Navigating cyber resilience in seaports: challenges of preparing for cyberattacks at the Port of Rotterdam

Eline Punt, Jochen Monstadt, Sybille Frank and Patrick Witte

(Information about the authors can be found at the end of this article.)

Received 29 December 2022
Revised 10 March 2023
Accepted 28 March 2023

The authors would like to thank all interviewees for their time and dedication. Many thanks to the colleagues of the Research Training Group KRITIS and the Institute for Sociology at the Technical University of Darmstadt and the Spatial Planning department at Utrecht University for their critical and constructive feedback on different versions of this article. The authors also thank Joy Burrough for the professional language editing of this paper.

Declaration of interest: This work was supported by the German Research Foundation (DFG) within the Research Training Group KRITIS at the Technical University of Darmstadt (Grant No. GRK 2222). The authors report there are no competing interests to declare.

Abstract

Purpose – *Cyber resilience has emerged as an approach for seaports to deal with cyberattacks; it emphasizes ports' ability to prepare for an attack and to keep operating and recover quickly. However, little research has been undertaken on the challenges of governing cyber risks in seaports. This study aims to address this gap.*

Design/methodology/approach – *Governing cyber resilience is shaped by distributed responsibilities, uncertainties and ambiguities. The authors use this conceptualization to explore the governance of cyber risks in seaports, taking the Port of Rotterdam as a case study and analyzing semistructured interviews with stakeholders, participatory observation and policy documents and legislation.*

Findings – *The authors found that many strategies for governing cyber risks remain dedicated to protecting computer systems against cyberattacks. Nevertheless, port stakeholders have also developed strategies in anticipation of disruptions. However, these strategies appear informal and uncoordinated due to a lack of information exchange, insufficient knowledge regarding cyber risks and disagreement about how to make the Port of Rotterdam cyber resilient. What mainly hampers the cyber resilience of the port is the lack of a comprehensive regulatory framework and economic incentives. The authors conclude that resilience is merely an ideal at the Port of Rotterdam, meaning related governance strategies remain incremental and await institutionalization.*

Originality/value – *This paper offers insights into the cyber resilience of critical socio-technical systems, which have been underexposed in cyber resilience debates, but, when exploited, can manifest in large-scale disruptions.*

Keywords *Cyber resilience, Seaports, Governance challenges, Critical infrastructures*

Paper type *Research paper*

1. Introduction

Ports are targets for cyberattacks because they are critical links in global supply chains and production processes (Ahokas *et al.*, 2017; Heilig and Voß, 2017). They are digitalizing at an ever-increasing pace by introducing initiatives for sharing logistical information, coordinating port processes and acquiring real-time information about assets to optimize the efficiency of port operations (Port of Rotterdam Authority, 2022). Ports' increasing dependence on and adoption of technological solutions is introducing vulnerability to a range of cyberattacks (Kapalidis, 2020; Molavi *et al.*, 2020). In recent years, cyberattacks have disrupted infrastructures at the ports of Antwerp (2011–2013, 2022), Rotterdam (2017), Los Angeles (2017), Barcelona (2018), Long Beach (2019) and Houston (2021) (de la Peña Zarzuelo, 2021). The most impactful cyberattack on the maritime sector to date was NotPetya in 2017, when the Danish logistics and transports company Maersk suffered significant business disruption and 76 port terminals were affected (Greenberg, 2018). With this attack, it became clear that cyberattacks could target not only systems that generate,

manage, store and exchange data but also the critical systems that ensure that terminals and bridges function, electric power and gas are distributed, and containers are transported (Kapalidis, 2020). Exploiting the vulnerabilities of these systems can manifest in the disruption of seaports and can have consequences reaching far beyond ports.

