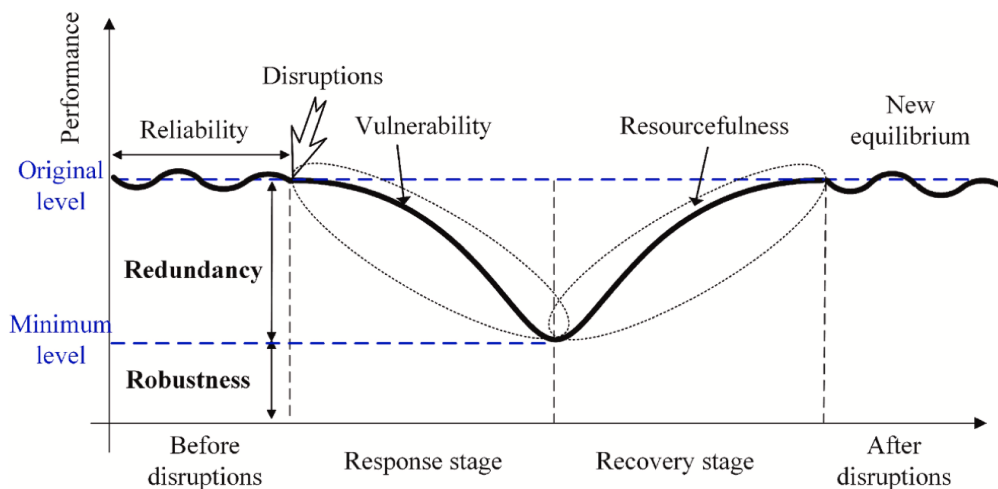


Figure 3.2. Four stages of resilience in shipping networks. Source: Gu and Liu (2023, as cited in Cao et al., 2025, Fig. 1).

In this thesis, the figure is used only as a conceptual reference, the empirical focus remains on how actors interpret, share and coordinate disruption-related information across infrastructure domains.

The contribution of these studies to the present thesis is therefore problem-defining rather than governance-prescriptive. They show why disruption should be analyzed beyond an individual port, asset, or transport mode and why system-level consequences require attention. They do not, however, establish how autonomous organizations should provide the data needed for such analyses, jointly interpret model outputs, or allocate responsibility for acting on them. These questions require a governance and organizational analysis in addition to network modelling.

Following, cyber resilience is particularly relevant for digitally mediated ports. Punt et al. (2023b) examine cyber resilience in the Port of Rotterdam and show that preparation for cyberattacks is shaped by distributed responsibilities, uncertainties, ambiguities, limited information exchange, and weak incentives. This gets directly important as it connects the port context, digital disruption, cyber risk, and governance all at once. At the same time though, it also cautions against assuming that technical cyber preparedness can automatically create and establish port-wide resilience.

Three Rotterdam-based studies provide the closest empirical foundation for the present case. Huck et al. (2021), drawing on 26 semi-structured interviews and documentary material, examine how the municipality can contribute to the resilience of interdependent urban infrastructures despite having limited direct control over many infrastructure operators. They identify divergent sectoral understandings, restricted information flows, resource-intensive cross-sector cooperation, and a mismatch between public responsibility and practical authority. The authors consequently argue for clearer roles and responsibilities, cross-sectoral budgeting, and stronger alignment between local, regional, and national levels.

Punt et al. (2023a), based on 17 interviews and 33 documents, reach a related conclusion for flood resilience at the Port of Rotterdam. Although they identify coordination across vertical, horizontal, and territorial dimensions, they also find continuing knowledge gaps, siloed budgeting and thinking, unclear divisions of responsibility, and insufficient cross-territorial arrangements. Their analysis shows that the institutionalization of resilience remains constrained by governance structures that were historically organized around flood protection rather than the resilience of interdependent critical infrastructures.

In their study of cyber resilience, Punt et al. (2023b) combine 18 semi-structured interviews, 15 participatory observations, and 46 policy and legal documents. They find that many cyber-risk strategies remain oriented toward protecting computer systems, while anticipatory and recovery-oriented practices are frequently informal and insufficiently coordinated. Limited information exchange, knowledge deficits, differing understandings of cyber resilience, incomplete regulation, and weak economic incentives constrain collective preparedness.

Across the three studies, the recurring conclusion is that infrastructure-resilience problems are recognized in Rotterdam, but relevant information, resources, responsibilities, and decision authority remain distributed across organizations and levels of governance. At the same time, the studies remain focused on urban infrastructure management, flood resilience, or cyber resilience. They do not directly examine the governance feasibility of a shared cross-infrastructure digital coordination layer operating across hazards and sectors. This is the more specific gap addressed by the present research.

Previous studies therefore establish that ports are interdependent socio-technical systems in which disruption can propagate across physical, digital, logistical, spatial, and institutional boundaries. They also establish that

Rotterdam's resilience challenges are shaped by fragmented responsibilities and cross-sector coordination constraints rather than by technical vulnerability alone.

What remains unresolved is how actors in an already populated port-governance environment recognize cross-infrastructure consequences, what forms of shared visibility they require, and whether a digital coordination layer could add value without displacing existing responsibilities and systems.

The interviews consequently examine how relevant actors understand cascading effects, how current coordination operates across infrastructure boundaries, and which governance and organizational conditions shape the possible role of EU-IDRP.

3.3 Digital resilience platforms and shared situational awareness

Digital resilience platforms, common operational pictures, digital twins, early-warning dashboards, and decision-support systems are increasingly discussed for their role as tools for improving infrastructure resilience.

Their main promise lies in integrating information from multiple systems, visualizing dependencies, supporting real-time monitoring, and helping actors anticipate cascading effects.

However, the literature also shows that shared data does not automatically produce shared understanding.

Steen-Tveit and Munkvold (2021) make a critical distinction between a common operational picture and common situational understanding. A common operational picture can provide a shared information base, but common situational understanding requires actors to interpret that information in relation to context, responsibilities, trust, communication processes, and operational priorities.

Figure 3.3 illustrates the basic idea of a common operational picture across multiple emergency-response organizations.

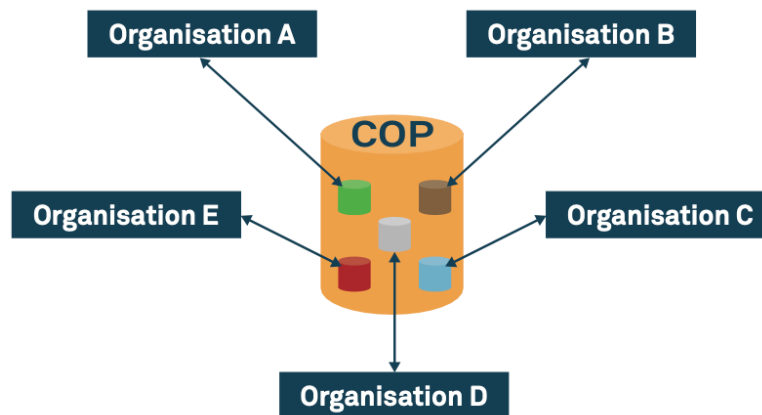


Figure 3.3. Common operational picture shared among teams and organizations involved in emergency response.

Source: Treurniet (2022, Figure 1).

For this thesis, the relevance of the figure lies not in emergency response as such, but in the broader problem of turning distributed information into shared situational awareness.

This distinction between shared data and shared understanding is now central to the thesis.

A cross-infrastructure platform should not be assessed only by whether it can display data from different infrastructures, it really should be evaluated by whether it helps actors understand what a disruption means for their own operations and for the actual wider port system.

Luukkala et al. (2017) address information overload by developing the concept of a Context-Aware Common Operational Picture. Their four-step conceptual method connects theories of situational awareness, cognition, perception, and human memory to the structures and processes of a common operational picture. Rather than presenting all available information with equal prominence, the proposed concept uses situational narratives and contextual relevance to identify and highlight information that is meaningful for a particular user and situation. Its contribution is therefore not simply a call for more information integration, but a model of selective and context-dependent information presentation.

This distinction is important for a cross-infrastructure platform because different actors require different forms of visibility. A port authority may need a system-level overview, an infrastructure operator may require technical status and timing information, and a crisis-management actor may need information relevant to escalation and public consequences. More information is therefore not necessarily more useful. The information must be filtered, contextualized, and presented in relation to the recipient's responsibilities.

The limitation of Luukkala et al.'s contribution is that the study develops a conceptual model rather than an implemented and user-validated prototype. It supports the principle of role- and context-sensitive information provision, but it does not establish how contextual relevance should be agreed across autonomous organizations or how such filtering would operate under real port-governance conditions.

Therrien et al. (2024) provide an empirical bridge between common-operating-picture technology and collaborative governance. Through 15 semi-structured interviews with public- and private-sector security professionals participating in the London Common Operating Picture, they compare two interpretations of a common operating picture, an information warehouse and a relational trading zone. Their findings support the second interpretation. The recurring common-operating-picture process functions as a space in which boundary spanners connect organizations, develop shared meanings, and build relationships of trust around information sharing and coordination.

The study therefore concludes that the value of a common operating picture lies not only in the information it contains, but also in the recurring collaborative relationships through which that information is exchanged and interpreted.

Brucherseifer et al. (2021) examine digital twins as potential resilience instruments for critical infrastructures and derive a conceptual framework from infrastructure, crisis-management, and resilience requirements. Their framework combines a virtual replica, smart analytical tools, virtual clones, scenario recording, and a human-operated control center that could support both normal operations and crisis situations. Four design principles are especially relevant. These principles are human-in-the-loop control, parsimonious modelling with explicit treatment of uncertainty, preparation for complexity and emergent behavior, and safe experimentation and training.

The authors also identify the integration of heterogeneous and uncertain data sources and system models, platform scalability, and reliability as central implementation challenges. They present federated digital twins as a promising alternative to a single system intended to solve every problem. This provides a more precise technical reference for EU-IDRP, particularly for human oversight, scenario analysis, and federated system design. Nevertheless, the proposed framework remains conceptual. It does not determine the institutional ownership, access rules, accountability arrangements, or inter-organizational data agreements required in the Port of Rotterdam.

Previous studies therefore establish that shared information infrastructures can support monitoring, forecasting, and coordination, but that their value depends on context-sensitive filtering, collective interpretation, recurring interaction, and human judgement. A common information base is therefore considered a possible input to coordination, and it is not equivalent to common situational understanding.

What still remains unresolved is how these conditions can be created across autonomous port and infrastructure organizations that use different systems, interpret events from different operational positions, and retain different responsibilities.

The interviews consequently examine what actors consider a useful shared picture, which information must be role-specific and actionable, and whether EU-IDRP could support shared understanding rather than simply introduce another information display.

3.4 Data sharing, trust, ownership, and information governance

Following the concept of situational awareness, a cross-infrastructure digital resilience platform also depends on access to relevant data. Yet data sharing among infrastructure actors is not a simple technical matter. Such practice raises questions of trust, confidentiality, commercial sensitivity, cybersecurity, liability, ownership, access control, data quality, and the use of derived insights. These questions are all particularly important in ports, especially where operational data may reveal vulnerabilities, business-sensitive information, or security-relevant dependencies.

Bharosa et al. (2010) provide particularly relevant empirical evidence because their study examines six multi-agency disaster-response exercises conducted in the Port of Rotterdam, each involving approximately 30 participants. Using participant observation and questionnaire surveys, they analyse barriers to information sharing at community, agency, and individual levels. Although participants broadly recognized the importance of sharing information, relief workers were frequently more concerned with receiving information from others than with providing information that might benefit the wider response network.

The study finds that incentives to share, understanding other organizations' work processes, and the usability of information systems have positive effects on information sharing and coordination. The findings are formulated as six grounded propositions for system designers and policymakers. The implication for platform feasibility is that technical connectivity does not create reciprocal information exchange by itself. Participation must generate recognizable value, fit existing operational processes, and enable users to provide and receive relevant information without creating excessive burden.

Rotterdam-specific cyber-resilience research reinforces this conclusion. Punt et al. (2023b) analyze cyber-risk governance through 18 semi-structured interviews, 15 participatory observations, and 46 policy and legal documents. They find that many existing strategies remain focused on protecting computer systems, while anticipatory and recovery-oriented practices are often informal and insufficiently coordinated. Limited information exchange, insufficient knowledge, differing understandings of cyber resilience, incomplete regulation, and weak economic incentives constrain collective preparedness.

The study therefore shows that reluctance to exchange cyber-related information is embedded in wider institutional, organizational, and incentive structures rather than being only a technical-security concern. Even where actors recognize their mutual exposure, information sharing remains dependent on perceived benefit, trusted arrangements, clear responsibilities, and the management of legal and reputational risk.

Cybersecurity data is especially sensitive because it may reveal vulnerabilities, incidents, or weaknesses in operational technology and information systems.

Data governance literature helps specify possible safeguards. Delacroix and Lawrence (2019) discuss data trusts as a way to move beyond one-size-fits-all data governance and simple ownership models. Although not specific to ports or critical infrastructure, this perspective can be useful because it suggests that trust can be institutionalized through stewardship arrangements, access rules, permitted use, and accountability.

European data regulation also shapes this governance environment. The Data Governance Act provides a framework for data-sharing mechanisms and data intermediation services (European Parliament & Council of the European Union, 2022c). The Data Act provides legal context for fair access to and use of data, including issues related to interoperability and data access (European Parliament & Council of the European Union, 2023).

For a cross-infrastructure resilience platform, data governance must really answer several practical questions. What data is shared, and at what level of aggregation? Who can access raw data, processed indicators, or alerts? Who owns derived insights generated by models? How are confidentiality, cybersecurity, and liability handled? Can actors restrict visibility or withdraw data? What happens when data is incorrect, delayed, or misinterpreted? These questions are vital as they show why data sharing is not simply a platform feature. It is a governance condition.

Previous studies therefore establish that cross-organizational information sharing depends on reciprocity, operational fit, trust, permitted use, access control, and accountability. They also show that a shared system may fail to generate meaningful exchange when contributing organizations assume unequal risks or receive little practical benefit from participation.

What is still unresolved is which categories of disruption information port actors would regard as sufficiently useful to justify sharing, where they would draw boundaries around sensitive data, and which safeguards would make participation acceptable. The literature does not establish in advance that the most valuable information is necessarily the most sensitive in every setting; this relationship must be examined empirically rather than assumed.

The interviews consequently examine what actors would share, what they would withhold, how they understand data ownership and derived insights, and which access, authorization, and governance arrangements they consider necessary for EU-IDRP.

3.5 Interoperability as a socio-technical governance condition

Interoperability is often treated as a technical issue, systems must exchange data through compatible interfaces, formats, and standards. Such concept, for a cross-infrastructure digital resilience platform is obviously considered necessary but it is still quite insufficient.

The literature on crisis and disaster management used for this research shows how interoperability also has semantic, organizational, procedural, legal, and relational dimensions. The idea is that actors must not only connect systems, but they must also interpret information similarly, align workflows, and as well operate under different compatible set of rules.

In their analysis of the Queensland disaster-management system, Eslami Andargoli et al. (2013) examine how several organizations can collaborate while relying on heterogeneous systems. Using an enterprise architecture perspective, they describe interoperability through three connected dimensions. Technical interoperability enables computer systems and services to exchange information. Semantic interoperability gives the exchanged information a shared meaning across the organizations involved. Organizational interoperability connects this exchange to compatible goals, processes, and collaborative arrangements. Together, these dimensions link technical exchange with common interpretation and coordinated action.

This specific distinction is highly relevant for a port resilience platform. That is, terms such as incident, disruption, availability, criticality, or dependency can in principle mean different things to different actors and if these meanings are not completely aligned, data exchange may produce confusion rather than coordination.

Legal and policy sources add a further dimension. The European Maritime Single Window environment illustrates that maritime information exchange increasingly depends on harmonized digital reporting interfaces (European Parliament & Council of the European Union, 2019). On this theme, the electronic freight transport information regulation similarly shows that European logistics policy is moving toward digital exchange of freight information

between economic operators and competent authorities (European Parliament & Council of the European Union, 2020). These are important regulations that are not necessarily resilience-platform regulations, but they illustrate the actual wider policy movement toward digitalized and interoperable information exchange in maritime and logistics systems.

The Data Act and Data Governance Act reinforce this point by making data access, interoperability, metadata, and data-sharing mechanisms part of the broader European digital governance context (European Parliament & Council of the European Union, 2022c, 2023). These regulations do not actually provide a ready-made interoperability solution for the port, but they pressure and strengthen the institutional relevance of interoperable data-sharing arrangements.

Interoperability should therefore be treated as a socio-technical governance condition. Technical APIs and data standards are necessary, but they must be embedded in shared definitions, operating procedures, legal bases, access rules, and organizational workflows. In a port environment, this is especially important because actors may use different systems, operate at different time scales, follow different procedures, and be governed by different legal obligations.

It is now important to note that a feasible platform must therefore support interoperability without forcing all actors into one single centralized system.

For the empirical analysis, interoperability can be examined through questions such as the following:

Can relevant systems exchange data? Do actors use compatible definitions? Are escalation procedures aligned across organizations? Is there a legal basis for sharing specific categories of information? Are there trusted interfaces between operational, tactical, and strategic levels? These questions connect technical platform design directly to governance feasibility.

3.6 Governance and coordination of cross-infrastructure disruption management

Following the discussion on interoperability, it is now important to address the governance and coordination conditions that make cross-infrastructure disruption management possible. Interoperability is not only a matter of connecting systems or exchanging data, but it also depends on whether actors have compatible responsibilities, shared procedures, trusted coordination spaces, and clear decision-making arrangements. The governance literature becomes a central part of the conceptual background.

If infrastructure interdependencies can create the possibility of cascading disruption, governance therefore can determine whether actors might collectively manage those specific risks. Interdependent infrastructures are difficult to govern because authority, ownership, expertise, operational capacity, and data are very distributed across different organizations. Public authorities may carry responsibility for safety, continuity, or crisis management, while private and semi-private operators control assets, systems, and operational information. The result of this situation is a governance setting in which no single actor has total complete authority, information, or implementation capacity.

OECD (2019) claims for a system-based approach to critical infrastructure resilience. That is, rather than focusing just on asset protection, governments and operators would need to take into consideration as well interdependencies, essential service continuity, public-private cooperation, and cross-sector effects. This specific policy framing is important because it recognizes that critical infrastructure resilience does require coordination across sectors and levels of governance. Still, it also points to persistent and continuous challenges, that is, information sharing, trust, investment incentives, and the allocation of responsibilities between governments and infrastructure operators.

Huck et al. (2021) provide the closest Rotterdam-specific examination of this governance challenge. Based on 26 semi-structured interviews and documentary analysis, they investigate the municipality's role in managing interdependent urban-infrastructure risks. They find that resilience is constrained by distributed control, divergent sectoral understandings, restricted information exchange, and the time and resources required for cross-sector cooperation. The authors conclude that networked resilience requires clearer role allocation, cross-sectoral budgeting, and stronger links between local, regional, and national governance. The study's limitation for the present thesis is that it examines urban-infrastructure governance broadly rather than the adoption and operation of a shared digital coordination platform.

The governance challenge is therefore intensified by public-private interdependence. Infrastructure operators often possess detailed operational knowledge and control key assets, but they may have commercial, reputational, legal, or security reasons not to share sensitive information. Public authorities may have legal mandates but limited direct control over privately operated infrastructure or digital systems. This becomes relevant as it creates a gap between formal responsibility and practical control. The idea is that actors may be expected to contribute to collective resilience, but their incentives, obligations, and risk perceptions may just not naturally align.

Considering that cross-infrastructure risks cut across a wide set of organizational boundaries, collaborative and network governance provide very important theoretical lenses that should be taken into account. Collaborative governance focuses on how public and private actors engage in collective decision-making or joint action when no single actor can solve a problem alone. Network governance focuses on the structure and management of interorganizational networks. Together, these literatures help explain why cross-sector coordination requires trust, inclusion, facilitation, shared problem framing, institutional design, and attention to power asymmetries.

Ansell and Gash (2008) derive a contingency model from a meta-analysis of 137 collaborative-governance cases across multiple policy sectors. They identify prior conflict or cooperation, participation incentives, power and resource imbalances, facilitative leadership, and institutional design as conditions shaping the prospects for collaboration. Within the collaborative process, face-to-face dialogue, trust building, commitment, shared understanding, and achievable intermediate outcomes can generate a reinforcing cycle of cooperation.

The authors also caution that much of the underlying collaborative-governance literature evaluates process outcomes rather than final policy performance. Applied to EU-IDRP, the framework therefore suggests that participation cannot be inferred from technical usefulness alone. Actors must perceive their interdependence, have meaningful incentives and voice, and trust both the rules and the leadership of the collaborative process.

Emerson et al. (2012) broaden the analysis by presenting collaborative governance as a regime shaped by system context, collaborative dynamics, action, impacts, and adaptation. This is useful because governance arrangements cannot be reduced to a single agreement or one-off design choice. They must be understood as evolving arrangements that adapt to changing risks, regulations, technologies, and actor relationships. In this sense, coordination across infrastructures is not only created once, but must be maintained over time through repeated interaction, learning and adaptation.

Provan and Kenis (2008) shift attention from the collaborative process to the structural governance of whole organizational networks. They distinguish three principal modes. Shared participant governance, governance by a lead organization, and governance through a separate network administrative organization. No mode is inherently superior. Its effectiveness depends on conditions such as the level of trust, the number of network members, agreement on network goals, and the need for network-level competencies.

The three modes also involve persistent tensions. These include efficiency versus inclusion, internal versus external legitimacy, and flexibility versus stability. For EU-IDRP, this typology makes ownership and operation an empirical rather than merely technical question. A participant-governed arrangement, a Port Authority-led model, and an independent coordinating entity would distribute authority, inclusion, accountability, and legitimacy differently.

A Rotterdam-specific illustration is provided by Chandra and van Hillegersberg (2018), who analyze the Port Community System through a longitudinal case study of governance across successive lifecycle stages. They examine governance mechanisms, governance aspects, actor roles, and governance models, finding that Rotterdam's port collaboration moved through three complete governance lifecycles and entered a fourth after the establishment of Portbase. During the two most recent lifecycles, the collaboration retained a network administrative organization model.

The study demonstrates that a shared port information system requires governance that evolves as the collaboration and system mature. EU-IDRP would perform a different function from the logistics-oriented Port Community System, but the case provides direct evidence that inter-organizational digital infrastructure in Rotterdam must be institutionally organized, maintained, and adapted over time. It also provides an empirical bridge between Provan and Kenis's governance typology and the platform context of the present thesis.

The collaborative and network governance literature therefore suggests that coordination depends on whether collaboration is structured in ways that are inclusive, legitimate, adaptive, and workable. It has to be more than stakeholder engagement. This means examining who should participate, who should convene, who is trusted, whose data and expertise matter, and how disagreements about access, authority, or responsibility are managed.

Crisis-management literature adds another relevant layer because cross-infrastructure disruption often becomes most problematic when situations are uncertain, time-sensitive, and multi-actor. In these moments, information must be interpreted quickly, responsibilities must be clear, and decisions must be taken under uncertainty. The crisis-management literature therefore helps distinguish between information sharing, shared situational awareness, advice, escalation, and decision authority.

Comfort (2007) argues that crisis management involves cognition, communication, coordination, and control. This specific framing shows that information alone is therefore insufficient. That is, actors must be able to recognize what is happening, communicate across organizational boundaries, coordinate actions, and exercise control within legitimate authority structures. For this reason, shared information does not automatically create collective cognition or coordinated control.

Following, Wolbers (2022) develops the concept of distributed sensemaking through a case study of the multi-level command response to the 2019 Utrecht terrorist attack. The analysis shows that different teams can retain partial and conflicting representations of the same event even when relevant information is available elsewhere in the command structure. Wolbers identifies interdependence, sensitivity to operations, plausibility, hierarchy, and identity as five factors shaping whether actors revise or retain an existing interpretation.

The central conclusion is that sensemaking failures are not corrected by information updates alone. They are shaped by the social and organizational structures through which different perspectives are voiced, questioned, and combined. For a cross-infrastructure platform, this means that a common information layer must support reciprocal interpretation and exposure to different operational perspectives rather than assume that centralizing information will automatically generate common understanding.

These governance and sensemaking perspectives also imply that a new platform would enter an existing coordination environment consisting of formal mandates, bilateral relationships, sector-specific systems, operational routines, and crisis-management procedures. The reviewed literature establishes that institutional fit and complementarity are important, but it does not demonstrate whether a distinct coordination gap exists in Rotterdam between routine operational handling and formal crisis escalation. Nor does it establish whether a digital platform would improve coordination in such a space or merely duplicate existing arrangements. These are therefore empirical questions for the interviews rather than conclusions of the literature review.

Previous studies therefore establish that cross-infrastructure coordination requires both a legitimate governance structure and social processes that enable participation, trust, shared understanding, and distributed sensemaking. A digital platform may support these processes, but it cannot independently create agreement on responsibilities, authority, information use, or collective action.

What still remains unresolved is which governance mode could credibly convene Rotterdam's public and private actors, how such an arrangement would relate to existing mandates and systems, and whether a shared digital layer could support coordination without acquiring command authority.

The interviews consequently examine who should participate, who could convene or operate the platform, how decision rights should be protected, and how EU-IDRP could be embedded in existing operational and crisis-management arrangements.

4. Findings

4.1 From literature to interview findings

This chapter presents the findings of the study. The chapter is structured in two steps. First, it presents a set of contextual findings derived from the literature review. These findings do not describe interview results yet, but they clarify the governance and institutional environment in which a cross-infrastructure digital resilience platform would have to be introduced. This is important because the feasibility of such a platform cannot be assessed only as a technical question. It also depends on existing actor responsibilities, crisis-management arrangements, digital infrastructures, regulatory pressures, and data-sharing conditions.

Second, the chapter presents the interview findings. These findings were developed through a first cycle of descriptive and ad-hoc coding, followed by a second cycle of analytical coding. The interview findings are organized thematically and cut across actor types, including rail business continuity, rail operations and net-centric working, public crisis management, port authority innovation, cyber-resilience information sharing, electricity distribution, infrastructure modelling, automated terminal operations, and interoperability research.

The chapter therefore first outlines the institutional and digital setting of platform feasibility, before turning to four cross-cutting interview findings. It then closes with a concise case-specific synthesis showing how cross-infrastructure disruption materializes within the operational setting of the Port of Rotterdam.

4.2 Literature based case context

Before turning to the interview findings, this section presents the contextual findings derived from the literature review. These findings are not treated as general background, but as part of the empirical basis for assessing platform feasibility. They clarify the institutional, infrastructural, digital, and regulatory setting in which a cross-infrastructure digital resilience platform would have to operate in the Port of Rotterdam.

The first contextual finding is that the Port of Rotterdam is embedded in dense cross-infrastructure dependencies. Digital systems are now part of energy networks, transport systems, communication services, water management, and port logistics, meaning that disruptions triggered by extreme weather, cyberattacks, technical failures, or geopolitical tensions may move beyond one sector and develop into wider systemic crises (Balakrishnan et al., 2024; Liu et al., 2022; Rydén Sonesson et al., 2021; Zhang et al., 2024). In this sense, the Port of Rotterdam is not only a maritime node, but also a socio-technical environment in which transport, energy, digital, industrial, and public-safety systems are connected.

The second contextual finding is that Rotterdam already has a populated coordination and digital environment. Dutch crisis-management arrangements, net-centric working, LCMS, Portbase, cyber-resilience initiatives, and European maritime and freight-data initiatives already shape how information is produced, shared, and acted upon.

The third contextual finding is that the regulatory environment, especially NIS2 and CER, increases the relevance of resilience, cybersecurity, incident reporting, risk management, and cross-sector cooperation. However, these directives do not provide a complete governance model for a cross-infrastructure digital resilience platform. They create pressure and direction, but they do not decide who should own, operate, fund, access, or act upon such a platform.

Together, these contextual findings prepare the ground for the interview findings. They show why the feasibility of a cross-infrastructure digital resilience platform is not only a technical question, but also a governance and organizational question.

4.2.1 The Port of Rotterdam as a cross-infrastructure resilience setting

The Port of Rotterdam is a relevant case for studying cross-infrastructure digital resilience because it combines maritime transport, hinterland logistics, industrial production, energy flows, digital systems, and urban functions. As Europe's largest seaport and a major hub for container traffic, energy imports, and industrial production, it depends on surrounding infrastructures while also hosting critical assets itself (Gemeente Rotterdam, 2016; Huck et al., 2021; Lu & Qiu, 2025; Mohsendokht et al., 2026). Disruptions in electricity or ICT networks may affect terminal operations, traffic management systems, pumping stations, industrial processes, and wider supply-chain continuity.

This makes Rotterdam a port-system environment in which cascading effects are especially relevant. Studies of Rotterdam's infrastructure networks show dense interdependencies and the potential for cascading failures across sectoral and spatial boundaries (Huck et al., 2021; OECD, 2019; Spaans & Waterhout, 2017). More specifically, research on flood and cyber resilience at the Port of Rotterdam highlights the challenge of coordinating authorities, infrastructure operators, and private actors across vertical, horizontal, and territorial governance dimensions (Punt et al., 2023a, 2023b; Rydén Sonesson et al., 2021).

The broader port-resilience literature also supports this framing. Port systems are increasingly studied as complex and interdependent infrastructure environments, where disruptions can affect maritime flows, hinterland connections, supply chains, and regional economies (Mohsendokht et al., 2026; Tsoufas, 2026; Zhang et al., 2024). Disruptions at ports can lead to delays, cargo rerouting, supply shortages, and broader economic consequences (Cao et al., 2025; Mohsendokht et al., 2026; Tsoufas, 2026). This matters for the present study because a digital resilience platform would not only need to support individual organizations but would also need to help actors understand cross-infrastructure consequences.

The literature on critical infrastructure interdependencies further strengthens this point. Existing work has clarified how failures can propagate across infrastructure systems and why integrated risk management becomes necessary when infrastructures are functionally, geographically, digitally, or organizationally linked (Arvidsson et al., 2021; Balakrishnan et al., 2024; Liu et al., 2022; Rydén Sonesson et al., 2021). Cross-infrastructure digital resilience platforms are therefore presented in the literature and practitioner guidance as tools that may support situational awareness, early warning, and coordinated response by integrating data from different operators, representing interdependencies, and providing decision support for cascading disruptions (Balakrishnan et al., 2024; C40 Cities Climate Leadership Group, 2019; Liu et al., 2022).

However, the same literature also implies a governance limitation. Digital platforms do not operate in an institutional vacuum. They have to fit into existing governance arrangements, organizational responsibilities, and regulatory requirements (OECD, 2019; Rydén Sonesson et al., 2021). For that reason, the Port of Rotterdam is not only a technically complex setting, but also an institutional setting in which platform feasibility depends on actor responsibilities, data-sharing rules, trust, authority, and operational fit.

4.2.2 A distributed actor landscape shapes platform feasibility

The actor landscape around the Port of Rotterdam is highly distributed. The Port of Rotterdam Authority is one of the central actors in this landscape. As a port authority, it is involved in the management and long-term development of the port area, infrastructure provision, safety, strategic positioning, and the competitiveness of the port cluster. Literature on port authorities describes their role in landlord-port contexts as providing and managing infrastructure, granting access to private operators through leases or concessions, and shaping the competitive environment of the port cluster (Dooms et al., 2013; Tijan et al., 2021). In Rotterdam, this means that the Port Authority is not only a commercial actor, but also an institutional actor positioned between public responsibilities, private firms, infrastructure development, and strategic port governance.

At the same time, the Port Authority is only one part of the wider actor landscape. Public authorities, including the municipality, the safety region, national government bodies, water authorities, and agencies involved in transport, security, infrastructure, and crisis management, become relevant when disruptions have public-safety, environmental, societal, or cross-territorial consequences. Huck et al. (2021) show that Rotterdam's infrastructure resilience depends on network management across local, regional, national, public, and private actors. This supports the conclusion that resilience in Rotterdam cannot be governed through one institutional center alone.

Infrastructure operators are another central group. These include actors responsible for rail, road, electricity, water, pipelines, digital infrastructure, and other critical services that support port functioning. Their importance lies in the fact that they hold operational knowledge, infrastructure-specific data, continuity procedures, and domain-specific responsibilities. A disruption in one infrastructure may affect others, but the authority to act usually remains with the responsible operator or single competent authority. This creates a governance environment in which shared visibility may be useful, while decision rights remain distributed.

Terminal operators, logistics firms, industrial companies, and shipping-related actors add another layer. They are directly involved in cargo handling, transport planning, port operations, business continuity, and private operational decision-making. Many of these actors operate under commercial constraints and may hold sensitive operational or business data. Their participation in a shared platform would therefore depend on trust, clear access rules, data protection, and a convincing operational value proposition.

Digital and cyber-security actors form a further layer of the ecosystem. Portbase and the Port Community System are especially relevant because they show that Rotterdam already has experience with shared digital infrastructures. Chandra and van Hillegersberg (2018) analyze the governance of Rotterdam's Port Community System and show how inter-organizational port systems require governance arrangements, actor roles, lifecycle development, data governance, and institutional embedding. This is important because a cross-infrastructure resilience platform would also need governance arrangements, but its function would differ from a logistics-oriented Port Community System. Whereas a Port Community System supports logistics, administrative processes, and operational information exchange, a resilience platform would focus on disruption awareness, interdependencies, scenario analysis, and cross-infrastructure coordination.

Cyber-resilience initiatives are also relevant because they show that digital disruption preparedness is already being organized in the Port of Rotterdam. Research on cyber resilience in Rotterdam points to the importance of information exchange, public-private cooperation, and organizational arrangements such as cyber-security communities or information-sharing structures (Punt et al., 2023b). These initiatives provide a useful reference point for this thesis because a cross-infrastructure platform would need to relate to existing arrangements for information sharing and disruption coordination.

The overall contextual finding is therefore that the Port of Rotterdam is a distributed governance environment. Different actors hold different forms of authority, knowledge, data, responsibility, and operational capacity. This does not make a platform impossible, but it does mean that platform feasibility must be assessed as a governance and organizational question. A platform would have to respect actor responsibilities, data ownership, public-private boundaries, and existing institutional arrangements.

4.2.3 Rotterdam's coordination and digital environment is already populated

A second contextual finding is that a cross-infrastructure platform would need to fit into an already existing coordination and digital environment. Three types of arrangements are especially relevant: Dutch crisis-management arrangements, port-specific digital systems, and wider European maritime and freight-data initiatives. Within Dutch crisis management, GRIP structures escalation, net-centric working organizes information exchange, and LCMS provides the digital environment used to maintain a shared situation picture. Port-specific systems such as Portbase support information exchange in logistics and maritime operations. European initiatives promote digital reporting, interoperability, and cross-organizational data flows.

In the Netherlands, safety regions coordinate regional crisis preparedness and response among emergency services, municipalities, and other crisis partners. For the Port of Rotterdam, this role lies with the Rotterdam-Rijnmond Safety Region. The *Gecoördineerde Regionale Incidentbestrijdingsprocedure* (GRIP; Coordinated Regional Incident Response Procedure) structures operational and administrative scale-up during complex incidents. It sets out which multidisciplinary teams are activated, where coordination takes place, and which authority is involved. A GRIP level therefore reflects the coordination required by the situation. Scale-up decisions draw on incident information and professional judgement (Cools et al., 2017; Lukassen et al., 2023).

Net-centric working, known in Dutch as *netcentrisch werken*, concerns the organization of crisis information across this network. Each organization maintains a situation picture suited to its own role. Information exchange is coordinated, while the participating partners maintain a current shared picture. This picture supports joint assessment and decision-making across organizations and levels (Treurniet et al., 2023; Van de Ven et al., 2008).

The *Landelijk Crisis Management Systeem* (LCMS; National Crisis Management System) provides the digital support for this working method. Crisis partners use LCMS to share text, documents, and geographical information and to maintain the shared situation picture. The system is used by all Dutch safety regions and by a wider network of national and sectoral crisis partners (Treurniet et al., 2023). Net-centric working provides the organizational method, while LCMS provides its digital support. Research on LCMS also identifies the conditions under which crisis technology creates practical value. Regular use and support for sense-making are central. The system also needs to fit distributed decision-making and keep cognitive demands manageable (Groenendaal & Helsloot, 2021).

Beyond public crisis management, Rotterdam also uses shared digital infrastructure for port logistics. Portbase is the executive organization of the Port of Rotterdam Authority and the Port of Amsterdam. It operates the Dutch Port Community System (PCS), a shared digital platform through which port and logistics actors exchange information with one another and with public authorities (Portbase, n.d.). The Port Community System operated through Portbase is especially important. In Rotterdam, coordination and information exchange for freight flows are managed through Portbase's digital Port Community System, which offers services for core supply-chain processes and supports information exchange between logistics actors, port authorities, and other port users (Port of Rotterdam Authority, n.d.). Chandra and van Hillegersberg (2018) show that Rotterdam's Port Community System developed through governance lifecycles and inter-organizational collaboration. Their study also highlights the importance of data governance, user roles, access arrangements, and financial sustainability in shared port information systems.

This is directly relevant for a resilience platform because it shows that shared digital systems in Rotterdam are not only technical infrastructures; they are institutionally embedded systems with rules, roles, and governance arrangements. However, the Port Community System and a cross-infrastructure resilience platform would not serve the same function. The Port Community System primarily supports logistics, administrative processes, and operational information exchange, while a cross-infrastructure resilience platform would be oriented toward disruption awareness, cascading effects, and coordination across infrastructure domains.

Wider European initiatives form another layer of this environment. The Common Information Sharing Environment (CISE) is a decentralized network that connects the systems of maritime authorities and supports controlled information exchange across borders and sectors (European Commission, n.d.). The European Maritime Single Window environment (EMSWe) harmonizes reporting for ships through national single-entry points and became applicable on 15 August 2025. The electronic Freight Transport Information (eFTI) framework supports digital freight documentation across transport modes. Member State authorities must accept information shared through certified eFTI platforms from 9 July 2027.

These initiatives serve maritime surveillance, ship reporting, and freight documentation. Their presence shows that Rotterdam's wider environment already contains several digital information-sharing arrangements. The empirical question therefore concerns the specific coordination value that EU-IDRP could provide within existing systems, responsibilities, routines, and information practices.

4.2.4 NIS2 and CER create pressure but not a complete governance model

A third contextual finding concerns the regulatory environment. The relevance of a cross-infrastructure digital resilience platform is strengthened by EU regulation, especially the NIS2 Directive and the Critical Entities Resilience Directive. These directives increase attention to resilience, cybersecurity, incident reporting, risk management, and cross-sector cooperation.

The NIS2 Directive establishes measures for a high common level of cybersecurity across the European Union. It expands the scope of EU cyber-security obligations and strengthens requirements related to cyber-risk management, incident reporting, supervision, cooperation, and resilience in critical and important sectors (European Parliament & Council of the European Union, 2022a). For the Port of Rotterdam, NIS2 matters because port operations depend on digital systems, cyber-security practices, logistics data exchange, ICT services, and actors that may fall within essential or important sectors. Its relevance is therefore not limited to IT departments. It also concerns the organizational and governance conditions under which cyber risk is managed across interconnected infrastructure and service providers.

The Critical Entities Resilience Directive addresses a broader all-hazards resilience agenda. It aims to strengthen the resilience of entities that provide essential services and to improve their ability to prevent, resist, absorb, respond to, recover from, and adapt to incidents (European Parliament & Council of the European Union, 2022b). This is relevant for a port ecosystem because transport, energy, water, digital infrastructure, and other essential services may be interconnected in ways that make disruption management a cross-sector problem. The CER Directive therefore supports the broader argument that resilience must include physical, organizational, and societal dimensions of disruption. In this sense, NIS2 and CER support the relevance of the thesis problem. They require more systematic attention to risk management, resilience measures, information sharing, incident reporting, and public-private cooperation. They also reflect a broader shift in critical infrastructure governance from isolated asset protection toward resilience across interdependent systems (OECD, 2019).

However, these directives do not automatically define the governance arrangements for a cross-infrastructure digital resilience platform. They do not determine who should own such a platform, who should operate it, who should fund it, who should access which information, or how platform outputs should relate to legal decision rights and crisis-management responsibilities. The regulatory context therefore creates both pressure and uncertainty. For this reason, NIS2 and CER should be understood as enabling pressures rather than as a complete governance solution. They strengthen the relevance of cross-infrastructure resilience, but they leave open the core empirical question of this thesis: how existing disruption-management practices, information flows, and governance arrangements shape the feasibility and potential added value of a cross-infrastructure digital resilience platform in the Port of Rotterdam context.

4.2.5 Implication for the interview findings

The contextual findings presented above establish the setting in which the interview findings should be read. The Port of Rotterdam is a strategic and interdependent infrastructure environment; its actor landscape is distributed; its coordination and digital systems are already populated; and its regulatory context creates pressure for resilience without resolving platform governance.

This means that the interview findings should not be interpreted as responses to a blank-slate platform proposal. Instead, they show how actors experience and evaluate platform feasibility within an already complex governance environment. The following sections therefore examine how this environment appears in practice: first, through

the grey space between routine operational incidents and formal crisis escalation; second, through the difference between partial visibility and shared system-level awareness; third, through interoperability as socio-technical alignment; and fourth, through the tension between the value and sensitivity of shared information.

4.3 Introduction to the interview findings

Building on these contextual findings, the following sections present the interview findings. The interview material shows how the distributed actor landscape, populated digital environment, and regulatory pressure described above are experienced in practice by actors involved in disruption management, infrastructure operation, crisis coordination, cyber-resilience information sharing, and port innovation.