With cyberattacks becoming more diverse, frequent and targeted (Dunn-Cavelty and Wenger, 2020), the chances of disruptions occurring in ports have increased. As a result, concerns regarding the insecurity of ports against cyberattacks and the need to be better prepared against disruptions have materialized among scholars and policymakers (Ahokas *et al.*, 2017; Tam *et al.*, 2022). Across disciplines, resilience has emerged as a way of thinking about the permanent, open-ended responsiveness of socio-technical systems to adversity and uncertainty (de Bruijne *et al.*, 2010; Dunn-Cavelty *et al.*, 2015). Some scholars observe a shift away from prevention and the politics of urgency to strategies of building resilience (Medd and Marvin, 2005; Walker and Cooper, 2011). Cyber resilience can be understood as the "ability of systems to prepare, absorb, recover, and adapt to cyberattacks" (Linkov and Kott, 2019, p. 2). Despite the rise in the use of the term resilience in policy-making, few studies in cyber risk management have included challenges for governing, steering or influencing socio-technical systems toward enhanced resilience against cyberattacks (van Eeten, 2017), although some have examined governance mechanisms and the cybersecurity institutional landscape (Kuerbis and Badiei, 2017). Van Eeten (2017) noticed a disconnect between governance literature, which tends to focus primarily on discourses of governance, and cybersecurity research, which tends to focus on technological solutions to security issues. Furthermore, there is an emerging body of literature on information technology (IT) governance (Priyadarsini and Kumar, 2022), but the governance of critical operating systems that ensure seaports function is underexposed in those debates (Tam *et al.*, 2022).

We explore the governance of cyberattacks in seaports, taking the Port of Rotterdam (PoR) as a case study. We assume that building cyber resilience in seaports is a complex governance task because capacities to deal with cyberattacks lie with a broad range of stakeholders and institutions across policy levels and infrastructure domains (Carr and Lesniewska, 2020; Kuerbis and Badiei, 2017), and decisions about cyber resilience are made in a context of limited knowledge and socio-political ambiguity (Dunn-Cavelty and Wenger, 2022; Egloff, 2020). In risk governance debates, dimensions of distributed responsibilities and uncertainty and ambiguity are used to investigate the complexity of governing risks (Klinke and Renn, 2012; Renn *et al.*, 2020). By developing a conceptual framework based on these insights and modifying and applying it to investigate the challenges of governing cyber risks in seaports (Dunn-Cavelty and Wenger, 2022; Egloff, 2020), we investigate how to govern seaports toward enhanced cyber resilience.

Section 2 develops a conceptual framework for governing cyber risks. A description of our methodology is presented in Section 3. Section 4.1 introduces the relevant institutional arrangements for cyber resilience at the PoR. Based on our empiric data, this article then examines the challenges in governing the PoR toward cyber resilience (Sections 4.2–4.4). Section 5 concludes by developing ideas on how seaports could be governed toward cyber resilience.

2. Governing cyber risks in seaports: distributed responsibilities, uncertainty and ambiguity

Recently, ports have undergone a digital transformation (Molavi *et al.*, 2020), driven by emerging technologies, such as the Internet of Things, big data and autonomous vehicles (Sanchez-Gonzalez *et al.*, 2019). The adoption of these technologies has enabled a high degree of automation and streamlining in port procedures (Heilig and Voß, 2017), but they have also introduced new vulnerabilities to a range of cyberattacks. Potential cyberattacks include data or identity theft, espionage, malware and direct denial-of-service in which

access to service is blocked (Linkov and Kott, 2019; Sanchez-Gonzalez *et al.*, 2019). The disruption of highly interdependent logistics in seaports as a result of a cyberattack can reduce the amount of freight a port can process for a certain duration (Lam *et al.*, 2017; Verschuur *et al.*, 2020).

The growing vulnerability of seaports to cyberattacks is spurring on seaports to address cyber risks in a variety of ways (Tonn *et al.*, 2019). They may include preventive measures like firewalls, software encryption and system compartmentalization, design methods which improve system architecture or measures related to system management and operation (Paté-Cornell *et al.*, 2018). These approaches fall under the umbrella of cyber security, which refers to "measures taken to protect a computer or computer system against unauthorized access or attack" (von Solms and van Niekerk, 2013, p. 97). Discussions on cyber security tend to focus primarily on technological strategies (van Eeten, 2017). However, the extensive nature of cyberattacks emphasizes that these measures cannot eliminate cyber risks completely and that sufficient cyber risk management cannot be achieved solely through cyber security measures (Collier and Lakoff, 2008; Medd and Marvin, 2005; Walker and Cooper, 2011).

Many global, interconnected and complex risks, such as those posed by climate change and digitalization, are challenging conventional risk management approaches because their effects are characterized by complexity and uncertainty and, as a result, are almost impossible to calculate or solve (Carr and Lesniewska, 2020; Renn *et al.*, 2020). Building resilience is seen as a way to deal with this complexity and as a shift away from what is perceived as *ad hoc* arrangements for responding to emergency situations (Medd and Marvin, 2005; Walker and Cooper, 2011). Lakoff (2007) contrasts permanent preparedness, which is a prerequisite for resilience, with the idea of prevention that is common in conventional risk management. The principle of prevention prescribes avoidance and rejects any form of risk-taking, whereas preparedness seeks to develop a set of operational criteria for response based on future scenarios. In the quest to achieve a permanent state of preparedness, the techniques applied include monitoring, scenario development, simulations, stockpiling and crisis communications systems (Lakoff, 2007, p. 254).

The "governance of preparedness" (Medd and Marvin, 2005) can be seen as a complex governance task because it requires stakeholders to continuously address risks across policy levels and infrastructure domains. Due to processes of deregulation and privatization of critical infrastructure (CI) systems, responsibilities for addressing cyber risks have increasingly shifted to nongovernmental organizations (Cedergren *et al.*, 2018; de Bruijne and van Eeten, 2007; Kuerbis and Badiei, 2017). These developments have created a situation where coordination between governmental and nongovernmental organizations has become increasingly necessary to provide cyber security and resilience for CI systems (Carr, 2016; Dunn-Cavelty and Suter, 2009). At the same time, these scholars have identified persistent ambiguity with regard to the parameters for this type of partnership and questioned to what extent the state should be abdicating authority and responsibility to private organizations (Carr, 2016; Dunn-Cavelty and Suter, 2009). In addition, building cyber resilience for CI systems takes place in a context of limited knowledge (Dunn-Cavelty and Wenger, 2022; Egloff, 2020). So far, few studies have analyzed the collective activities needed for building cyber resilience in seaports and the governance challenges that come with preparing for cyberattacks (van Eeten, 2017). This study applies three dimensions commonly used in risk governance debates, namely, distributed responsibilities, uncertainty and ambiguity, to describe particular challenges of governing cyber risks and building resilience in seaports.

The first dimension is *distributed responsibilities*, which refers to the way institutional capacities are distributed across a range of stakeholders (Voß *et al.*, 2007). For cybersecurity, responsibility for protecting computer systems against cyberattacks primarily lies with internet and communications technology (ICT) managers, who should monitor system vulnerabilities

and potential cyber risks and intervene where necessary. However, preparing for potentially disruptive cyberattacks requires the collective effort of all port stakeholders, including governmental authorities and private and public stakeholders (Heilig and Voß, 2017; Kuerbis and Badiei, 2017). Decision-making in a context where responsibilities lie with a broad range of heterogeneous stakeholders is complicated by the fact that these stakeholders have different problem perceptions, values and interests. For seaports to be prepared for cyberattacks, the stakeholders' perceptions, values and interests need to be aligned and decision-making processes coordinated (Heilig and Voß, 2017).

Second, governing cyber risks is characterized by *uncertainty*, which refers to the "limitedness or even absence of knowledge that makes it difficult to assess the probability and possible outcomes" of cyberattacks (Klinke and Renn, 2012, p. 276). According to Sanderson (2012), the core problem is not the difficulty of assessing data on which to base decisions but the fact that such data does not yet exist and might never do so. This uncertainty can be a consequence of rapid technical development, where there are few chances to establish a priori the whole spectrum of possible interactions of technologies and foresee the nature and impact of cyberattacks (Bonfanti, 2022; Linkov and Kott, 2019). Despite the limitations of knowledge regarding new technologies, potential attack targets and consequences, decisions about governing cyber risks are still being made. For cybersecurity, uncertainty is addressed by avoiding cyberattacks from occurring, for example, by encrypting software or patching vulnerabilities. Cyber resilience requires "ongoing construction of the appearance of certainty and clarity in the midst of uncertainty" (Atkinson *et al.*, 2006, p. 696). Potential strategies to achieve that involve simulating cyberattacks in crisis exercises or developing scenarios.