The interviews resulted in four main findings. First, cross-infrastructure disruption becomes a coordination problem before it becomes a formally declared crisis. Second, existing systems and communication channels provide useful partial visibility, but not shared system-level awareness. Third, interoperability is not only a technical issue, but also depends on shared meanings, compatible routines, aligned responsibilities, legal agreements, and organizational fit. Fourth, the information that would be most valuable for cross-infrastructure resilience is often also the information that organizations find most difficult to share.

These findings are presented thematically rather than by actor group. This makes it possible to show how similar governance and organizational issues appear across different infrastructures and institutional positions. After the four thematic findings, Section 4.4 consolidates the empirical observations that are specific to the Port of Rotterdam case.

Table 4.1 presents the final empirical findings, the number of validated quotation segments and the spread of evidence across actor profiles and institution types. The table is based on the final codebook. Quotations refer to validated quotation segments used in the final findings, while actor profiles refer to the distinct interview profiles represented in the evidence. Institution type refers to the broader institutional categories already introduced in the interview overview.

Table 4.1 Empirical findings, quotation segments and institutional coverage

Empirical finding	Validated quotation segments	Supporting evidence	Actor profiles	Institution types
Cross-infrastructure disruption becomes a coordination problem before it becomes a formal crisis	17	7	8	7
Existing systems create partial visibility, but not shared system-level awareness	14	6	8	7
Interoperability is socio-technical alignment	17	5	6	6
The most valuable information to share is often also the most sensitive	20	6	9	8

4.3.1 The grey space between routine operational incidents and formal crisis escalation

The first presented finding is that cross-infrastructure disruption becomes a coordination problem before it becomes a formal crisis. According to the final codebook, coded material supporting this finding was present in eight out of the ten interviews. Represented by 17 validated segments (10 core and 7 supporting) across seven institution types. The supporting interview profiles were rail operations and net-centric working (I2), rail business continuity and resilience (I3), automated terminal IT operations (I4), cross-sector infrastructure modelling (I5), electricity-distribution risk management (I6), port-authority innovation (I7), public crisis management and network governance (I8), and port cyber-resilience information sharing (II0). Across this evidence, actors did not describe the Port of Rotterdam as a setting in which incidents remain neatly contained within one organization or infrastructure. They pointed to dependencies between rail, road, waterborne transport, energy, digital systems, cybersecurity, terminal operations, and public crisis-management structures. A disruption may therefore start locally while quickly becoming operationally relevant to other actors.

This theme was visible across examples in which a locally managed incident became operationally relevant to another transport mode, infrastructure, or port process. Because the concrete configuration of these Rotterdam interfaces is case-specific, these examples are consolidated in Section 4.4.

The central empirical issue is therefore located between two existing forms of response. On one hand, routine incidents are handled through operational organizations, control centers, existing contacts, calls, and practical problem-solving. On the other hand, major crises can activate formal crisis-management structures and public authority. Between these two ends, the interviews point to a middle layer where disruption effects may already be interconnected, while the response is still largely organized through operational coordination, existing relationships, and escalation thresholds.

On such theme, a rail business-continuity actor described this middle layer most directly. That is, smaller disruptions, in this account, are handled by operational organizations and 24/7 actors, while very large disasters involve formal authority: “If it’s a smaller disruption, then... operational organizations... find each other, really the 24-7 people... But if it’s a really big disaster, then it’s the mayor, but there’s nothing in between. It’s small or big... for the cases that are in between... there’s just operational coordination... but not... a strategic view on the situation.” [SEG009] This quotation shows that the existing response structure is divided between operational coordination and formal escalation, while cross-infrastructure situations in between may lack a complete shared strategic view.

On this line, a public crisis-management actor from a rail institution described a similar tension from the perspective of organizational routines. ProRail, as the organization responsible for the Dutch railway infrastructure, is quite used to handling many smaller incidents, but this experience does not automatically create a structure for cross-organizational, middle-layer disruption management, “Because ProRail has so many small accidents, they are very good in handling them. Crisis management has become something for bigger crisis... But by doing so you don’t have much look on that smaller crisis... fast coordination, rapid decision making, network governance, those things are not built in a normal line management organization.” [SEG010] This quotation helps clarify why the grey space is here important. That is, smaller crises may still require rapid coordination and networked decision-making, even when they do not formally activate the full crisis-management apparatus.

The same public crisis-management perspective also shows that the grey space is shaped by distributed authority. As the actor explained, “Every organization, like ProRail, has its own background and legislations of where they are responsible for the crisis... the safety region is like a technical commander, but cannot say you have to do

that... in the functional column, there are about 42 different organizations who have their own authorities.” [SEG014] This quotation adds an institutional layer to the finding as it shows that even when crisis structures or coordinating bodies exist, the involved organizations keep their own responsibilities, mandates, and legal authority. Middle-layer coordination therefore depends on aligning actors that remain responsible within their own organizational and legal domains.

The interviews then move from authority and escalation to the practical ways in which coordination is carried out. A rail netcentric-working actor added that much of this coordination is still carried by people rather than by systems that support shared coordination. As this actor explained, “Coordination is not mainly by systems but mostly by people with a phone, pen and paper, and tools like SpoorWeb... to inform people, but not to coordinate actions in the way you mean... There is a lot of coordination and many calls, but a lot of it is ad hoc. We have structures, but we do not have systems to support them.” [SEG011] This points to a practical limitation within the current disruption-management environment. That is, there are existing relationships, structures, and tools, but the coordination work in this described grey space often still depends on ad hoc communication and personal or organizational routines.

The interview from Stedin also supports this same threshold logic from the perspective of electricity distribution and enterprise risk management. That actor explained that different organizations retain responsibility for many risks, but that the situation does change once a threat reaches a societal level: “To a certain extent, we are the ones that can decide... what we do and how we manage our risk... But with such a law... if that threat hits a certain level, the government takes over... because it’s a societal disruption.” [SEG016] This shows that formal public authority becomes more prominent beyond a certain level of disruption. Before that point, coordination depends more on existing agreements, organizational responsibilities, and the ability of actors to align their actions.

Across these interviews, the grey space appears as a coordination situation between ordinary operational handling and formal crisis escalation. In this space, actors may already need to coordinate across infrastructures, but the available arrangements remain partly operational, partly informal, and partly dependent on thresholds for escalation. The finding therefore describes a middle layer in which cross-infrastructure consequences are emerging, while shared strategic overview, mandate alignment, and joint response arrangements remain uneven across actors.

4.3.2 Existing systems produce partial visibility, but not shared system-level awareness

Following, the second finding is that existing systems and communication channels produce useful partial visibility, but not shared system-level awareness. According to the final codebook, coded material supporting this finding was present in eight out of the ten interviews, comprising 14 validated segments (8 core and 6 supporting) across seven institution types. The supporting interview profiles were national crisis management and net-centric working (I1), rail operations and net-centric working (I2), rail business continuity and resilience (I3), automated terminal IT operations (I4), electricity-distribution risk management (I6), port-authority innovation (I7), public crisis management and network governance (I8), and port cyber-resilience information sharing (I10). Across these interviews, actors referred to incident-management tools, crisis-management systems, cyber-information-sharing groups, internal dashboards, operational communication channels, roundtables, phone calls, and informal networks. These arrangements therefore provide visibility for specific roles or communities, but the visibility remains bounded rather than system-wide.

The ProRail netcentric-working evidence is here particularly important because it shows both the presence and the limits of existing systems. One rail netcentric-working actor described SpoorWeb as a central source of

incident-management information, while also explaining that access is role-based: “SpoorWeb... is our incident-management tool... one central source of information for all participants on a need-to-know basis and, of course, role-based. Some players have all the information... But when you only have a task to manage, you have visibility of the task... but not all the information.” [SEG018] This type of visibility is therefore operationally meaningful, but it is not the same as system-level awareness across different organizations and infrastructures. That is, it gives actors what they need for their specific role, while wider cross-infrastructure understanding still remains more limited.

This distinction between role-based information and wider overview appeared repeatedly in the interviews. The problem described by actors was not simply whether a system exists, but how the information inside different systems is divided, filtered, accessed, and interpreted by different groups. The concept is that a system can support a specific operational task while still leaving other actors without a broader understanding of what is happening across the disruption environment.

The same previous actor connected this limitation to the absence of a common operational picture. The issue was described as organizational as much as informational: “We do not have a common operational picture of where we can do something... sources already internally available at ProRail but not brought together... every internal ProRail party is sitting on its own data. It is not the availability of data, but a real organization of power.” [SEG019] This quotation is central to the finding because it shows that the problem is not simply a lack of data. Data may already exist internally, but it remains distributed across organizational units, systems, responsibilities, and forms of ownership. That is, shared system-level awareness requires quite more than the availability of separate information sources.

The same problem becomes even more visible during multiple incidents. A rail netcentric-working actor explained that “when we have multiple incidents, we spend too much time getting a real common operational picture... Netcentric working... starts with a common operational picture... It would help us a lot. We are absolutely not there.” [SEG020] This quotation adds a practical crisis-management dimension to the finding. It shows that the absence of a common operational picture affects the time needed to understand the situation when several incidents or effects are happening at once. In that sense, partial visibility becomes especially problematic when disruption is no longer isolated.

Fragmentation of information channels

A second layer of this finding concerns the fragmentation of channels through which information moves. The interviews suggest that fragmentation is visible both in the systems that actors use and in the communication routes that are activated during disruption. Some information is located inside role-based operational systems, some is exchanged through crisis-management tools, some through cyber-specific communities, and some through direct calls, roundtables, WhatsApp, or personal contacts.

On this line, the port authority interview illustrates a similar pattern from the perspective of the Port of Rotterdam. That is, communication channels exist between managers, cybersecurity actors, the harbour master function, the CIO (Chief Information Officer) function, and FERM, but this does not yet amount to a shared platform for internal and external actors during a disruption. As a port authority innovation actor explained, “There is different communication channels between the managers... maybe even the Harbor Master... cyber security... CIO... FERM... but... we do not have it in place, a system or platform to use internally with external actors. The

communication is mainly done when the incident happens... through maybe a round table... phone.” [SEG023] This quotation highlights that the port has real communication arrangements that are currently in place, but they are fragmented and often activated around happening incidents rather than embedded in a shared cross-infrastructure operational picture.

A public crisis-management actor described this fragmentation through the relation between LCMS and ProRail systems. As the actor explained, “ProRail doesn’t use the LCMS... when all the emergency services are on that system and ProRail was not on the system, they have to telephone or WhatsApp... that’s a loss of information... You have to share your information in a real time connected system.” [SEG022] This quotation gives a concrete example of the problem. Different actors may be involved in the same disruption environment, but they are not necessarily connected to the same information system. As a result, information can move through phone calls or WhatsApp, which may be practical in the moment but can also create loss of information and reduce the possibility of a shared real-time picture.

FERM additionally provides another example of partial but valuable visibility. That is, the cyber-resilience information-sharing arrangement gives participating organizations a way to exchange signals, warnings, and indicators that are related and relevant to different cyber incidents. A cyber-resilience information-sharing actor explained: “We have a signal group with organizations that are part of FERM... a lot of situational awareness... when a mailbox... is compromised... or attacks from certain IPs or domains... we can share it in a group, and then organizations could anticipate.” [SEG024] This can support situational awareness within a cyber community, especially when different organizations need to anticipate attacks or risks of compromised systems. At the same time though, this is still a well-defined and domain-specific information-sharing community. That is, it does not automatically create a broader operational picture across energy, rail, road, shipping, terminals, and crisis-management authorities.

The interviews also show that shared awareness is not only defined as bringing information together. It is also about making information understandable and usable for actors who have different responsibilities. Moving on this line, the RWS netcentric-working evidence better sharpens the distinction between information and awareness. One actor stated: “There is lots of information. That’s not a problem. The only thing is to comprehend and to extract the essence... what the problem is... technical information doesn’t get you to the solution... stop, think what’s the shared problem?” [SEG026] This quotation points to sense-making and highlights its importance as an empirical requirement. Shared situational awareness depends on selecting, interpreting, and translating information into a shared understanding of the problem. Consequently, more data can even become a load if actors cannot really identify what the disruption means for them and for others.

Usefulness of information shared

A final layer of this finding concerns the type of information actors considered useful. Across the interviews, actors did not describe shared awareness as full access to all available data. They described it more practically as access to information that helps them understand consequences, timing, dependencies, and next steps. The information needs that have been identified by other actors confirm this point. That is, actors specifically asked for information that helps them act, such as the scale of an incident, the affected area, expected duration, operational consequences, root cause, timing, planning, location, and effects on other modalities.

On this theme, a rail business-continuity actor explained this concept in relation to cascading effects: “It would be very helpful if you could have some impression about what’s the impact, how big is the incident, what is the

area that is affected, and what is the expected time... and what will other modalities... do... a good forecast... and the way that parties will deal with it... could help reduce or prevent cascade effects.” [SEG028] This shows that shared system-level awareness is closely connected and related to actionability. That is, actors need useful information that helps them understand how a disruption may affect their own operations and how others are likely to respond.

An automated terminal IT actor described the same need in more operational terms. As the actor explained, “What is very key is that in the right frequency, you give a short notification on where you are, your root cause analysis... how much longer... and if you don’t know... tell when you will come with the next update... otherwise companies start calling each other and keeping each other from their work.” [SEG027] This quotation shows that shared awareness is also about timing and communication rhythm. Actors need updates that are frequent enough, specific enough, and useful enough to prevent parallel calls and additional workload.

The Stedin interview confirms this need for actionable information from the perspective of electricity distribution. As the actor explained, “We want to know the root cause. We want to know some planning... where are you? When do you expect to solve stuff? Because the moment that they... activate again, there will be a power shock to our network... we need to know... what’s your planning... so we can protect our network.” [SEG031] This quotation adds a further cross-infrastructure dimension. It shows that information about root cause, planning, and expected timing can be directly relevant for another infrastructure actor. In this case, Stedin does not need all available information, but it does need information that allows it to anticipate effects on the electricity network and protect its own system.

4.3.3 Interoperability as socio-technical alignment, not only technical integration

Moving on, the third finding is that interoperability is a socio-technical condition rather than only a technical integration problem. According to the final codebook, coded material supporting this finding was present in six out of the ten interviews, including 17 validated segments (12 core and 5 supporting) across six institution types. The supporting interview profiles were national crisis management and net-centric working (I1), rail operations and net-centric working (I2), cross-sector infrastructure modelling (I5), port-authority innovation (I7), public crisis management and network governance (I8), and interoperability research (I9). Through this evidence, technical connectivity was considered necessary but insufficient: actors also emphasized shared meanings, compatible routines, aligned responsibilities, legal conditions, accountability, and operational fit. Interoperability therefore emerged as a practical condition for collaboration among organizations that use different terms, systems, mandates, procedures, and decision-making routines.

The first layer that emerged from the interviews was semantic and organizational. One interoperability researcher expressed this most explicitly by describing interoperability layers as socio-technical: “For me, all of these layers are socio-technical... I see all of this as having human interaction as an element... semantic, syntactic, and organizational interoperability would all be evoked... do they mean the same thing when they talk about the grid? What is the grid to them? How do they define it?” [SEG034] This is relevant because it shows that interoperability begins already at the level of meaning. Before information can be used across organizations, actors need to understand whether they are using the same concepts in the same way. Terms such as “grid,” “disruption,” or “crisis” may appear self-evident within one organization, while carrying different meanings in another.

The MOVICI interview adds a modelling and data-coupling perspective to the same finding theme. A cross-sector infrastructure-modelling actor explained that technical coupling already depends on semantic agreement: “We’re realizing that this interoperability seems to be a great issue. We need to get the semantics right... not just what

variables actually mean and how they're represented, but how the data itself is represented... different encodings... different frequency of updates." [SEG033] This shows that even the technical side of interoperability contains interpretive choices. A variable, dataset, or model output must be meaningful to other systems and users. Different encodings, different update frequencies, and different representations of data can be dangerous as they create misalignment even when actors are willing to connect their systems.

The interviews also show that this semantic and technical alignment is tied to prior agreements between organizations. The same interoperability researcher added a legal and accountability layer to this issue, "In terms of building the interface, you would have to agree before building it... Are the data aligned syntactically and semantically? Are there legal and organizational agreements in place? Who will take accountability in case of a data leak?" [SEG044] This quotation brings together several layers of interoperability at once. It shows that building an interface also involves agreements about data alignment, legal responsibilities, organizational conditions, and accountability. In the interview material, interoperability therefore appears as something that has to be arranged before systems are connected, rather than only adjusted after connection.

The same issue appears as well in crisis-management practice. A rail netcentric-working actor described the problem as one of shared language across Dutch organizations: "We use the same terms and mean different things with them... we cannot let everybody look into the system directly. You have to translate, also from Dutch to Dutch. The meaning of crisis is different... for government, for ProRail, for NS, for Rijkswaterstaat and for the Port of Rotterdam." [SEG036] This quotation grounds semantic interoperability in day-to-day coordination. The actor describes translation as an operational task between organizations that may all work in Dutch but still attach different meanings to the same terms. In this account, interoperability concerns the ability to make information understandable across professional, organizational, and institutional boundaries.

A further layer concerns procedures, roles, and mandates. Organizational and procedural alignment was especially visible in the public crisis-management interview with ProRail. The actor explained that crisis-management organizations need to become more interoperable by aligning their procedures and roles: "Those crisis management organizations must look how to get more interoperable... align your procedures more with each other. Names and roles have to be as much as the same, so you have a more common picture of how those management organizations plug into each other." [SEG038] This quotation introduces a governance and organizational lens for interoperability. It connects interoperability to how different crisis-management organizations recognize each other's roles, responsibilities, and ways of working.

The same actor made this point even more directly by linking interoperability to collaboration itself, "Interoperability is the condition to collaborate with each other. If you are not interoperable, you cannot collaborate. We often simplify it by speaking about collaboration, but that's only a small element in crisis management." [SEG039] This quotation shows that interoperability was understood as one of the conditions that makes collaboration possible. It also indicates that collaboration was not described only as willingness to work together. In this part of the interview material, collaboration depends on whether organizations can align their procedures, systems, mandates, language, and decision structures sufficiently to act together during disruption.

The interviews also retained the technical layer as a necessary part of the problem. A public crisis-management actor explained this through the need for standardized ways of connecting IT systems, "You have to have standard sets, standards, ways to let IT systems communicate with each other... a water authority next has built their own platform and in the same canal, there was a different water level... because they built two different systems." [SEG047] This quotation gives a practical example of technical misalignment. When different systems represent the same situation differently, actors may receive conflicting operational pictures. The technical layer

therefore remains relevant, but it appears in the interviews together with the need for shared meaning and organizational agreement.

Following on this line, RWS evidence adds an important warning about technology-first approaches. A netcentric-working actor argued that the solution lies in intersectoral understanding rather than deeper technical information: “The solution is not on a technical, more technical information, more depth. The solution is in intersectoral understanding... almost every technical platform or digital platform is focusing on the technical aspects, and they all fail or end up like a sectoral helping system.” [SEG040] This quotation shows that the actor did not reject technology itself. The concern was that digital systems can remain sectoral when they are developed mainly around technical depth and without enough attention to intersectoral understanding. In the interview, the difficulty was described as the ability of different sectors to understand each other’s situation, terminology, and operational priorities.

The port authority interview supports this from an implementation perspective. A port authority innovation actor explained that “I wouldn't say that the innovation per se is the issue here, but how can you simplify the process that you want to visualize with the digital platform? How can you make it as simple as possible for the actors and how can you make the different stakeholders be on board rather than the digital platform itself?” [SEG042] This quotation brings the finding back to the Port of Rotterdam context as it shows that the implementation issue was described less as the innovation itself and more as the process that actors are expected to understand and use. The actor links the usefulness of a digital platform to process simplification, actor involvement, and stakeholder acceptance.

4.3.4 The most valuable information to share is often also the most sensitive

Lastly, the fourth finding is that the information considered most valuable for cross-infrastructure resilience is also the most sensitive to share. According to the final codebook, coded material supporting this finding was present in nine of the ten interviews, comprising 20 validated segments (14 core and 6 supporting) across eight institution types. The supporting interview profiles were national crisis management and net-centric working (I1), rail operations and net-centric working (I2), rail business continuity and resilience (I3), cross-sector infrastructure modelling (I5), electricity-distribution risk management (I6), port-authority innovation (I7), public crisis management and network governance (I8), interoperability research (I9), and port cyber-resilience information sharing (I10). Across these interviews, actors identified causes of disruption, root causes, vulnerabilities, expected duration, operational weaknesses, capacity constraints, cyber indicators, network architecture, commercially sensitive patterns, and privacy-relevant data as especially useful for anticipating cross-infrastructure effects. The same information can, however, expose security risks, legal liabilities, commercial interests, or organizational weaknesses.