A third characteristic is *ambiguity*, which pertains to the variability of (legitimate) interpretations of the same risk phenomena and their circumstances (Klinke and Renn, 2012). Two types of ambiguity can be distinguished: *interpretative ambiguity*, which denotes "the variability of (legitimate) interpretations based on identical observations or data assessments" (Renn *et al.*, 2020, p. 3) and *normative ambiguity*, where different concepts of what is tolerable can be distinguished (Klinke and Renn, 2012). Cyberattacks take place in a contested environment with a lack of public transparency and trusted knowledge regarding who launched a cyberattack, with what purpose, the quality and effects of an attack and the appropriate reactions to it (Dunn-Cavelty and Wenger, 2020). According to Egloff (2020), the contested information environment creates fractured narratives of a shared cyber event and increases *interpretive ambiguity*. Moreover, substantially different conceptualizations of which risks are deemed acceptable may exist between stakeholders, increasing *normative ambiguity*. As a result of fundamentally different value systems and worldviews, stakeholders might perceive the risk differently and set different priorities for technical developments and governance strategies (Goerlandt, 2020). Moreover, the difference between accepting the risk of an infrastructure disruption and preparing for one (cyber resilience) versus making a system impregnable (cyber security) can lead to alternative decisions about where to invest.

We can differentiate between distributed responsibilities, uncertainty and ambiguity as characteristics of governing cyber risks. These characteristics not only individually lead to governance challenges but also reinforce each other. For example, a lack of knowledge about cyberattacks can contribute to disputes about how cyber resilience should be implemented. These disputes are reinforced by more stakeholders becoming involved in cyber risk management. In the next sections, we will introduce our methodology that served to assess how these characteristics emerge in the port environment.

3. Methodology

This article draws on a case study design to understand the complexity of governing the PoR toward cyber resilience as a complex and context-specific issue (Harrison *et al.*, 2017). The PoR

has a sophisticated and interconnected CI system that is vulnerable to infrastructure disruptions and had suffered a large-scale cyberattack in 2017. We chose a qualitative approach since governance processes are difficult to capture effectively through quantitative study (Yadav and Banerjee, 2022). Qualitative research allows us to examine cyber risk governance challenges and processes in seaports in depth. To this end, three qualitative research methods were used: desk research of policy documents and law and legislation, participatory interviews and semistructured interviews. We triangulated the data to corroborate findings across data sets and reduce researcher and respondent bias (Bowen, 2009).

First, we reviewed and analyzed documents (n = 46), including various international, national, and regional law and legislation, cyber security assessments, guidelines and strategies (between 2011 and 2022) to gain an understanding of cyber resilience regulatory frameworks (Table A1). This analysis also informed the design of the semistructured interviews. Second, between June 2020 and April 2022, we observed and participated in (n = 15) events organized by FERM (a foundation focused on raising awareness about cyber resilience at the PoR) and the national cyber security center (NCSC) to gain understanding of relevant topics around cyber resilience in the PoR and to come into initial contact with key stakeholders for interviews (Table A2). We wrote fieldnotes based on these observations.

Finally, we conducted semistructured interviews (n = 18) between July 2020 and February 2022 to analyze the governance challenges and coping strategies of governing cyber resilience at the PoR. Our aim was to cover a broad spectrum of stakeholders to limit the bias of a narrow scope of respondents. This is especially relevant as preparing for disruptive cyber-attacks requires the collective effort of most port stakeholders (Heilig and Voß, 2017; Kuerbis and Badiei, 2017). We also created some overlap regarding function descriptions and backgrounds to be able to compare and contrast interview material. To that extent, our selection criteria were organizations that own, manage or use infrastructure connected to the PoR, are affiliated with cyber risk management in Rotterdam and are concerned with crisis management. Interviewees included stakeholders from organizations, such as the PoR Authority, the Rotterdam–Rijnmond Safety Region, the municipality of Rotterdam, the Dutch Ministries of Justice and of Safety and Economic Affairs and various cyber consultancies, port companies and CI providers (Table A3). To select interviewees, we first mapped the institutional arrangements relevant to attaining cyber resilience in the PoR. Participatory observations brought us into initial contact with some key stakeholders. From there, we used a snowballing method to come to our full list of interviews. The interviews were based on a thematic interview guide that was inspired by the conceptual framework developed in Section 2. Questions included how port stakeholders would respond to a cyber-attack scenario; how they cope with uncertainty, ambiguity and distributed responsibilities; and what they saw as the biggest challenges and opportunities for governing cyber resilience.