On this line, a rail business-continuity actor explained this tension through the example of aggregated information. Aggregation can in theory protect confidentiality, but it may also remove the context that other actors need to assess whether they face a similar risk: “To only share aggregated information... I choose to give only a limited amount of information... I might hold back information that might be interesting for other parties. For instance, about the cause of the disruption... sabotage... extreme heat causing computers to collapse... other companies can anticipate and ask themselves, could this happen also to me?” [SEG048] As highlighted by this quotation, cause and context information are valuable because they help others anticipate, prepare, or adapt. At the same time, these are precisely the details that may be sensitive to share. The actor’s point is therefore not only about how much information is shared, but about what kind of information remains useful once sensitive details are removed.

The same actor, however, did not present sensitivity as a reason to avoid sharing altogether. Instead, the actor connected meaningful information sharing to controlled access, authorization, and governance: “We should be as open as possible... Of course, we have to do some limited access and authorization procedures... People should be screened... That asks something about the governance... all the CEOs must decide... we want to share information.” [SEG049] This quotation adds an important contrast to the previous one. The issue is not simply whether sensitive information should be shared or withheld. The actor describes a more conditional form of openness, where sharing depends on access procedures, authorization, screening, and organizational commitment from senior decision-makers.

The port authority interview shows that this tension is also present at the port-system level. Here, the focus shifts from the value of cause information to the organizational boundary around data. A port authority innovation actor stated, “We do not easily share our data because we have confidential data, we have internal data, there is lots of safeguards to monitor what data we share outside.” [SEG050] This points directly to the fact that data sharing is filtered through internal safeguards and responsibilities. It is not only a matter of whether an organization is willing to share. It also concerns what kind of data is considered internal, what safeguards are already in place, and who carries responsibility for information that leaves the organization.

The Stedin interview gives a particularly clear example of why some operational information cannot simply be made visible to a wider network. On this theme, an electricity-distribution actor described network architecture and OT/IT information as highly sensitive, “Confidentiality of how... the architecture of the network... that’s gold for us... there are some killer switches in the network... if that information becomes available to some wrong actors... it’s a problem... OT and IT network, that’s gold for us.” [SEG052] This quotation shows that some information is too sensitive because it could increase vulnerability if accessed by the wrong actor. In this case, the issue is not only commercial confidentiality or internal policy but also the possibility that operational architecture could become a security risk if shared too widely.

RWS evidence adds another important nuance to this sensitivity problem. The reluctance to share does not only come from security risks or formal confidentiality rules. It can also come from the fact that disruption information may reveal mistakes, weaknesses, or failures. A netcentric-working actor explained that barriers may involve “military... strategic reasons, police... privacy... medical departments... privacy... commercial aspects... energy sectors,” but also that “you’re sharing your faults... you’re sharing what went wrong and we are not used to that sharing.” [SEG066] This quotation broadens the meaning of sensitivity. In this context, sensitivity appears here as strategic, privacy-related, commercial, operational, and reputational. Sharing disruption information may mean making visible what went wrong, and this can be difficult even when the information would be useful for others.

Several actors therefore framed information sharing in terms of controlled visibility. Stedin’s evidence was especially detailed on classification and access conditions. The actor explained that the organization classifies information according to confidentiality, integrity, and availability, and then decides whether data is public, confidential, or highly confidential: “We classify from the CIA, confidentiality integrity availability and with that classification we decide whether data is public, confidential or highly confidential information: public can be used on a trust basis, confidential with additional measures, highly confidential not on a trust basis or an agreement basis.” [SEG054] This suggests that trust alone is not treated as sufficient for all types of information. Different categories of information require different access rules, safeguards, and agreements. Public information may circulate more easily, while highly confidential information could require additional special formal arrangements.

FERM’s experience over the interviews adds another layer to this finding. In this case, the issue is not only what information is sensitive, but also how organizations come to see value in sharing at all. A cyber-resilience

information-sharing actor explained that participation depends first on actors understanding the benefit of sharing: “The vital thing is to make organizations understand what the benefit of such a sharing platform is... that if their neighbor is affected, then also indirectly always has an effect on them. That is the most important thing to make companies understand.” [SEG055] This quotation shows that sensitive information sharing depends partly on perceived interdependence. If organizations do not understand how another actor’s disruption may also affect them, they may have limited incentives to accept the risks and effort involved in sharing.

The same FERM experience also shows that participation is supported by clear expectations and transparent governance. A cyber-resilience information-sharing actor explained: “We have made a multilateral agreement in which we set all our expectations from companies, what we expect from them, and what they can expect from us... very transparent on how we govern... not let it be from an authority... FERM are a nongovernmental organization, we’re not out for profits.” [SEG056] This quotation shows how information sharing is organized in one existing community. It is supported by a multilateral agreement, transparent expectations, and a governance position that is presented as non-governmental and non-profit. In the interview material, this helps explain why sensitive information sharing is not described as a simple act of sending data, but as an arrangement shaped by expectations, perceived benefit, access conditions, and trust in the organization managing the exchange.

4.4 Rotterdam-specific manifestations of cross-infrastructure disruption

The four findings presented above cut across actor types and infrastructure domains. The interview material also provides a smaller set of observations that are specific to the Port of Rotterdam case. These observations do not constitute an additional thematic finding. Instead, they specify where cross-infrastructure dependencies become visible within the port’s operational setting.

First, the interviews located interdependence at concrete interfaces between infrastructures and transport modes. A rail business-continuity actor described a movable bridge in Rotterdam on which trains operate while ships pass underneath. When the bridge cannot move, maintaining continuity for one transport mode requires interrupting the other. The actor explained that “on the bridge the trains run and under the bridge the ships move” and that, following a failure, a choice may have to be made between rail and shipping, while “both modalities will be blocked” [SEG002]. This example presents a Rotterdam-specific operational point at which one physical asset connects rail transport, waterborne transport, and the movement of cargo between them.

A second interface appeared in automated terminal operations. A former terminal IT actor described how a database slowdown could increase the time required to process truck access from seconds to several minutes. Because trucks continuously enter and leave the terminal, the delay could rapidly extend beyond the terminal itself: “a query [...] made a database slow, and that could result immediately [in] a traffic jam” [SEG008]. In this example, the digital system did not need to stop completely before wider operational effects emerged. Reduced digital performance was sufficient to create a physical congestion effect on the surrounding road network. The interview material therefore shows that cross-infrastructure effects in Rotterdam can originate from relatively small delays at highly automated operational interfaces as well as from major infrastructure failures.

The interviews also connected port disruption with particular operational and supply-chain processes. A cyber-resilience information-sharing actor described Rotterdam as a network containing several interdependent supply chains. According to this account, a disruption affecting one organization may also become relevant to chemical companies, logistics processes, and traffic elsewhere in the port [SEG004]. An electricity-distribution actor similarly identified the interconnected planning and communication systems used for ship arrival and departure as a possible point of disruption. The actor explained that malfunction or cyber interference affecting this planning

process could create cascading consequences for daily port operations [SEG005]. These accounts provide more specific detail on where dependencies are situated: within the digital and organizational handovers connecting individual port processes, organizations, and infrastructure services.

Finally, the Port Authority interview described an internal distinction between physical incidents, cybersecurity disruptions, and commercial or logistics disruptions. The actor explained that these domains had historically been approached separately, even though their consequences may overlap, “in the past [they] were treated in isolation” while, for example, “something that happens with cybersecurity [...] would affect the physical side of the port” [SEG003]. From the perspective of this interviewee, clear guidance for combining responses across these domains had not yet been fully established. Coordination between an energy disruption and affected terminal operations, for example, could still need to be organized when the event occurs [SEG013]. The account therefore describes cross-domain coordination as an area still being developed across operational domains that were previously approached separately.

These observations provide a more detailed empirical picture of the Port of Rotterdam. Cross-infrastructure disruption is experienced through shared physical assets, digitally mediated operational bottlenecks, linked port processes, and the interaction between physical, cyber, and commercial or logistics disruption domains.

5. Discussion

5.1 Introduction to the discussion

After having presented the research findings, this chapter finally address the discussion of such findings in relation to the research aim, research questions, and conceptual framework. At this point of the research, the purpose is therefore to move from the empirical findings, that were presented in Chapter 4, to a broader interpretation of what they exactly mean for the feasibility and added value of a cross-infrastructure digital resilience platform as EU-IDRP in the Port of Rotterdam.

As seen, existing systems, operational routines, bilateral contacts, cyber-resilience communities, and formal crisis structures already play an important part in supporting important segments of coordination in and around the port. For this reason, the value shown in the findings does not suggest the complete replacement of existing disruption-management or crisis-management arrangements. However, it is important to state that these arrangements do not always create a full shared system-level awareness especially when disruption effects move across infrastructure domains. This is especially relevant for any disruptions that affect operationally interconnected infrastructure but have not yet become formal crises.

As main argument, it is therefore now central to address platform feasibility primary as a governance and organization problem. More specifically, a cross-infrastructure digital resilience platform may add value if it is able to helps different actors to develop system shared situational awareness, understand cascading consequences, and coordinate earlier across infrastructure boundaries. However, this added value is presented as conditional.

The discussion therefore separates two related questions. Potential added value concerns what a platform could improve relative to current coordination arrangements in Rotterdam. Feasibility concerns whether that function could be adopted and sustained within existing mandates, systems, information safeguards, and operational routines.

5.2 Synthesis of the findings: platform feasibility as a governance problem

The presented findings show how the possible added value of a cross-infrastructure digital resilience platform should be implied in relation to the current existing coordination environment of the Port of Rotterdam. That is, the port is already significantly supported by several operational systems, crisis-management arrangements, information-sharing communities and organizational routines. As consequence, actors already make use of internal dashboards, incident-management tools, bilateral contacts, phone calls, roundtables, LCMS, SpoorWeb, FERM, Portbase and other sector-specific measures. All these existing systems and practices already support important parts of current disruption management in the area. For this reason, as emerged from the analysis, the problem is that these same existing arrangements are the ones that produce fragmented and role-specific visibility, while cross-infrastructure disruptions still require system-wide shared understanding across different domains and actors.

The first element of this synthesis concerns the actual timing of cross-infrastructure disruption. The findings show that disruption can potentially become relevant across infrastructures before it fully becomes a formally declared crisis. This is important since formal crisis-management structures are normally activated through different escalation thresholds, while operational disruptions are usually handled directly by the single responsible organization, control center or sector-specific network. Between these two situations, a grey zone is therefore presented where a disruption effect may already move across infrastructures, but where coordination is still bounded and depends mainly on operational contacts, informal routines and the ability of actors to align their actions. In this specific defined space, a digital resilience platform could add significant value by supporting earlier recognition of interdependencies, potential cascading effects and shared operational consequences. Its role would therefore be to support coordination and sense-making before formal escalation becomes necessary, while still remaining compatible with formal crisis structures if escalation does occur.

The second element concern the difference between partial visibility and shared system-level awareness. The findings show that actors already have access to different forms of information. However, this information is usually constrained by the organizational roles, system access, professional communities and sectoral responsibilities. For this reason, practices and tools as SpoorWeb, LCMS, FERM, Portbase and internal systems all create useful forms of visibility, but they do not automatically generate a full shared cross-infrastructure picture. This distinction has become central for platform feasibility in this thesis, as its added value would depend on whether a platform would help actors to understand what a disruption directly means beyond their own organization or infrastructure domain. For this reason, it would not be valuable simply because it collects more information.

To support this point, there is one quotation from the findings that is worth repeating, a net-centric working actor, stated that “There is lots of information. That’s not a problem. The only thing is to comprehend and to extract the essence... what the problem is... technical information doesn’t get you to the solution... stop, think what’s the shared problem?” [SEG026] This is here important as it captures the core issue of shared situational awareness. As emerged, the challenge is expressed as the capacity to interpret information collectively and not pure access to information. A cross-infrastructure platform would therefore need to support shared problem framing, relevance filtering, consequence interpretation and communication rhythm. In this sense, platform value lies in formulating disruption information understandable and actionable for different actors rather than in data accumulation.

The third element respects the lens of interoperability. That is, the findings show that interoperability should not be reduced in simple terms of technical integration between diversified systems. Technical interfaces, data standards and model coupling are obviously necessary, but they represent only one part of the whole

interoperability spectrum. As emerged, actors need compatible definitions, shared meanings, aligned procedures, clear responsibilities, legal agreements and organizational routines that would allow information to be used across well-defined boundaries. This is therefore relevant as it confirms the actual importance of treating interoperability as a socio-technical condition. That is, a platform may technically connect different systems, but this does not guarantee that any actors can interpret the same terms, risks, timeframes or operational consequences in the same exact way. Specifically, for the Port of Rotterdam, this is especially relevant because the ecosystem includes public authorities, infrastructure operators, terminal actors, cyber-resilience actors, logistics systems and crisis-management organizations, each with its own routines, mandates and different information needs.

The fourth and last element is about the actual sensitivity of information itself. The findings here show that the most useful information for cross-infrastructure resilience is often the same information that actors find most difficult to share with each other's. More specifically, information about any root causes, expected disruption duration, affected or impacted assets, operational weaknesses, cyber indicators, network architecture or recovery planning can be very helpful for other actors to anticipate different consequences and prepare their own response during a disruption. At the same time though, this information can expose security vulnerabilities, commercial interests, privacy concerns, legal risks or reputational weaknesses as well. This therefore creates a core feasibility tension. A platform that only shares general or aggregated information may be considered safe privacy wise but may also provide only limited operational value while a platform that asks for detailed sensitive information may be useful in practice but may be challenging to trust and to adopt. For this specific reason, the findings point toward controlled visibility rather than open information sharing.

These findings show that platform feasibility is primarily considered as a governance and organizational problem. The technical question of whether a platform can act as intersection of data sources, producer of alerts or representator of interdependencies is important, but it is not totally sufficient. The central question is whether actors can all agree on the purpose of the platform itself, the type of information to be shared, the level of visibility provided to different users, the authority of data owners, the relationship with existing systems, and the role of the platform during escalation. For this reason, feasibility is expressed as dependent on concepts like trust, access rules, data safeguards, role clarity, institutional sponsorship, usability and long-term embedding.

This synthesis is therefore crucial to clarify the kind of platform that would be relevant and possible in the Port of Rotterdam context. Additionally, the findings do not advocate a fully centralized platform that would replace existing systems, decision rights or crisis-management structures. On the contrary, they recommend toward a federated and role-based coordination layer. Such a platform would therefore allow different organizations to keep the control over their own systems and data, while only sharing selected indicators, alerts, consequences and disruption-relevant updates under agreed conditions. Its function would be to strengthen shared situational awareness and cross-infrastructure sense-making, especially in the described grey zone between routine incidents and formal crisis escalation.

The main implication is that the platform's potential added value and its feasibility are related but analytically distinct. Potential added value concerns whether the platform could improve cross-infrastructure consequence interpretation relative to current arrangements, particularly in the pre-escalation coordination space identified above. Feasibility concerns whether that function could be adopted and sustained within Rotterdam's existing systems, distributed responsibilities, information-sharing constraints, and operational routines. Existing arrangements therefore have a dual effect: they create the coordination gap from which potential value arises, while also defining the conditions under which that value could be realized.

A platform could have substantial potential value but limited feasibility if it depended on information that actors were unwilling or unable to share. Conversely, a platform restricted to safe but highly aggregated information might be easier to introduce yet provide little incremental value over existing tools and practices. For the Port of Rotterdam, the relevant issue is therefore whether governance and organizational arrangements can convert a bounded potential value into a workable and sustainable coordination function. This requires the platform to make cross-infrastructure consequences more visible without increasing workload, duplicating existing systems, or weakening established responsibilities. In this sense, the platform should be understood as a governed coordination and sense-making layer rather than as a standalone technical solution.

5.3 Contribution to the literature: from interdependence to governed coordination

This section distinguishes what the interviews confirm, what they refine or extend, and whether they contradict the reviewed literature. The findings broadly confirm that the Port of Rotterdam is an interdependent socio-technical system, that shared situational awareness is different from data availability, and that information sharing and interoperability depend on governance and organizational conditions. The evidence does not directly contradict the main literature reviewed in Chapter 3. Its contribution is instead to specify how these established problems appear in Rotterdam's already populated coordination environment and what this means for the possible role of a cross-infrastructure digital platform.

The clearest empirical extension concerns the timing and location of the coordination problem. Huck et al. (2021) and Punt et al. (2023a, 2023b) already identify fragmented responsibilities, sectoral boundaries, information-exchange difficulties, and incomplete institutionalization in Rotterdam. The interviews narrow this broader problem to a pre-escalation space. That is, cross-infrastructure consequences may already require coordination while incidents are still handled by responsible operators and formal crisis arrangements have not yet assumed a central role [SEG009; SEG013]. This does not establish that a digital platform would resolve the gap. It identifies the specific situation in which its incremental value would need to be demonstrated.

The first contribution regards the understanding of the Port of Rotterdam as an interdependent socio-technical infrastructure system. On this theme, critical-infrastructure literature has long shown that different infrastructures such as energy, transport, ICT, water, logistics and emergency services are all connected through physical, cyber, geographic and logical interdependencies (Little, 2002; Rinaldi et al., 2001). The findings therefore support this view in the Rotterdam port context. That is, interviewees described a port environment in which rail, road, waterborne transport, terminal operations, electricity, ICT, cyber systems and crisis-management structures can easily become connected during disruption.

This point confirms the literature's broader understanding of cascading disruption' nature as characterized by both technical and organizational sides. The presented idea is that a failure may still start in a specific physical asset, an ICT system, a terminal process, a cyber incident or a transport corridor while its consequences actually depend on how other actors notice the event, interpret its relevance, communicate its possible effects and adjust their own operations in the right time. The interview material therefore enforces the view that port resilience depends on the whole wider capacity of actors to acknowledge and manage dependencies across the full port system. The Rotterdam case also adds an observed tone to this literature. That is, interdependencies can still exist without being fully visible to the actors who depend on them. On this theme, the findings show that actors can be aware of the general interdependent character of the port, while still having limited insight into how a disruption in one organization, modality or infrastructure domain may affect other ones. This polishes the literature on interdependence by presenting that the practical challenge is characterized by the uneven visibility and interpretation of dependencies across different actors and not only the existence of dependencies themselves.

This also connects to port-resilience literature. Recent studies increasingly describe seaports as complex systems involving physical, organizational, technological, environmental, digital and institutional capacities (Mohsendokht et al., 2026; Tsoulfas, 2026). In the Port of Rotterdam, resilience depends on maritime flows, rail and road access, inland waterways, energy systems, industrial activity, terminal operations, cyber arrangements and digital coordination. This confirms that port resilience is defined as a cross-infrastructure and cross-actor issue.

The second contribution concerns the concepts of shared situational awareness. The literature makes a distinction between shared data, a common operational picture and common situational understanding (Luukkala et al., 2017; Steen-Tveit & Munkvold, 2021). The findings support this distinction. That is, actors already use different set of systems and communication channels, including operational tools, crisis-management arrangements, cyber-information-sharing groups, internal dashboards, phone calls, informal networks and role-specific platforms. All these arrangements in place are advantageous and create useful forms of visibility, but such visibility still remains partial and quite bounded by different organizational roles, diversified system access and infrastructure domains. This finding is therefore important because it shows that shared situational awareness also depends on interpretation and relevance as well. A platform that is able to display more information load would not automatically be enough to support better coordination per se. that is, its value would still depend on whether it can help different actors in better understanding what a disruption means for their own responsibilities and for the wider port system, to help addressing the “common picture”. This means that information must be filtered, translated and connected to consequences, timing, dependencies and possible actions. In this sense, shared situational awareness is defined as a process of cross-actor sense-making and not as a simple product of data availability.

The findings here refine the literature by showing how this distinction appears in a populated coordination environment. As mentioned, Rotterdam already has digital systems and coordination arrangements. The issue is therefore that existing systems are designed for particular roles, sectors, communities or escalation. For this reason, a cross-infrastructure digital resilience platform would have to add value in the spaces where existing systems are not able to produce shared system-level awareness. This becomes crucial as it makes complementarity with existing arrangements a central feasibility condition for the platform adoption.

The third contribution follows the idea of the practice of data sharing defined as a governance condition. The literature on information sharing and data governance shows that such practice of data exchange among infrastructure and crisis-management actors is highly shaped by trust, confidentiality, incentives, work processes, access rules, accountability and different organizational boundaries (Bharosa et al., 2010; Delacroix & Lawrence, 2019; Punt et al., 2023b). The findings confirm this concept quite strongly. That is, interviewees described it as a conditional practice shaped by sensitivity, data ownership, cybersecurity, commercial interests, legal responsibility, reputational risk and trust in the actor or arrangement managing the exchange. The most important empirical extension is that the information that has the highest resilience value is also the same information that often is most difficult to share. The information about disruption causes, root causes, vulnerabilities, expected duration of incidents, cyber indicators, clear operational dependencies, recovery planning or network architecture can be very helpful for other actors to anticipate consequences and prepare their own response accordingly. However, the exact same information may also expose weaknesses, security risks, commercial interests or legal liabilities. This means that the value and sensitivity of information increase proportionally together.

This extends the literature by showing why a platform cannot simply rely on a general call for “openness”. That is, data sharing is a crucial process that need to be governed through controlled visibility, access rules, clear expectations and data-owner authority. The findings therefore point toward selective and role-based sharing rather

than unrestricted information exchange. This is significant because the practical feasibility of a platform depends on whether actors can contribute useful information without losing control over their sensitive data, internal responsibilities or any legal exposure.

This discussion also connects to the findings on the concept of interoperability. As seen, interoperability is usually and often treated as a technical concern, but the findings support the broader literature that better frames it as socio-technical dimension. Obviously, actors still need to have compatible systems, data formats and interfaces, but they also need shared definitions, well-aligned procedures, legal agreements, role clarity and a set of common organizational routines. In the Rotterdam case, interoperability therefore becomes part of the same governed-coordination problem. Technical connection becomes therefore more than useful when actors know exactly what the actual information means, who is allowed to have access to it, who is responsible for acting on it, and how it relates to existing decision rights.

What has been learned beyond the literature is therefore narrower than the general statement that Rotterdam is interdependent or institutionally fragmented. The interviews add three case-specific refinements. First, the coordination gap is concentrated in the interval between routine operator-led handling and formal escalation. Second, the central information problem is the translation of role-specific information into shared consequences within an already populated system landscape. Third, confidentiality measures such as aggregation can remove the causal context that makes information useful to other operators [SEG048]. By contrast, the importance of socio-technical interoperability, trust, and distributed authority primarily confirms existing literature.

The contribution is therefore an empirical specification and qualification of prior research rather than a claim that these governance problems were previously unknown. For port-resilience research, the findings show that a digital platform should be assessed within an existing coordination ecology rather than as a standalone solution. For critical-infrastructure governance research, they show that managing interdependence requires arrangements through which disruption information becomes understandable, relevant, and actionable across organizational boundaries. The thesis consequently shifts attention from interdependence as a structural condition to governed consequence interpretation as an operational coordination problem.

5.4 Answering the research questions

At this point of the discussion, after having defined the literature contribution, it is now finally time to address the research question and sub-questions that fully characterize this thesis research. This section therefore aims to answers the four sub-questions and the main research question in a clear and explicit way. The answers build on the empirical findings presented in Chapter 4 and on the synthesis developed in the previous sections of this discussion.

SQL: How are cross-infrastructure disruptions and cascading effects currently understood in and around the Port of Rotterdam?

Cross-infrastructure disruptions are understood by actors as disruptions whose consequences may move beyond the infrastructure domain where the original problem starts. In and around the Port of Rotterdam, disruption is therefore not understood only through maritime operations or terminal activity. It is also connected to rail, road, inland waterways, electricity, ICT systems, cyber resilience, industrial activity, water-related infrastructure, logistics chains and public crisis-management arrangements. The findings show that actors actually recognize the port as a connected operational environment. For this reason, a disruption in one domain can become relevant for

other actors because port continuity depends on shared corridors, digital systems, energy flows, operational schedules, data exchange and public-private coordination.

The interview evidence makes these dependencies more concrete. A Port Authority actor described the absence of clear guidance for combining responses between energy and terminal actors as a disruption develops [SEG013]. An electricity-distribution actor explained that information about recovery and restoration matters because reactivation by another organization may itself create consequences for the grid [SEG031]. Cascading effects are therefore understood not only as physical chains of failure, but also as consequences transmitted through operational timing, restoration decisions, shared systems, and distributed responsibilities.

At the same time, this understanding remains uneven across different actors. Some of them understand cascading effects through their own operational domain, while others focus more on crisis escalation, cyber-risk signals, information-sharing arrangements, modelling, or system interoperability. This means that awareness of interdependence exists, but it is often role-specific and partial. The findings therefore address the answer of SQ1 by showing that cross-infrastructure disruption is actually recognized as a real problem, but that shared system-level understanding of cascading consequences remains limited.

The Rotterdam-specific answer is therefore that interdependence is widely recognized, while its operational consequences remain interpreted through different actor roles rather than through one consistently shared system-level view. This has a direct implication for platform feasibility. A cross-infrastructure digital resilience platform could add value by making interdependencies, consequences and timing more visible across organizational boundaries. However, this value depends on whether the platform helps actors understand consequences that are relevant for their responsibilities, rather than simply showing more technical information.

SQ2: How are disruption management, coordination practices, information flows, responsibilities, and decision rights currently organized across relevant actors?

Disruption management in the Port of Rotterdam context is organized through a distributed set of actors, systems, routines and escalation structures. Individual infrastructure operators, terminal actors, cyber-resilience actors, public authorities and crisis-management organizations each retain their own responsibilities and decision rights. This means that disruption management is not organized through one single hierarchy or one single port-wide command structure. It is organized through a combination of operational responsibility, sector-specific systems, public crisis-management arrangements, existing relationships and escalation thresholds. At the operational level, many disruptions are handled by the actors directly responsible for the affected infrastructure, asset, system or service. These actors use internal procedures, control centers, operational tools, phone calls, informal contacts and bilateral coordination to manage the situation. This can work well for incidents that remain close to one domain or that can be solved through existing operational routines.

At the formal crisis-management level, arrangements such as GRIP, LCMS and net-centric working provide structures for escalation, shared crisis information and public coordination. These arrangements become especially relevant when disruptions reach a level where public safety, societal continuity, environmental risk or multi-actor crisis response becomes central. In those cases, public crisis-management actors and formal coordination structures become more prominent.

Between these two levels, as previously explained, the findings identify a valid grey space. Some disruptions may already have cross-infrastructure consequences, while still being handled through operational coordination rather than formal crisis escalation. In this actual space, actors may need faster shared understanding, cross-domain

interpretation and alignment of possible consequences, while legal decision rights and operational responsibilities remain distributed. This is one of the most important answers to SQ2. Existing coordination exists, but it is fragmented across systems, routines and thresholds.

Information flows reflect this distributed structure. Actors use systems such as SpoorWeb, LCMS, FERM, Portbase, internal dashboards, operational communication channels, meetings, roundtables, phone calls and informal networks. These systems and practices create useful forms of information exchange, but they remain bounded by role, access, community, sector and organizational responsibility. Decision rights also remain with the responsible actors. A platform could support shared awareness and coordination, but it would not replace the authority of infrastructure operators, public authorities or crisis-management structures.

This produces a layered coordination ecology rather than a single port-wide structure. That is, SpoorWeb and operator systems support sector-specific disruption management, FERM supports cyber-related exchange within a bounded community, GRIP, net-centric working, and LCMS support formal crisis coordination and phone calls, WhatsApp, roundtables, and personal contacts bridge gaps between systems. The ProRail–LCMS example shows that actors may need to rely on telephone or WhatsApp when they do not participate in the same information system, creating a risk of information loss [SEG022]. The Port Authority interview therefore similarly shows that communication with external actors is often assembled through roundtables and calls once an incident occurs [SEG023]. The answer to SQ2 is consequently that responsibilities and decision rights remain distributed, while information exchange is organized through overlapping systems and relationships with an incomplete pre-escalation cross-domain layer.

SQ3: What barriers and enabling conditions do stakeholders identify for the adoption and use of a cross-infrastructure digital resilience platform?

The findings identify several barriers to adoption and use. The first barrier is problem fit. Rotterdam already has many systems and coordination arrangements. A new platform would therefore need to address a clear gap. If actors see the platform as another dashboard, another reporting obligation or another parallel system, adoption would result weak. The strongest problem fit is the grey space between routine operational incidents and formal crisis escalation, where cross-infrastructure effects may already matter but shared system-level awareness remains limited.

A second barrier is data sensitivity. The information that could be most useful for cross-infrastructure resilience is often sensitive. Information about root causes, expected duration, cyber indicators, operational vulnerabilities, network architecture, recovery planning, capacity constraints or dependencies may help other actors anticipate cascading consequences. The same information may also create security, commercial, legal or reputational risks. This makes open data sharing unrealistic as a general principle. The platform would need controlled visibility, access rules, information classification and data-owner authority.

A third barrier is interoperability. Stakeholders identify interoperability as more than technical system integration. Data formats, interfaces and model coupling matter, but they are not enough. Actors also need shared definitions, compatible procedures, agreed meanings, legal arrangements, aligned responsibilities and operational routines. Without these conditions, technical integration could still produce confusion, conflicting interpretations or unused outputs.

A fourth barrier is operational usability. Actors are unlikely to adopt a platform that increases workload during disruption. In crisis and operational settings, additional reporting, duplicate systems or unclear interfaces can

create platform fatigue. The platform would need to reduce coordination burden, provide relevant information quickly, support existing routines and avoid creating extra work for already busy operational actors.

A fifth barrier is ownership and legitimacy. Stakeholders would need clarity about who owns, operates, funds, governs and maintains the platform. They would also need confidence that the platform is neutral, secure, useful and aligned with existing responsibilities. A platform led by one actor without broader legitimacy could raise concerns about control, access, strategic interests or data use.

SQ3 is therefore an adoption and use question. It identifies what makes organizations more or less willing and able to participate. These conditions include a visible incremental benefit over existing tools, acceptable information-sharing risk, semantic and procedural compatibility, low additional workload, and confidence in the platform's sponsor and rules. These enabling conditions are not simply considered as the reverse of the barriers as they are mechanisms through which participation can become credible. Rotterdam-specific evidence illustrates this distinction. Actors warned against another technology-first sectoral platform [SEG040], stressed process simplification and stakeholder involvement [SEG042], and described reciprocal expectations under FERM's multilateral agreement as one existing mechanism for trusted participation [SEG056].

SQ4: What governance and organizational conditions would need to be in place for such a platform to be trusted, used, and institutionally embedded in the Port of Rotterdam context?

SQ4 builds on SQ3 but serves a different analytical function. SQ3 identifies adoption barriers and enabling conditions as perceived by stakeholders. SQ4 translates those perceptions into questions of authority, rules, accountability, and institutional placement.

First, participating organizations would retain their operational authority and legal decision rights; platform outputs would support interpretation rather than command action. Second, data owners would need formal authority to determine which outputs are shared, for which purpose, with which users, and at what level of detail. Third, a legitimate multi-actor arrangement would need to assign convening, platform operation, funding, maintenance, security responsibility, accountability for information use, and procedures for revising participation and access rules. Fourth, the platform would need an explicit relationship with existing coordination arrangements. It could be tested as support for pre-escalation consequence interpretation, while GRIP, LCMS, and mandated crisis actors retain their formal functions when escalation occurs.

The evidence is insufficient to select a final owner or governance mode. The Port Authority is a plausible convener because of its position in the port ecosystem, but the interviews do not justify treating it as the sole owner or commander. The answer to SQ4 is therefore not a completed institutional design, but a set of governance requirements that any future arrangement would have to resolve.

Main research question:

How do existing disruption-management practices, information flows, and governance arrangements in and around the Port of Rotterdam shape the feasibility and potential added value of a cross-infrastructure digital resilience platform?

Existing practices shape potential added value by revealing a bounded coordination need rather than a general absence of coordination. The strongest case for a platform is the pre-escalation interval in which a disruption remains under operator responsibility, but its possible consequences have already become relevant to other

infrastructure domains. In this interval, existing systems provide valuable but role-specific visibility, while cross-domain interpretation still depends heavily on bilateral contacts, separate information environments, and the ability of individual actors to identify who else may be affected.

The same practices shape feasibility because the Port of Rotterdam already contains specialized systems, distributed mandates, established crisis arrangements, and differentiated information-security regimes. A platform would therefore have to demonstrate incremental value over arrangements such as SpoorWeb, LCMS, FERM, Portbase, operator systems, and existing bilateral contacts. It would also need to preserve operator decision rights, support purpose-limited and role-based information sharing, align meanings and procedures across organizations, and avoid creating an additional reporting burden.

At the conceptual and governance level assessed in this study, a cross-infrastructure platform therefore appears conditionally feasible as an advisory coordination and sense-making layer. Its potential added value lies in making cross-domain consequences, expected timing, and relevant response information more understandable before formal escalation. This conclusion concerns perceived governance and organizational feasibility. It does not demonstrate the technical performance, operational effectiveness, or actual user behaviour of an implemented platform.

5.5 Governance and organizational considerations for platform adoption

The evidence does not support a complete governance framework that allocates final authority, ownership, funding, and accountability among all relevant actors. This section therefore presents governance and organizational considerations that a future arrangement would need to resolve. These considerations are derived from the interview findings and interpreted in relation to the network-governance and digital-infrastructure literature. Their purpose is to structure further design and testing rather than to present an empirically validated governance model.

Network-governance literature distinguishes shared-participant, lead-organization, and separate network-administrative forms, whose suitability depends on factors such as trust, goal consensus, network size, and the competencies required at network level (Provan & Kenis, 2008). The development of Rotterdam's Port Community System also shows that the governance of interorganizational digital infrastructure can evolve over time rather than remain fixed from the outset (Chandra & van Hillegersberg, 2018). The present evidence does not justify selecting one of these modes for EU-IDRP. The considerations below therefore identify the questions that would need to be settled before a pilot or institutional arrangement could be assessed.

Table 5.1. Governance and organizational considerations for platform adoption

Governance and organizational considerations	Questions to be resolved	Implication for the Port of Rotterdam
Purpose and Problem fit	Which coordination problem would the platform address, and what incremental value would it provide?	The initial use case should concern cross-domain consequence interpretation before formal escalation and demonstrate value beyond existing systems.
Institutional placement	Where would the platform sit in relation to operator systems,	It could be tested as a support layer between operator-led

	FERM, Portbase, GRIP and LCMS?	disruption handling and formal crisis escalation, without replacing existing arrangements.
Decision Authority and escalation	Who may activate the platform, validate information and act on its outputs, and what changes after formal escalation?	Platform outputs should remain advisory, domain decisions remain with responsible operators and formal crisis authority remains with mandated actors.
Information governance	Who decides what is shared, for which purpose, with which users, at what level of detail and for how long?	Information sharing should be data-owner-controlled, purpose-limited, role-based and supported by classification and authorization rules.
Socio-technical interoperability	How will formats, meanings, update rhythms, procedures, responsibilities and legal conditions be aligned?	Common definitions, workflows and accountability arrangements should precede or accompany technical integration.
Operational integration and usability	How will the platform avoid parallel reporting, duplication and additional workload?	It should provide limited consequence-oriented outputs and connect to current work processes wherever possible.
Institutional stewardship	Who convenes, operates, funds, secures, maintains and revises the arrangement?	The Port Authority may be a convener, but final stewardship requires broader multi-actor legitimacy and remains unresolved by the study.

The most plausible institutional placement suggested by the findings is between operator-specific disruption handling and formal crisis escalation. In this position, the platform would not replace SpoorWeb, Portbase, FERM, LCMS, operator control systems, or existing bilateral contacts. Its bounded function would be to translate selected disruption updates into consequences that are understandable across domains before escalation and to remain compatible with formal crisis-information processes when escalation occurs.

Within this thesis, the term federated should be used carefully. It refers primarily to a distributed data- and decision-control principle. Under this principle, participating organizations retain their own systems, data, and mandates, while selected outputs are shared under agreed access and use rules. It does not by itself define who governs the joint arrangement, how collective rules are made, or who is accountable for its operation. Because federated data control was part of the EU-IDRP concept before the interviews, the empirical result is that interviewees' emphasis on local control, authorization, and distributed authority supports and refines that pre-existing principle, therefore the interviews did not independently generate a complete model of "federated governance."

The governance mode therefore remains open. The Port Authority may act as a convener or sponsor, a participant-led arrangement may distribute governance among the involved organizations, or a separate administrative entity may eventually be required. The evidence supports only the more limited conclusion that one actor should not be assumed to command all participants and that institutional stewardship would need sufficient public-private legitimacy.

These considerations should be applied as a staged assessment and not as a final institutional proposal. The immediate question is whether a bounded set of actors can agree on one use case, authority and access rules, shared meanings, and operating responsibility, and then demonstrate practical value without duplication or additional burden.

5.6 Design and staged implementation considerations for the Port of Rotterdam

The sequence below is a researcher-derived pathway for staged testing rather than an empirically validated implementation plan. It operationalizes the considerations in Table 5.1 and connects each step to the findings. The pre-escalation coordination gap justifies selecting a bounded use case, partial visibility justifies consequence-oriented outputs rather than another general dashboard, socio-technical interoperability justifies agreeing meanings and workflows before technical connection and information sensitivity justifies data-owner-controlled and role-based access.

The first step should be the selection of a bounded coordination use case and the provisional identification of the actors directly connected to it. One empirically grounded option would be an energy disruption with consequences for terminal operations and restoration sequencing. The interviews identify both the absence of clear guidance for combining energy and terminal responses [SEG013] and the importance of restoration information to an electricity operator [SEG031]. This should be treated as a candidate for testing rather than as the only or definitively best pilot scenario.

The second step should be the formation of an exploratory coalition around the selected use case. Its composition should follow the dependency being tested rather than attempt to represent the entire port ecosystem from the beginning. For the energy–terminal example, this could include the relevant infrastructure operator, one or more terminal actors, the Port Authority in a convening role, and the relevant public crisis-management actor. The coalition’s first task would be to agree on the coordination problem and the limits of the platform’s role.

The third step should be the development of a bounded governance and information-sharing agreement. This agreement should identify the participating organizations, data owners, permitted users, purposes of use, information categories, update rhythm, status of platform outputs, and responsibility for inaccurate or outdated information. Initial outputs should be limited to information repeatedly identified as useful in the interviews: the affected function or area, current disruption status, expected duration, likely consequences for other modalities, confidence level, response or restoration intention, and the time of the next update [SEG027; SEG028; SEG031]. FERM’s multilateral agreement provides a Rotterdam-based example of how reciprocal expectations and transparent governance can support information sharing, although a cross-infrastructure pilot would involve a wider actor constellation and should not simply reproduce the FERM arrangement [SEG056].

The fourth step should be a limited pilot using federated data control. Participating organizations would retain their internal systems and data, while only approved disruption-relevant outputs would be shared. The pilot should test whether these outputs support cross-domain interpretation without exposing unnecessary operational detail. Wherever possible, it should connect to existing work processes and interfaces rather than create an additional reporting channel.

The fifth step should be evaluation through an exercise or tabletop scenario. Evaluation should examine whether the pilot reduces the time needed to form a shared interpretation, reduces parallel calls and duplicate updates, preserves data-owner control, makes access and responsibility clear, and remains compatible with GRIP and LCMS escalation practices. It should also identify whether actors interpret the information consistently and

whether the platform creates any additional workload or uncertainty. Failure on these criteria should lead to redesign before any expansion is considered.

Only after this evaluation should gradual expansion be considered. Expansion should depend on demonstrated coordination value rather than technical possibility alone. Additional actors, infrastructure domains, or disruption scenarios should be added only where the pilot shows that shared consequence interpretation improves, sensitive information remains protected, and existing responsibilities remain clear. The Port Authority may play a convening or sponsoring role because of its position in the port ecosystem, but final stewardship should remain an open institutional question to be negotiated with operators, public crisis actors, and relevant information-sharing intermediaries.

The practical implication is therefore that platform development should start as a governance and learning process. A first pilot should test whether actors can create a trusted, useful and controlled coordination space around one concrete disruption scenario. This approach would make implementation more feasible than starting from a full technical platform. It would also allow the Port of Rotterdam to assess whether the platform adds value where the findings identify the strongest need: earlier cross-infrastructure awareness in situations that are already interconnected but not yet formally escalated as crises.

5.7 Methodological reflection, limitations and future research

This study was framed as a qualitative single-case study of governance and organizational feasibility. This design was chosen because the research did not aim to measure the operational performance of a digital platform or test a technical prototype. Instead, the study examined how relevant actors understand cross-infrastructure disruption management, information sharing, responsibilities, decision rights, trust, interoperability and institutional embedding in the Port of Rotterdam context. The platform concept was used in the research as a methodological entry point. The platform concept helped participants reflecting on current practices and on the conditions under which a shared digital resilience tool could become useful or problematic.

Accordingly, the governance considerations in Section 5.5 and the staged pathway in Section 5.6 should be read as analytically derived propositions for further testing. They do not constitute a validated governance model or an operationally tested implementation roadmap.

This design was able to create several strengths. First, it allowed the research to study platform feasibility before actual implementation, which is important because many barriers to adoption appear before a technical system is built. Second, it made it possible the comparison of perspectives across different actor types, including infrastructure operators, public crisis-management actors, port-related actors, cyber-resilience actors, digital modelling experts and interoperability experts. Third, it kept the analysis close to the governance problem of the thesis. The interviews did not only ask whether a platform would be technically possible, but also what it would mean for data sharing, ownership, trust, roles, workload, institutional fit and long-term embedding.

At the same time, the study has several limitations that are important to address and that shape how the findings should be interpreted. The first limitation is about the interview sample. Due to time constraints and access limits, the study is based on ten expert interviews. Although the sample does cover a diverse set of actor types, it does not represent the full port ecosystem in its entirety. Some relevant perspectives may be underrepresented. This means that the findings should be read as an in-depth qualitative interpretation of key governance conditions, rather than as a complete map of all views in the Port of Rotterdam.

Following, the second limitation obviously concerns access to sensitive information. That is, the research topic touches on very critical infrastructure, cybersecurity, operational disruption and organizational responsibility. For this specific reason, it was neither realistic nor appropriate to ask participants for additional information on detailed system schematics, confidential incident procedures, cyber vulnerabilities or commercially sensitive operational data. This strengthens the ethical position of the study, but it also limits the level of technical and operational detail that could have otherwise been analyzed. This research is therefore deeper on governance patterns, perceived barriers, organizational conditions and platform feasibility than on detailed technical design or real incident reconstruction.

The third limitation concerns the role-specific nature of expert interviews. Participants spoke from their own institutional position, professional experience and organizational responsibility. This is considered valuable because the study focuses on a quite distributed actor landscape. However, it also means that interview evidence may reflect role-specific priorities, organizational assumptions or socially desirable accounts. Cross-actor comparison helped reduce this limitation by identifying patterns that appeared across different actor types. Still, the findings remain interpretive and should not be treated as a neutral description of the entire port system.

Following, the fourth limitation is about the conceptual nature of the platform. EU-IDRP was treated in the research as an unfinished platform concept rather than as a functioning prototype. This was useful because it allowed participants to discuss feasibility, risks and governance requirements without being constrained by a fixed technical design. However, it also means that the study cannot evaluate actual platform usage, specific user behavior, detailed interface quality, operational reliability, cyber-security performance or effectiveness during real happening disruptions. The findings identify governance and organizational conditions for feasibility as they do not prove that the platform would perform effectively in practice.

Lastly, the fifth limitation concerns the single-case design. The Port of Rotterdam was selected as an information-rich case because it is a large European landlord port with dense infrastructure interdependencies, a distributed public-private actor landscape, and relevance under EU resilience and cybersecurity regulation. This makes the case valuable for analytical insight, but it does not allow statistical generalization to all European or worldwide ports. The findings may be relevant for other large ports and infrastructure hubs, but only where similar conditions exist, such as multi-actor governance, critical infrastructure interdependencies, digitalization, data sensitivity and regulatory pressure.

If the study were repeated or extended, several methodological improvements would be useful. First, broader actor coverage would highly strengthen the whole analysis. Additional interviews with terminal operators, logistics firms, shipping actors, road transport actors, telecom providers, municipal actors, emergency services, regulators and private technology providers would make it possible to test whether the governance conditions identified in this thesis are recognized more widely across the whole port ecosystem.

Second, a validation workshop could be very valid as it would improve the robustness of the findings. The idea would be to bring together a small group of participants from different actor categories. That would allow the findings and governance and organizational considerations to be better discussed collectively. This would be especially useful because platform feasibility depends on interaction between different actors. A workshop could then show whether actors agree or not on the grey-zone coordination problem, whether they recognize the same data-sharing barriers, and whether the proposed governance conditions are realistic and approved system wise.

Third, scenario-based exercises or simulations would provide a stronger test of platform value. Instead of discussing the platform concept in general terms, participants could be asked to respond to a concrete disruption

scenario involving several infrastructure domains. Such an exercise could test what information actors need, when they need it, who should provide it, how sensitive it is, and whether a shared platform would reduce or increase coordination burden. This would make the analysis far more operational while still remaining safe and controlled.

Fourth, connected to the previous point, a more concrete platform mock-up could help refine the findings. The interviews were based on a broad conceptual description of EU-IDRP. A mock-up showing possible screens, information categories, access levels, alerts or dependency visualizations would allow participants to react to a more tangible object. This could reveal usability issues, trust concerns and information needs that are difficult to identify through abstract discussion alone.

Additionally, future research could add value by building on this thesis in four different main directions. First, performing comparative port studies would be quite valuable. Rotterdam is an information-rich case, but other European ports may have different governance structures, ownership models, crisis-management arrangements and digital infrastructures. Therefore, comparing Rotterdam with ports such as Antwerp-Bruges, Hamburg, Amsterdam, Valencia or Singapore could show which governance conditions are case-specific and which are more widely relevant for large port ecosystems.

Second, future research should test real prototype or actual pilot settings. The reason is that this thesis mainly identifies governance and organizational conditions for adoption, but it does not evaluate any implemented system. For this reason, a pilot study could examine how different actors actually approach and use a platform using federated data control and role-based access during exercises or controlled operational scenarios. This would be very helpful in assessing whether the proposed platform improves shared situational awareness, supports cross-infrastructure sense-making and avoids additional workload.

Following, legal and data-governance research is particularly needed. As the findings show that sensitive information sharing is one of the central feasibility issues, future research should examine which legal agreements, data-sharing models, liability arrangements, confidentiality rules and access-control mechanisms are most suitable for cross-infrastructure resilience platforms. This would be especially important where cyber-security information, operational technology data, commercial information or critical infrastructure dependencies are involved and interconnected.

Last, future research should also take into examination how NIS2 and CER are implemented in practice across the port ecosystems. These directives are fundamental as they increase the relevance of resilience, cybersecurity, risk management and cooperation, but their lack is that they do not provide a complete governance model for shared digital resilience platforms. Research on their implementation could therefore show whether they encourage cross-sector coordination, create new reporting burdens, support information sharing, or leave important governance gaps unresolved.

All these limitations do not weaken the value of the study, but they define its scope. That is, the thesis provides an empirically grounded governance interpretation of platform feasibility in the Port of Rotterdam. Its actual value is to show which conditions would need to be addressed before a cross-infrastructure digital resilience platform could be realistically developed, piloted or embedded. Further research should therefore move from feasibility exploration toward validation, comparison and practical testing.

6. Conclusion

This thesis initially started from the idea of addressing the development of a “European Union Infrastructure Digital Resilience Platform”, here referred to as EU-IDRP. At the very beginning of the research, this platform was first understood as a potential digital tool able to support coordination across different interdependent infrastructures. Throughout the development of the research, this initial design idea later became an actual feasibility question. The central addressed issue was therefore no longer whether a digital platform could be imagined and developed, but under which governance and organizational conditions such a platform could realistically be adopted, trusted, used and embedded in a complex port ecosystem to address the complexity behind cascading disruption.

The Port of Rotterdam provided an important case for this research because it represents a dense cross-infrastructure environment. That is, its operational continuity depends on the interaction between maritime transport, terminal operations, road and rail corridors, inland waterways, pipelines, energy systems, ICT systems, cyber-resilience arrangements, industrial activity, water-related infrastructures and public crisis-management structures. In this context, disruption management therefore cannot be reduced to just one single organization, one single infrastructure or one single technical system. That is, it actually depends on multiple public and private actors that currently hold different responsibilities, information, operational priorities, legal obligations and decision rights.

This research was directed by the question of how existing disruption-management practices, information flows and governance arrangements in and around the Port of Rotterdam shape the feasibility and potential added value of a cross-infrastructure digital resilience platform. To answer this question, the thesis used a qualitative single-case study design. The study combined literature review, actor and infrastructure mapping, and ten semi-structured expert interviews. The interview sample used for this research included actors and experts connected to public crisis management, rail infrastructure, terminal operations, energy distribution, port innovation, cyber-resilience information sharing, digital modelling and interoperability. The platform concept was used in the research and in the interviews as a methodological entry point, because it gave participants a concrete object through which they could reflect on current disruption-management practices and on the possible role of shared digital coordination.

The literature review positioned the study within debates on port resilience, critical infrastructure interdependencies, shared situational awareness, data governance, interoperability and collaborative governance. Across these fields, the same broad insight emerged. That is, resilience in ports and infrastructure systems also depends on how actors share information, interpret disruption consequences, coordinate across organizational boundaries and make decisions under distributed authority and cannot be understood only through physical robustness or technical capacity.

The main deduction of this thesis is that a cross-infrastructure digital resilience platform could, in principle, have added value in the Port of Rotterdam ecosystem, but its feasibility depends primarily on different governance and organizational conditions. The findings of the research confirm that Rotterdam already has many existing systems, current routines and coordination arrangements. That is, actors do use operational systems, crisis-management structures, cyber-information-sharing communities, internal dashboards, bilateral contacts, phone calls, roundtables and informal networks. As emerged, all these arrangements are very valuable, and they support important parts of current disruption management in the area. However, they often produce partial visibility and are quite limited in producing shared system-level awareness. They are helpful for actors to understand what is happening within their own organization, sector or operational community, while cross-infrastructure consequences may still remain quite difficult to see and interpret in a collective way.

As it emerged from the analysis, the clearest space where a platform could add potential value is described as the grey area that is created between routine operational incidents and full formal crisis escalation. In this specific space, disruption effects may already move across different infrastructure domains, while the situation has not yet reached the threshold of a formal crisis. In such scenario, actors already need to understand dependencies, timing, operational consequences and possible cascading effects, but coordination still depends heavily on existing contacts, sector-specific systems and ad hoc communication. For this reason, a platform could potentially support earlier recognition of these interdependencies and play a crucial role in helping actors to mature a more shared understanding of the situation.

At the same time, these same conditions that make the platform relevant also make it challenging to implement. That is, the Port of Rotterdam is presented as populated digital and institutional environment. For this reason, a new platform would therefore need to be functionally complementary to existing arrangements such as GRIP, LCMS, FERM, Portbase, operator systems and internal crisis procedures. As additional key layer, a platform would also need to carefully respect distributed responsibilities. That is, infrastructure operators, public authorities, terminal actors, cyber-resilience actors and other organizations would still continue to hold their own mandates and decision rights. For this reason, a platform as EU-IDRP should be addressed as a governed coordination and sense-making layer. Its purpose would therefore be to support shared situational awareness, interdependency recognition and cross-actor interpretation to every actor included in the system. It should not be designed as a centralized command system or as a replacement for existing crisis-management structures. Its value would lie in helping actors see and interpret disruption consequences across infrastructure boundaries, while preserving the responsibilities and authority of the actors involved.

This thesis contributes to the literature by moving the discussion from infrastructure interdependence to governed coordination. Existing literature already shows that ports and critical infrastructures are interdependent. This thesis adds that recognizing interdependence is only the starting point. For interdependence to become actionable during disruption, actors need trusted arrangements for sharing, interpreting and using information across organizational boundaries. The study also contributes to debates on shared situational awareness. On this theme, the findings show that the main issue is not merely the actual availability of data. That is, actors often already have wide access to large amounts of information. The presented challenge is therefore to extract the relevant meaning of that information and to understand what it implies for other actors, infrastructures and possible cascading effects. Shared awareness consequently depends on interpretation, relevance, timing, trust and operational usefulness.

A further contribution regards data sharing and interoperability. The research shows how the most valuable information for cross-infrastructure resilience is often also the most sensitive one to share. That is, information about root causes, expected duration, vulnerabilities, cyber indicators, operational constraints or infrastructure dependencies can help other actors anticipate consequences. Yet this information may also contain vulnerable actors' data and therefore create security, commercial, legal or reputational risks. This concept therefore makes controlled visibility more realistic than wide open information sharing. Interoperability must therefore be addressed to include technical interfaces, shared meanings, legal safeguards, access rules, data-owner authority and organizational routines.

In practical terms, this thesis proposes that the Port of Rotterdam should approach a platform such as EU-IDRP through a staged and limited process. The most realistic starting point would be a focused pilot around one cross-infrastructure disruption scenario. Such a pilot should involve a limited group of actors, a clear coordination problem, controlled information-sharing rules and an explicit link to existing crisis-management and operational routines. The aim should therefore be to test whether the platform reduces coordination burden, supports shared

awareness and protects sensitive information. Only after such value is clearly demonstrated should greater expansion be considered.

This means that platform development should begin as a governance process rather than as a technical rollout. Before actors can rely on a shared platform, they need to agree on its purpose, ownership, access rules, data safeguards, user roles, relation to existing systems and long-term maintenance. In this sense, the platform's practicability depends on the institutional work that makes digital coordination trustworthy and useful.

The addressed research however has presented several important limitations. It is based on a qualitative single-case study of the Port of Rotterdam. The case is information-rich and analytically useful, but the findings cannot be statistically generalized to all ports. The empirical material is also based on ten expert interviews. These interviews cover several relevant actor types, but they do not represent and cover the whole port ecosystem mechanism. For this reason, additional perspectives and points of views from terminal operators, logistics firms, road transport actors, telecom providers, emergency services, regulators and private technology providers would significantly strengthen the analysis. The study also focused on governance and organizational feasibility. For this reason, it did not test a fully functional technical prototype, evaluate interface design, measure operational effectiveness or reconstruct any real disruption event. EU-IDRP was solely treated as a conceptual object that has allowed different actors to reflect on actual and conceptual platform feasibility. For this reason, the findings identify conditions for possible adoption and embedding, leaving aside evidence of actual platform performance.

Relevant future research could build on this thesis by testing the findings through validation workshops, scenario-based exercises or pilot studies. For example, a concrete mock-up or prototype would also be helpful for actors to evaluate usability, access levels, information categories and dependency visualizations in a more practical way. Additionally, comparative research across other European ports could further show which specific governance conditions are particular to Rotterdam and which are more generally relevant for other large port ecosystems.

Counterintuitively, the final reflection and contribution of this thesis is that digital resilience is not uniquely achieved by technology alone. That is, in a complex port ecosystem, resilience depends on the actual ability of distributed actors to be in a position to share relevant information, protect sensitive data, understand each other's responsibilities and needs, and coordinate across institutional boundaries. For this reason, a platform can support this process, but it cannot replace the governance arrangements that today make coordination possible. EU-IDRP is therefore most valuable when meant as a tool for governed shared awareness. That is, a way to help actors to interpret cross-infrastructure disruption together, while preserving the trust, respecting responsibility and institutional legitimacy on which port resilience highly depends.

References

- Ahlin, E. M. (2019). Semi-structured interviews with expert practitioners: Their validity and significant contribution to translational research. In *SAGE Research Methods Cases Part 2*. SAGE Publications. <https://doi.org/10.4135/9781526466037>
- Ahmed, S. K., Mohammed, R. A., Nashwan, A. J., Ibrahim, R. H., Abdalla, A. Q., Ameen, B. M. M., & Khdir, R. M. (2025). Using thematic analysis in qualitative research. *Journal of Medicine, Surgery, and Public Health*, 6, Article 100198. <https://doi.org/10.1016/j.glmedi.2025.100198>
- Ansell, C., & Gash, A. (2008). Collaborative governance in theory and practice. *Journal of Public Administration Research and Theory*, 18(4), 543–571. <https://doi.org/10.1093/jopart/mum032>
- Arvidsson, B., Johansson, J., & Guldaker, N. (2021). Critical infrastructure, geographical information science and risk governance: A systematic cross-field review. *Reliability Engineering & System Safety*, 213, Article 107741. <https://doi.org/10.1016/j.res.2021.107741>
- Balakrishnan, S., Jin, L., Cassottana, B., Costa, A., & Sansavini, G. (2024). Developing resilience pathways for interdependent infrastructure networks: A simulation-based approach with consideration to risk preferences of decision-makers. *Sustainable Cities and Society*, 115, Article 105795. <https://doi.org/10.1016/j.scs.2024.105795>
- Bharosa, N., Lee, J., & Janssen, M. (2010). Challenges and obstacles in sharing and coordinating information during multi-agency disaster response: Propositions from field exercises. *Information Systems Frontiers*, 12, 49–65. <https://doi.org/10.1007/s10796-009-9174-z>
- Brucherseifer, E., Winter, H., Mentges, A., Mühlhäuser, M., & Hellmann, M. (2021). Digital twin conceptual framework for improving critical infrastructure resilience. *at – Automatisierungstechnik*, 69(12), 1062–1080. <https://doi.org/10.1515/auto-2021-0104>
- C40 Cities Climate Leadership Group. (2019). *How to manage infrastructure interdependencies and cascading risk*. C40 Knowledge Hub. https://www.c40knowledgehub.org/s/article/How-to-address-infrastructure-interdependencies-when-adapting-to-climate-change?language=en_US
- Cao, Y., Xin, X., Jarumaneeroj, P., Li, H., Feng, Y., Wang, J., Wang, X., Pyne, R., & Yang, Z. (2025). Data-driven resilience analysis of the global container shipping network against two cascading failures. *Transportation Research Part E: Logistics and Transportation Review*, 193, Article 103857. <https://doi.org/10.1016/j.tre.2024.103857>
- Chandra, D. R., & van Hillegerberg, J. (2018). Governance of inter-organizational systems: A longitudinal case study of Rotterdam's Port Community System. *International Journal of Information Systems and Project Management*, 6(2), 47–68. <https://doi.org/10.12821/ijispm060203>
- Comfort, L. K. (2007). Crisis management in hindsight: Cognition, communication, coordination, and control. *Public Administration Review*, 67(s1), 189–197. <https://doi.org/10.1111/j.1540-6210.2007.00827.x>
- Cools, F., Van Duin, M., & Wijkhuijs, V. (2017). *GRIP en de flexibele toepassing ervan*. Instituut Fysieke Veiligheid.

- De Paoli, S. (2024). Performing an inductive thematic analysis of semi-structured interviews with a large language model: An exploration and provocation on the limits of the approach. *Social Science Computer Review*, 42(4), 997–1019. <https://doi.org/10.1177/08944393231220483>
- Delacroix, S., & Lawrence, N. D. (2019). Bottom-up data trusts: Disturbing the one size fits all approach to data governance. *International Data Privacy Law*, 9(4), 236–252. <https://doi.org/10.1093/idpl/ipz014>
- Delft University of Technology. (2022). *Human Research Ethics: Checklist for Human Research* (Version January 2022). Unpublished institutional checklist.
- Dooms, M., van der Lugt, L., & de Langen, P. W. (2013). International strategies of port authorities: The case of the Port of Rotterdam Authority. *Research in Transportation Business & Management*, 8, 148–157. <https://doi.org/10.1016/j.rtbm.2013.06.004>
- Emerson, K., Nabatchi, T., & Balogh, S. (2012). An integrative framework for collaborative governance. *Journal of Public Administration Research and Theory*, 22(1), 1–29. <https://doi.org/10.1093/jopart/mur011>
- Eslami Andargoli, A., Bernus, P., & Kandjani, H. (2013). Analysis of interoperability in the Queensland disaster management system. In *Proceedings of the 15th International Conference on Enterprise Information Systems* (pp. 310–317). <https://doi.org/10.5220/0004443503100317>
- European Commission. (2023). *Common Information Sharing Environment (CISE): Governance structure for the operational phase*.
- European Union Agency for Cybersecurity. (2020). *Cyber risk management for ports: Guidelines for cybersecurity in the maritime sector*. <https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Guidelines%20-%20Cyber%20Risk%20Management%20for%20Ports.pdf>
- European Parliament & Council of the European Union. (2019). Regulation (EU) 2019/1239 of the European Parliament and of the Council of 20 June 2019 establishing a European Maritime Single Window environment and repealing Directive 2010/65/EU. *Official Journal of the European Union*. <http://data.europa.eu/eli/reg/2019/1239/oj>
- European Parliament & Council of the European Union. (2020). Regulation (EU) 2020/1056 of the European Parliament and of the Council of 15 July 2020 on electronic freight transport information. *Official Journal of the European Union*. <http://data.europa.eu/eli/reg/2020/1056/oj>
- European Parliament & Council of the European Union. (2022a). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive). *Official Journal of the European Union*. <http://data.europa.eu/eli/dir/2022/2555/oj>
- European Parliament & Council of the European Union. (2022b). Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. *Official Journal of the European Union*. <http://data.europa.eu/eli/dir/2022/2557/oj>

European Parliament & Council of the European Union. (2022c). Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). *Official Journal of the European Union*. <http://data.europa.eu/eli/reg/2022/868/oj>

European Parliament & Council of the European Union. (2023). Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). *Official Journal of the European Union*. <http://data.europa.eu/eli/reg/2023/2854/oj>

Flyvbjerg, B. (2006). Five misunderstandings about case-study research. *Qualitative Inquiry*, 12(2), 219–245. <https://doi.org/10.1177/1077800405284363>

Gemeente Rotterdam. (2016). *Rotterdam resilience strategy: Ready for the 21st century* [Consultation document]. https://s3.eu-central-1.amazonaws.com/storage.resilientrotterdam.nl/uploads/2016/05/09115601/ResilienceBoekIntegraal_compleet_ENG_Onlinecompressed.pdf

Groenendaal, J., & Helsloot, I. (2021). Why technology not always adds value to crisis managers during crisis: The case of the Dutch nation-wide crisis management system LCMS. In A. Adrot, R. Grace, K. Moore, & C. Zobel (Eds.), *Proceedings of the 18th International Conference on Information Systems for Crisis Response and Management* (pp. 936–945).

Huck, A., Monstadt, J., Driessen, P. P. J., & Rudolph-Cleff, A. (2021). Towards resilient Rotterdam? Key conditions for a networked approach to managing urban infrastructure risks. *Journal of Contingencies and Crisis Management*, 29(1), 12–22. <https://doi.org/10.1111/1468-5973.12295>

Little, R. G. (2002). Controlling cascading failure: Understanding the vulnerabilities of interconnected infrastructures. *Journal of Urban Technology*, 9(1), 109–123. <https://doi.org/10.1080/106307302317379855>

Liu, W., Shan, M., Zhang, S., Zhao, X., & Zhai, Z. (2022). Resilience in infrastructure systems: A comprehensive review. *Buildings*, 12(6), Article 759. <https://doi.org/10.3390/buildings12060759>

Lu, Z., & Qiu, W. (2025). Resilience analysis of seaport-dry-port network in container transport: Multi-stage load redistribution dynamics following cascade failure. *Systems*, 13(4), Article 299. <https://doi.org/10.3390/systems13040299>

Lukassen, B., Genga, L., & Zhang, Y. (2023). Discovering explicit scale-up criteria in crisis response with decision mining. In M. Sellmann & K. Tierney (Eds.), *Learning and Intelligent Optimization: 17th International Conference, LION 17, Nice, France, June 4–8, 2023, Revised Selected Papers* (pp. 459–474). Springer. https://doi.org/10.1007/978-3-031-44505-7_31

Luokkala, P., Nikander, J., Korpi, J., Virrantaus, K., & Torkki, P. (2017). Developing a concept of a context-aware common operational picture. *Safety Science*, 93, 277–295. <https://doi.org/10.1016/j.ssci.2016.12.009>

Mohsendokht, M., Kontovas, C., Chang, C.-H., Qu, Z., Li, H., & Yang, Z. (2026). Resilience analysis of seaports: A critical review of development and research directions. *Maritime Policy & Management*, 53(2), 227–262. <https://doi.org/10.1080/03088839.2025.2483410>

- Nederlands Instituut Publieke Veiligheid. (n.d.). *Landelijk Crisis Management Systeem (LCMS)*. Retrieved July 20, 2026, from <https://nipv.nl/informatievoorziening/voorzieningen/landelijk-crisis-management-systeem/>
- Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods*, 16(1), 1–13. <https://doi.org/10.1177/1609406917733847>
- OECD. (2019). *Good governance for critical infrastructure resilience*. OECD Publishing. <https://doi.org/10.1787/02f0e5a0-en>
- Ollivier, P., Sahu, S. P., & Saragiotis, P. (Eds.). (2024). *Port community systems: Lessons from global experience*. World Bank. <https://doi.org/10.1596/42269>
- Ouyang, M. (2014). Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering & System Safety*, 121, 43–60. <https://doi.org/10.1016/j.ress.2013.06.040>
- Port of Rotterdam Authority. (n.d.). *Port Community System*. Retrieved June 22, 2026, from <https://www.portofrotterdam.com/en/services/online-tools/port-community-system>
- Portbase. (n.d.). *About us*. Retrieved July 20, 2026, from <https://www.portbase.com/en/about-us/>
- Provan, K. G., & Kenis, P. (2008). Modes of network governance: Structure, management, and effectiveness. *Journal of Public Administration Research and Theory*, 18(2), 229–252. <https://doi.org/10.1093/jopart/mum015>
- Punt, E., Monstadt, J., Frank, S., & Witte, P. (2023a). Beyond the dikes: An institutional perspective on governing flood resilience at the Port of Rotterdam. *Maritime Economics & Logistics*, 25(2), 230–248. <https://doi.org/10.1057/s41278-022-00234-w>
- Punt, E., Monstadt, J., Frank, S., & Witte, P. (2023b). Navigating cyber resilience in seaports: Challenges of preparing for cyberattacks at the Port of Rotterdam. *Digital Policy, Regulation and Governance*, 25(4), 420–438. <https://doi.org/10.1108/DPRG-12-2022-0150>
- Ridder, H.-G. (2017). The theory contribution of case study research designs. *Business Research*, 10, 281–305. <https://doi.org/10.1007/s40685-017-0045-z>
- Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 21(6), 11–25. <https://doi.org/10.1109/37.969131>
- Rydén Sonesson, T., Johansson, J., & Cedergren, A. (2021). Governance and interdependencies of critical infrastructures: Exploring mechanisms for cross-sector resilience. *Safety Science*, 142, Article 105383. <https://doi.org/10.1016/j.ssci.2021.105383>
- Spaans, M., & Waterhout, B. (2017). Building up resilience in cities worldwide—Rotterdam as participant in the 100 Resilient Cities Programme. *Cities*, 61, 109–116. <https://doi.org/10.1016/j.cities.2016.05.011>

- Steen-Tveit, K., & Munkvold, B. E. (2021). From common operational picture to common situational understanding: An analysis based on practitioner perspectives. *Safety Science*, 142, Article 105381. <https://doi.org/10.1016/j.ssci.2021.105381>
- Therrien, M.-C., Manrique Rueda, G., Normandin, J.-M., Veillette, S., Chelihi, M., & Arnaud, J. (2024). The common operating picture as a collaborative governance tool for urban resilience. *Journal of Contingencies and Crisis Management*. <https://doi.org/10.1111/1468-5973.12500>
- Tijan, E., Jović, M., Panjako, A., & Žgaljić, D. (2021). The role of port authority in port governance and Port Community System implementation. *Sustainability*, 13(5), Article 2795. <https://doi.org/10.3390/su13052795>
- Treurniet, W. (2022). *Between chaos and continuity: A common operational picture in support of emergency response networks* [Doctoral dissertation, Vrije Universiteit Amsterdam].
- Treurniet, W., Korpel, M., Suitela, V., & van Dijk, E. (2023). *Referentiekader netcentrische crisisbeheersing 2023: Informatiegestuurd optreden in het netwerk van de crisisbeheersing* (Version 1.0). Nederlands Instituut Publieke Veiligheid. <https://nipv.nl/wp-content/uploads/2023/04/20230330-NIPV-Referentiekader-Netcentrische-Crisisbeheersing.pdf>
- Tsoufas, G. T. (2026). Port resilience: A systematic literature review. *Maritime Economics & Logistics*, 28, 388–408. <https://doi.org/10.1057/s41278-025-00326-3>
- United Nations Conference on Trade and Development. (2022). *Building capacity to manage risks and enhance resilience: A guidebook for ports* (UNCTAD/TCS/DTL/INF/2022/3). <https://unctad.org/publication/building-capacity-manage-risks-and-enhance-resilience-guidebook-ports>
- Van de Ven, J., van Rijk, R., Essens, P., & Frinking, E. (2008). Network centric operations in crisis management. In F. Fiedrich & B. Van de Walle (Eds.), *Proceedings of the 5th International ISCRAM Conference* (pp. 764–773).
- Van den Bosch, F. A. J., Hollen, R., Volberda, H. W., & Baaij, M. G. (2011). *The strategic value of the Port of Rotterdam for the international competitiveness of the Netherlands: A first exploration*. Rotterdam School of Management, Erasmus University Rotterdam.
- Wolbers, J. (2022). Understanding distributed sensemaking in crisis management: The case of the Utrecht terrorist attack. *Journal of Contingencies and Crisis Management*, 30(2), 166–178. <https://doi.org/10.1111/1468-5973.12382>
- Zhang, D., Tao, J., Wan, C., Huang, L., & Yang, M. (2024). Resilience analysis of maritime transportation networks: A systematic review. *Transportation Safety and Environment*, 6, Article tdae009. <https://doi.org/10.1093/tse/tdae009>

Appendix

Appendix 1. Inductive codebook

This appendix documents the inductive movement from first-cycle descriptive coding to second-cycle analytical codes and final empirical themes. First-cycle codes stayed close to interview language and captured concrete statements about disruption, coordination, information sharing, interoperability, data sensitivity, trust and platform feasibility. In the second cycle, related first-cycle codes were consolidated into broader analytical codes. These analytical codes were then synthesized into the four final themes used in the findings chapter.

Code tree overview

F1. Cross-infrastructure disruption becomes a coordination problem before it becomes a formal crisis

- **F1-C1 Interdependencies and cascading effects as disruption context:** Cross-infrastructure dependency; Infrastructure failure propagation; Common-cause infrastructure failure; Cross-boundary disruption effects; Cyber-physical communication disruption; Chain-level resilience perspective; Multi-modal transport interdependency; Energy dependency of port operations; Physical port access dependency
- **F1-C2 Routine operational coordination through existing relationships:** Informal operational coordination; Existing operational communication lines; Control-center coordination; Human-mediated crisis coordination; Ad hoc coordination practices; Existing bilateral notification practices; Operational coordination role
- **F1-C3 Formal crisis escalation structures and thresholds:** Formal mayoral escalation; Hierarchical crisis authority; Multi-sector escalation threshold; Crisis activation thresholds and mandates; Multi-level crisis escalation structure; Government-led crisis management; Pre-agreed crisis roles; Formalized crisis governance structure
- **F1-C4 Middle-layer coordination gap / grey space:** Missing intermediate escalation layer; Lack of strategic coordination for intermediate disruptions; Operational incident handling vs crisis management; Limited attention to smaller crises; Crisis organization maturity gap; Line organization limits crisis response; Coordination structure without system support
- **F1-C5 Distributed authority and coordination without command:** Sectoral mandate boundary; Formal authority versus decision competence; Conflicting decision rights; Fragmented legal responsibilities; Coordination without command authority; Functional column autonomy; Limited delegated authority in crisis teams; Coordination bodies lack enforcement power

F2. Existing systems create partial visibility, but not shared system-level awareness

- **F2-C1 Existing systems and sectoral/role-based visibility:** Existing national information-sharing platform; Digital information-exchange platform; Existing crisis-management platform; Existing operational information platform; Existing ITSM tools as platform basis; Restricted platform access and licensing; Domain-specific impact visibility
- **F2-C2 Missing common operational picture / system-level overview:** Shared operational picture; Common operational picture as coordination bottleneck; Shared operational understanding; Cross-domain impact visibility; Dependent actor situational awareness; Affected area visibility; External network risk visibility
- **F2-C3 Fragmented information flows, silos and parallel channels:** Siloed disruption management; No shared external coordination platform; Fragmented organizational responsibilities; Fragmented crisis governance; Non-participation in shared crisis platform; Parallel communication channels undermine platform use; Uncontrolled platform fragmentation
- **F2-C4 Actionable disruption information needs:** Incident impact assessment; Expected disruption duration; Other actors' response intentions; Basic operational information needs; Dangerous-goods information need; Incident-characterization information; Safety and environmental risk information; Passenger-transfer coordination need; Infrastructure usability status; Estimated time to recovery
- **F2-C5 Shared problem framing and cross-actor sense-making:** Platform as sense-making tool; Scenario-based sense-making; Joint sense-making among infrastructure managers; Shared problem framing; Intersectoral understanding; Critical dilemma sharing; Plain-language crisis information; Problem-centred information need; Information overload and essence extraction

F3. Interoperability is socio-technical alignment, not only technical integration

- **F3-C1 Technical integration and model/data coupling:** Model coupling across sectors; Data as integration layer; Data-mediated model interoperability; Bring-your-own-model architecture; Cross-system technical integration; Technical integration requirement; Data interchange standards; Input-output transparency; Data format incompatibility; Temporal data mismatch; Model integration complexity
- **F3-C2 Semantic alignment and common language:** Semantic interoperability barrier; Semantic alignment requirement; Shared disruption definition; Shared meaning as minimum interoperability; Semantic misalignment risk; Cross-actor terminology mismatch; Information translation role; Common language for rapid crisis response; Different crisis meaning across actors; Role-name similarity but mandate difference
- **F3-C3 Organizational/procedural interoperability and mandate alignment:** Socio-technical interoperability; Multi-dimensional interoperability requirement; Interoperability barriers across organizations; Need for crisis-management interoperability; Standardized crisis roles and terminology; Plug-in compatibility between crisis organizations; Platform embedded in crisis organization; Implementation coordination requirement; Clear operational rulebook
- **F3-C4 Legal, accountability and institutional alignment:** Legal data-sharing arrangements; Data governance accountability; Legal interoperability as enabling condition; Legal backbone for platform participation; Binding participation commitment; Contractual basis for collaboration; Cybersecurity agreements for data sharing; Decision rights over data access; Data-owner-controlled sharing
- **F3-C5 Operational fit and technology-first/dashboard risk:** Platform implementation workload; FTE capacity constraint for platform adoption; Human capacity as implementation constraint; Organizational burden of participation; Platform usability for crisis actors; Low-threshold platform interface; User-centred operational interface; No additional workload requirement; System overlap as adoption barrier; Technology-first platform failure risk; Dashboard solutionism

F4. The most valuable information to share is often also the most sensitive

- **F4-C1 Sensitive operational, security and commercial information:** Data-sharing reluctance; Critical infrastructure data sensitivity; Security-based data restriction; Commercial sensitivity of asset data; Asset-location exploitation risk; Privacy constraints on infrastructure data; Consumer-identifiable operational data; Competitive sensitivity of operational data; Network architecture confidentiality; OT system sensitivity; IT/OT infrastructure sensitivity
- **F4-C2 Cause/context information as high-value but sensitive:** Sharing disruption cause information; Sharing disruption background context; Sabotage as shared warning signal; Shared vulnerability warning; Root-cause and response-progress information; Root-cause and recovery planning information; Near-miss incident reporting; Weak-signal reporting; Anticipatory cross-actor learning; Cross-actor learning from incident reporting
- **F4-C3 Controlled visibility, authorisation and data minimisation:** Access control safeguards; User screening requirement; Federated data-sharing workaround; Minimum viable data sharing; Purpose-limited data sharing; Role-based authorization for platform access; Data-owner access control; Actor-controlled visibility rules; Data classification-based sharing; Confidentiality-integrity-availability classification; Tiered data sensitivity levels; Revocable information access
- **F4-C4 Trust, reciprocity and perceived benefit as participation condition:** Trust as prerequisite for participation; Human trust in socio-technical systems; Trust as data access enabler; Trust enables deeper data sharing; Trust-building through outreach; Informal trust as coordination asset; Trust as willingness to share; Trust as reciprocal information responsiveness; Multi-level trust requirement; Strategic-level trust barrier; Reliable and useful information; Reciprocal value for data sharing
- **F4-C5 Ownership, sponsorship and formal agreements/regulation:** Consortium-based platform ownership; Distributed platform ownership; Government-led platform governance; National public authority platform hosting; Ministry-led platform governance; Multilateral platform governance agreement; Transparent platform governance; Non-authority platform governance preference; Ministerial ownership of crisis platform; Trusted platform sponsor; Institutional backing for platform legitimacy; Responsible platform owner; Mandated platform use; High-level mandate for platform adoption; High-level organizational anchor

Operational codebook and inductive trail

Table 1. Inductive codebook: first-cycle indicators, analytical codes, final themes and evidence examples.

Final theme	Second-cycle analytical code	Representative granular first-cycle indicators	Coding definition and use rule	Illustrative evidence extracts	Evidence coverage
F1. Coordination before formal crisis	F1-C1 Interdependencies and cascading effects as disruption context	Cross-infrastructure dependency; Infrastructure failure propagation; Common-cause infrastructure failure; Cross-boundary disruption effects; Cyber-physical communication disruption; Chain-level resilience perspective; Multi-modal transport interdependency; Energy dependency of port operations; Physical port access dependency	Actors describe the port/infrastructure environment as interconnected, where disruption may cross technical, organisational, modal or supply-chain boundaries. Use when: Use for dependencies, knock-on effects, cross-impact, cyber-physical links, logistics spillovers, multimodal dependencies.	SEG001: What's in my resilience strategy, as a very important point is to take into account the resilience of the whole chain not one company like ProRail but the whole chain especially the transport chain... a lot of modalities come together especially in Rotterdam because of course the railway traffic and the traffic on the roads but also on the water, from the...	Segments: 10 Core/support: 6/4 Actors: 7
F1. Coordination before formal crisis	F1-C2 Routine operational coordination through existing relationships	Informal operational coordination; Existing operational communication lines; Control-center coordination; Human-mediated crisis coordination; Ad hoc coordination practices; Existing bilateral notification practices; Operational coordination role	Actors describe day-to-day coordination that already exists through people, control rooms, bilateral contacts, recurring calls or informal relationships. Use when: Use for operational contacts, control-centre coordination, phone calls, WhatsApp, known counterparts, existing practices that work in routine incidents.	SEG011: Coordination is not mainly by systems but mostly by people with a phone, pen and paper, and tools like SpoorWeb... to inform people, but not to coordinate actions in the way you mean... There is a lot of coordination and many calls, but a lot of it is ad hoc. We have structures, but we do not have systems to support them.	Segments: 2 Core/support: 2/0 Actors: 2
F1. Coordination before formal crisis	F1-C3 Formal crisis escalation structures and thresholds	Formal mayoral escalation; Hierarchical crisis authority; Multi-sector escalation threshold; Crisis activation thresholds and mandates; Multi-level crisis escalation structure; Government-led crisis management; Pre-agreed crisis roles; Formalized crisis governance structure	Actors describe formal crisis-management arrangements, escalation thresholds, mayoral/safety-region roles, GRIP/LCMS or government takeover logic. Use when: Use for formal authority, GRIP, mayor, safety region, crisis teams, national/ministry-level escalation, legal takeover thresholds.	SEG016: To a certain extent, we are the ones that can decide... what we do and how we manage our risk... But with such a law... if that threat hits a certain level, the government takes over... because it's a societal disruption.	Segments: 5 Core/support: 3/2 Actors: 4
F1. Coordination before formal crisis	F1-C4 Middle-layer coordination gap / grey space	Missing intermediate escalation layer; Lack of strategic coordination for intermediate disruptions; Operational incident handling vs crisis management; Limited attention to smaller crises; Crisis organization maturity gap; Line organization limits crisis response; Coordination structure without system support	Actors describe the empirical gap between routine operational handling and full formal crisis escalation. Use when: Use when actors describe "nothing in between," smaller crises being overlooked, ad hoc handling of serious-but-not-disaster-level disruptions, or absence of strategic coordination.	SEG009: If it's a smaller disruption, then... operational organizations... find each other, really the 24-7 people... But if it's a really big disaster, then it's the mayor, but there's nothing in between. It's small or big... for the cases that are in between... there's just operational coordination... but not... a strategic view on the situation.	Segments: 6 Core/support: 3/3 Actors: 4
F1. Coordination before formal crisis	F1-C5 Distributed authority and coordination without command	Sectoral mandate boundary; Formal authority versus decision competence; Conflicting decision rights; Fragmented legal responsibilities; Coordination without command authority; Functional column autonomy; Limited delegated authority in crisis teams; Coordination bodies lack enforcement power	Actors describe situations where multiple organisations keep their own mandates and responsibilities, requiring coordination without one actor fully commanding the others. Use when: Use for mandate conflicts, functional-column authority, unclear lead, coordination across independent organisations, decision rights divided across actors.	SEG014: Every organization, like ProRail, has its own background and legislations of where they are responsible for the crisis... the safety region is like a technical commander, but cannot say you have to do that... in the functional column, there are about 42 different organizations who have their own authorities.	Segments: 9 Core/support: 5/4 Actors: 3

Final theme	Second-cycle analytical code	Representative granular first-cycle indicators	Coding definition and use rule	Illustrative evidence extracts	Evidence coverage
F2. Partial visibility vs system awareness	F2-C1 Existing systems and sectoral/role-based visibility	Existing national information-sharing platform; Digital information-exchange platform; Existing crisis-management platform; Existing operational information platform; Existing ITSM tools as platform basis; Restricted platform access and licensing; Domain-specific impact visibility	Actors describe existing tools or channels that provide useful but partial visibility, often limited by sector, role, community or need-to-know logic. Use when: Use for SpoorWeb, LCMS, FERM signal group, MyTerminal, internal dashboards, role-based views, sectoral information-sharing arrangements.	SEG018: SpoorWeb... is our incident-management tool... one central source of information for all participants on a need-to-know basis and, of course, role-based. Some players have all the information... But when you only have a task to manage, you have visibility of the task... but not all the information.	Segments: 6 Core/support: 4/2 Actors: 4
F2. Partial visibility vs system awareness	F2-C2 Missing common operational picture / system-level overview	Shared operational picture; Common operational picture as coordination bottleneck; Shared operational understanding; Cross-domain impact visibility; Dependent actor situational awareness; Affected area visibility; External network risk visibility	Actors explicitly describe the absence, incompleteness or difficulty of creating a shared operational picture across organisations or infrastructures. Use when: Use for lack of common operational picture, spending time constructing the picture, not seeing where action is possible, no shared system-level view.	SEG019: We do not have a common operational picture of where we can do something... sources already internally available at ProRail but not brought together... every internal ProRail party is sitting on its own data. It is not the availability of data, but a real organisation of power.	Segments: 4 Core/support: 2/2 Actors: 3
F2. Partial visibility vs system awareness	F2-C3 Fragmented information flows, silos and parallel channels	Siloed disruption management; No shared external coordination platform; Fragmented organizational responsibilities; Fragmented crisis governance; Non-participation in shared crisis platform; Parallel communication channels undermine platform use; Uncontrolled platform fragmentation	Actors describe information being split across internal silos, parallel channels, phone/WhatsApp/email, separate datasets or unconnected systems. Use when: Use for fragmented communication, information loss, data sitting with separate parties, parallel channels, lack of integration.	SEG022: ProRail doesn't use the LCMS... when all the emergency services are on that system and ProRail was not on the system, they have to telephone or WhatsApp... that's a loss of information... You have to share your information in a real time connected system.	Segments: 7 Core/support: 6/1 Actors: 4
F2. Partial visibility vs system awareness	F2-C4 Actionable disruption information needs	Incident impact assessment; Expected disruption duration; Other actors' response intentions; Basic operational information needs; Dangerous-goods information need; Incident-characterization information; Safety and environmental risk information; Passenger-transfer coordination need; Infrastructure usability status; Estimated time to recovery	Actors specify which information would be operationally useful during disruption. Use when: Use for expected duration, location, ETA, impact area, root cause, dangerous goods, capacity, response status, recovery progress, who needs what.	SEG028: It would be very helpful if you could have some impression about what's the impact, how big is the incident, what is the area that is affected, and what is the expected time... and what will other modalities... do... a good forecast... and the way that parties will deal with it... could help reduce or prevent cascade effects.	Segments: 7 Core/support: 3/4 Actors: 5
F2. Partial visibility vs system awareness	F2-C5 Shared problem framing and cross-actor sense-making	Platform as sense-making tool; Scenario-based sense-making; Joint sense-making among infrastructure managers; Shared problem framing; Intersectoral understanding; Critical dilemma sharing; Plain-language crisis information; Problem-centred information need; Information overload and essence extraction	Actors stress that the main issue is understanding the shared problem, dilemma, impact or meaning of the situation rather than collecting more technical detail. Use when: Use for shared problem, dilemma, "why is this a problem," essence, intersectoral understanding, interpretation, sense-making..	SEG025: The whole goal of LCMS and netcentric way of working is... to share your critical dilemmas, and not your whole information and all of your data, but only the things that are relevant for your situation and your dilemmas... it should be readable for anyone... someone who is not technical involved.	Segments: 7 Core/support: 6/1 Actors: 3
F3. Interoperability as socio-technical alignment	F3-C1 Technical integration and model/data coupling	Model coupling across sectors; Data as integration layer; Data-mediated model interoperability; Bring-your-own-model architecture; Cross-system technical integration; Technical integration requirement; Data interchange standards; Input-output transparency; Data format incompatibility; Temporal data mismatch; Model integration complexity	Actors describe the technical layer of connecting systems, datasets, models, dashboards, sensors, APIs or simulation tools. Use when: Use for model coupling, data formats, update frequency, adapters, platform architecture, technical representation of dependencies.	SEG032: Movici is a platform which allows for you to plug in these different models together and couple them... data comes out of these models and they go into these data sets and then from these data sets, they go onto some other model.	Segments: 6 Core/support: 1/5 Actors: 2

Final theme	Second-cycle analytical code	Representative granular first-cycle indicators	Coding definition and use rule	Illustrative evidence extracts	Evidence coverage
F3. Interoperability as socio-technical alignment	F3-C2 Semantic alignment and common language	Semantic interoperability barrier; Semantic alignment requirement; Shared disruption definition; Shared meaning as minimum interoperability; Semantic misalignment risk; Cross-actor terminology mismatch; Information translation role; Common language for rapid crisis response; Different crisis meaning across actors; Role-name similarity but mandate difference	Actors describe meaning-level interoperability: the same words, data categories or concepts may mean different things across organisations. Use when: Use for same terms/different meanings, defining disruption/grid/crisis, common language, translation between organisations. Exclude:	SEG033: We're realizing that this interoperability seems to be a great issue. We need to get the semantics right... not just what variables actually mean and how they're represented, but how the data itself is represented... different encodings... different frequency of updates.	Segments: 6 Core/support: 5/1 Actors: 4
F3. Interoperability as socio-technical alignment	F3-C3 Organisational/procedural interoperability and mandate alignment	Socio-technical interoperability; Multi-dimensional interoperability requirement; Interoperability barriers across organizations; Need for crisis-management interoperability; Standardized crisis roles and terminology; Plug-in compatibility between crisis organizations; Platform embedded in crisis organisation; Implementation coordination requirement; Clear operational rulebook	Actors describe the need to align organisational routines, roles, procedures, training, crisis structures or mandates so actors can work together. Use when: Use for aligned procedures, compatible crisis roles, training/certification, plug-in points between crisis organisations, organisational readiness.	SEG037: Every organization has its own character, its own names of crisis management rules, its own authorities, duties, and the more different the organizations are organized, the harder the collaboration will be.	Segments: 7 Core/support: 5/2 Actors: 2
F3. Interoperability as socio-technical alignment	F3-C4 Legal, accountability and institutional alignment	Legal data-sharing arrangements; Data governance accountability; Legal interoperability as enabling condition; Legal backbone for platform participation; Binding participation commitment; Contractual basis for collaboration; Cybersecurity agreements for data sharing; Decision rights over data access; Data-owner-controlled sharing	Actors describe formal or institutional conditions required for interoperable action and data use. Use when: Use for legal ground, accountability, liability, contracts, MOUs, regulation, institutional permission, data-leak responsibility.	SEG045: Perhaps it just has to be legally binding. There has to be a why... the why has to be strong, and I think it has to have a legal ground. We have to ensure that none of the parties is able to back out.	Segments: 7 Core/support: 5/2 Actors: 3
F3. Interoperability as socio-technical alignment	F3-C5 Operational fit and technology-first/dashboard risk	Platform implementation workload; FTE capacity constraint for platform adoption; Human capacity as implementation constraint; Organizational burden of participation; Platform usability for crisis actors; Low-threshold platform interface; User-centred operational interface; No additional workload requirement; System overlap as adoption barrier; Technology-first platform failure risk; Dashboard solutionism	Actors warn that a platform will fail if it adds workload, duplicates existing tools, over-focuses on technical dashboards, or does not fit operational routines. Use when: Use for "not another dashboard," "should not take time," low-level/intuitive use, operational burden, use existing platforms, technology-first risk.	SEG040: The solution is not on a technical, more technical information, more depth. The solution is in intersectoral understanding... almost every technical platform or digital platform is focusing on the technical aspects, and they all fail or end up like a sectoral helping system.	Segments: 10 Core/support: 9/1 Actors: 3

Final theme	Second-cycle analytical code	Representative granular first-cycle indicators	Coding definition and use rule	Illustrative evidence extracts	Evidence coverage
F4. Valuable information is sensitive	F4-C1 Sensitive operational, security and commercial information	Data-sharing reluctance; Critical infrastructure data sensitivity; Security-based data restriction; Commercial sensitivity of asset data; Asset-location exploitation risk; Privacy constraints on infrastructure data; Consumer-identifiable operational data; Competitive sensitivity of operational data; Network architecture confidentiality; OT system sensitivity; IT/OT infrastructure sensitivity	Actors identify information as confidential, security-sensitive, commercially sensitive, privacy-sensitive or reputationally risky. Use when: Use for network architecture, OT/IT exposure, confidential data, cyber indicators, commercial sensitivity, privacy and security constraints.	SEG050: We do not easily share our data because we have confidential data, we have internal data, there is lots of safeguards to monitor what data we share outside.	Segments: 7 Core/support: 4/3 Actors: 5
F4. Valuable information is sensitive	F4-C2 Cause/context information as high-value but sensitive	Sharing disruption cause information; Sharing disruption background context; Sabotage as shared warning signal; Shared vulnerability warning; Root-cause and response-progress information; Root-cause and recovery planning information; Near-miss incident reporting; Weak-signal reporting; Anticipatory cross-actor learning; Cross-actor learning from incident reporting	Actors explain that the cause or background of a disruption is valuable to others, but may also be sensitive. Use when: Use for root cause, sabotage, heat/cyber/near-miss context, incident background, why something happened, warning value for other actors.	SEG048: To only share aggregated information... I choose to give only a limited amount of information... I might hold back information that might be interesting for other parties. For instance, about the cause of the disruption... sabotage... extreme heat causing computers to collapse... other companies can anticipate and ask themselves, could this happen also to...	Segments: 2 Core/support: 1/1 Actors: 2
F4. Valuable information is sensitive	F4-C3 Controlled visibility, authorisation and data minimisation	Access control safeguards; User screening requirement; Federated data-sharing workaround; Minimum viable data sharing; Purpose-limited data sharing; Role-based authorization for platform access; Data-owner access control; Actor-controlled visibility rules; Data classification-based sharing; Confidentiality-integrity-availability classification; Tiered data sensitivity levels; Revocable information access	Actors describe ways to share information safely through limited access, authorisation, screening, role-based visibility or processed/aggregated indicators. Use when: Use for access control, authorisation, screening, classification, federated/local sharing, aggregated outputs, purpose-limited sharing.	SEG049: We should be as open as possible... Of course, we have to do some limited access and authorization procedures... People should be screened... That asks something about the governance... all the CEOs must decide... we want to share information.	Segments: 6 Core/support: 6/0 Actors: 3
F4. Valuable information is sensitive	F4-C4 Trust, reciprocity and perceived benefit as participation condition	Trust as prerequisite for participation; Human trust in socio-technical systems; Trust as data access enabler; Trust enables deeper data sharing; Trust-building through outreach; Informal trust as coordination asset; Trust as willingness to share; Trust as reciprocal information responsiveness; Multi-level trust requirement; Strategic-level trust barrier; Reliable and useful information; Reciprocal value for data sharing	Actors describe willingness to participate or share as dependent on trust, mutual benefit, reciprocity, value, openness or confidence in other actors. Use when: Use for trust as willingness to share/listen, visible benefit, reciprocal exchange, stakeholder buy-in, platform value proposition.	SEG055: The vital thing is to make organizations understand what the benefit of such a sharing platform is... that if their neighbor is affected, then also indirectly always has an effect on them. That is the most important thing to make companies understand.	Segments: 13 Core/support: 8/5 Actors: 6

Final theme	Second-cycle analytical code	Representative granular first-cycle indicators	Coding definition and use rule	Illustrative evidence extracts	Evidence coverage
F4. Valuable information is sensitive	F4-C5 Ownership, sponsorship and formal agreements/regulation	Consortium-based platform ownership; Distributed platform ownership; Government-led platform governance; National public authority platform hosting; Ministry-led platform governance; Multilateral platform governance agreement; Transparent platform governance; Non-authority platform governance preference; Ministerial ownership of crisis platform; Trusted platform sponsor; Institutional backing for platform legitimacy; Responsible platform owner; Mandated platform use; High-level mandate for platform adoption; High-level organizational anchor	Actors describe institutional embedding of the platform or data-sharing arrangement: host, owner, sponsor, agreement, alliance, regulation or mandate. Use when: Use for platform host/owner, responsible sponsor, formal agreements, multilateral agreements, ministry/government platform, legal/regulatory backbone.	SEG056: We have made a multilateral... agreement... in which we set all our expectations from companies, what we expect from them, and what they can expect from us... very transparent on how we govern... not let it be from an authority... FERM are a nongovernmental organization, we're not out for profits.	Segments: 14 Core/support: 9/5 Actors: 7

Appendix 2. Semi-structured interview protocol

The interviews followed a semi-structured protocol organized around recurring question families. The exact wording, order, and emphasis of the questions varied depending on the expertise and institutional position of each participant. The table below reconstructs the main guiding themes used across the interviews and shows how they relate to the thesis sub-questions.

Interview theme	Indicative guiding question(s)	Actor-specific emphasis	Link to sub-question
Cross-infrastructure disruption risks	What are the most relevant cross-infrastructure disruption risks in or around the Port of Rotterdam? Which infrastructure domains are most strongly connected?	Crisis-management and infrastructure actors were asked about operational disruptions, power outages, transport failures, water-related risks, cyber incidents, and cascading effects. Port and cyber-resilience actors were asked more specifically about port-domain risks, supply-chain dependencies, and digital disruption.	SQ1
Cascading effects and interdependencies	How can a disruption in one infrastructure domain create consequences for other domains? Can you give	Infrastructure and modelling experts were asked to explain how dependencies between systems such as energy,	SQ1

	examples of such cascading effects?	transport, water, ICT, and logistics can be represented or understood. Operational actors were asked about real or plausible disruption pathways affecting their own domain.	
Current coordination practices	How is coordination currently handled when a disruption affects multiple actors, sectors, or infrastructure domains? What currently works well?	Crisis-management actors were asked about GRIP, LCMS, net-centric working, safety-region coordination, and escalation structures. Infrastructure and port actors were asked about operational contacts, bilateral communication, calls, existing systems, and informal workarounds.	SQ2
Responsibilities, escalation, and decision rights	How are responsibilities, escalation steps, and decision rights currently structured during disruptions? Where do ambiguities or delays appear?	Public crisis-management actors were asked about formal roles, mayoral authority, safety-region responsibilities, and functional-column actors. Infrastructure operators were asked about internal escalation, operator autonomy, and the limits of external command.	SQ2
Information needs during disruption	What information would be most useful to receive from other actors during a disruption? What information could your organization share back?	Operational actors were asked about practical information needs such as location, expected duration, recovery status, affected assets, safety risks, response progress, and expected operational impacts.	SQ2 / SQ3
Shared situational awareness	What are the main bottlenecks to achieving a shared operational picture or shared	Crisis-management and operational actors were asked about common operational pictures,	SQ2 / SQ3

	situational awareness across organizations?	information overload, outdated information, interpretation, common language, and the need to extract the essence of a disruption.	
Governance bottlenecks	What are the main governance bottlenecks in cross-infrastructure disruption management? Are they related to fragmented information, unclear responsibilities, different incentives, legal constraints, lack of trust, or something else?	This question family was asked across most interviews, but the emphasis varied. Public actors discussed mandates and escalation; operators discussed internal priorities and organizational constraints; digital and interoperability experts discussed institutional permissions and alignment.	SQ3
Data sharing, confidentiality, and safeguards	What are the main concerns or limits around sharing operational or sensitive information? Under what conditions could data or indicators be shared?	Digital, modelling, cyber, and port actors were asked about data sensitivity, confidentiality, cybersecurity, privacy, commercial sensitivity, aggregation, local data control, and access rules.	SQ3
Trust and participation	What would make organizations willing to participate in a shared digital resilience initiative? What would they need to trust the platform and the actors behind it?	Cyber-resilience and port actors were asked about stakeholder buy-in, perceived benefits, information-sharing agreements, reciprocity, trust, and the credibility of the organization introducing or managing the platform.	SQ3 / SQ4
Interoperability and system integration	What technical, semantic, organizational, legal, or procedural interoperability issues would need to be addressed?	Digital-modelling and interoperability experts were asked about data formats, model coupling, semantic alignment, update frequency, institutional mandates, APIs, adapters, and the	SQ3 / SQ4

		limits of aggregating data.	
Platform value and usability	What would a shared cross-infrastructure digital resilience platform need to provide in order to be useful during disruptions? What would make it practical or impractical to use?	Operational actors were asked about usability, workload, system availability, simplicity, role-based information, avoiding duplication, and whether the platform would become useful or just another tool.	SQ3 / SQ4
Ownership and institutional embedding	What governance conditions, ownership arrangements, sponsorship, or institutional safeguards would be needed for such a platform to become part of real operational routines?	Infrastructure, port, cyber, and crisis-management actors were asked about ownership, public or private sponsorship, legal grounding, institutional legitimacy, integration into crisis-management routines, and long-term maintenance.	SQ4
Regulation and broader relevance	How do regulatory pressures such as NIS2, CER, or broader resilience requirements affect the need for coordination and information sharing?	Cyber-resilience and infrastructure actors were asked more directly about regulation, legal obligations, resilience pressure, and whether regulation could create incentives for participation.	SQ3 / SQ4

Appendix 3. Common oral EU-IDRP introduction used before the platform-related questions

can be summarized as follows:

For the second part of the interview, participants were asked to consider a hypothetical cross-infrastructure digital resilience platform for the Port of Rotterdam. The platform was described as a possible coordination platform that would connect existing organizational systems. Participating organizations would retain control over their own systems and data, while selected disruption-relevant information could be filtered, translated, or aggregated through a local component such as the Adaptive Data Adaptor. The platform could combine approved outputs to make cross-infrastructure dependencies and possible cascading effects more visible, support scenario analysis, and provide alerts or decision-support information. It would not make operational decisions autonomously, and the responsible actors would retain their existing mandates and decision rights. The purpose of the discussion was therefore not to validate a finished product, but to examine whether such a concept could add value, what its limitations and risks might be, and under which governance conditions it could be trusted, used, and institutionally embedded.

Appendix 4. Informed consent

Informed Consent - Interview Study

Governing Cross-Infrastructure Digital Resilience in European Ports: A Feasibility Study in the Port of Rotterdam

You are being invited to participate in a research study titled “Governing Cross-Infrastructure Digital Resilience in European Ports: A Feasibility Study in the Port of Rotterdam.” This study is being conducted by Lorenzo Bettin, MSc student in Engineering and Policy Analysis at TU Delft. You are being asked to take part in an interview about cross-infrastructure disruption management in and around the Port of Rotterdam, including governance arrangements, coordination practices, information sharing, and the feasibility of shared digital resilience tools or platforms.

The interview will be recorded and will also involve note taking by the researcher.

The information you provide will be analyzed together with input from other participants and will be presented in an anonymous or non-attributable manner in the master’s thesis and, where relevant, in academic publications, presentations, and/or educational material. To the best of our ability, your answers in this study will remain confidential.

We will minimize any risks by storing personal data and interview material in secure TU Delft institutional storage, accessible only to the research team. All personal data will be handled according to the General Data Protection Regulation (GDPR) and TU Delft research data procedures. All personal data collected in the project will be deleted at the latest 1 month after the completion of the study (07/2026). Within 2 weeks of the

interview, you will receive an anonymous summary of our conversation. This summary will be made publicly available with the associated manuscript. You will be welcome to suggest modification within 2 weeks.

Your participation in this study is entirely voluntary, and you can withdraw without any consequences. If you decide to withdraw, we will make every reasonable effort to remove your data. You are free to omit any questions.

Questions or concerns

If you have any questions regarding data handling or the information provided, please contact the research team:

Responsible researcher: Lorenzo Bettin, Faculty of Technology, Policy and Management, TU Delft,

Second contact / Supervisor: Tamara Metze, Organization and Governance, Faculty of Technology, Policy and Management, TU Delft

Statement	Yes	No
I have read and understood the study information, or it has been read to me.	☐	☐
I have been able to ask questions about the study and my questions have been answered to my satisfaction.	☐	☐
I consent voluntarily to be a participant in this study and understand that I can refuse to answer questions and I can withdraw from the study at any time, without having to give a reason.	☐	☐
I understand that taking part in the study involves an interview.	☐	☐
I understand that personal information collected about me that can identify me will not be shared beyond the study team.	☐	☐
I understand that after the research study the anonymous summary of our conversation will be made publicly available with the thesis.	☐	☐
I understand that the interview will be recorded and the data will be stored in a TU Delft OneDrive / institutional storage environment.	☐	☐
I agree that my responses, views or other input can be quoted anonymously in research outputs.	☐	☐

I have read and understood the study information above, and I consent to participate in the study and the data processing described above:

Date: _____

Signature: _____

Appendix 5. Interview question example

Rijkswaterstaat (RWS) – Interview question example

1. From your perspective in water safety and crisis management, what are the most relevant cross-infrastructure disruption risks in and around the Port of Rotterdam?
2. When a disruption affects multiple infrastructure domains at once, how is coordination currently handled between organizations such as Rijkswaterstaat, the safety region, municipalities, water authorities, port actors, and private operators?
3. In your experience, what are the main governance bottlenecks in cross-infrastructure crisis management: unclear responsibilities, fragmented information, different mandates, lack of trust, legal or confidentiality constraints, or something else?
4. How should responsibilities, escalation, and decision rights ideally be organized when a disruption crosses sectoral or territorial boundaries?
5. What kind of information from other infrastructure actors would genuinely improve crisis-management decision-making during a disruption?
6. If a shared cross-infrastructure digital resilience platform were introduced for the Port of Rotterdam region, what would it need to provide to be genuinely useful for crisis managers and infrastructure operators?
7. Based on your experience with working in networks, what governance conditions would need to be in place for such a platform to be trusted, used, and maintained over time?