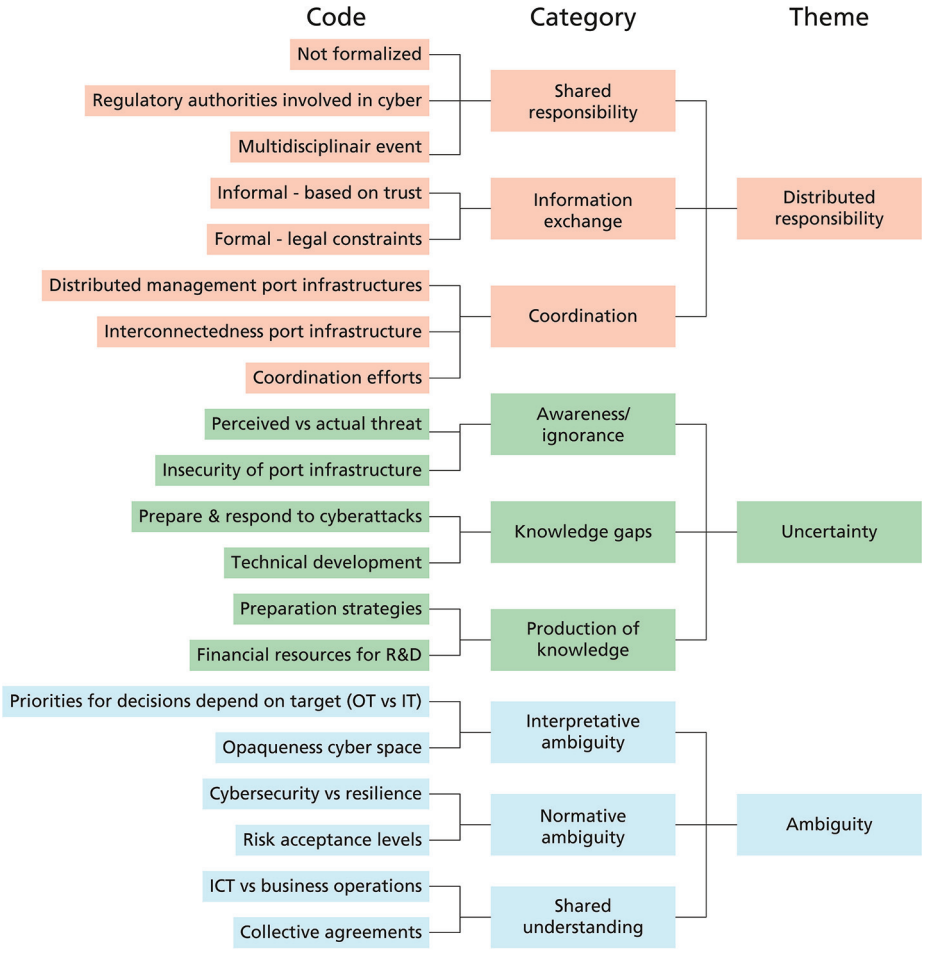
The interviews were conducted in Dutch and consequently transcribed and translated into English. We approached the interview transcripts, field notes and relevant documents inductively through qualitative content analysis (Mayring, 2000). We coded the material because it allowed us to capture the essence of the data and actively facilitated the development of categories and the analysis of their connections (Saldaña, 2013). We conducted the analysis in two steps. First, we used initial and open coding. Second, we themed and categorized these codes and connected them to the conceptual framing detailed in Section 2. The progress of the analysis was checked by the coauthors and a selection of participants. Figure 1 depicts the codes and themes that emerged from the analysis.

4. Governing cyber resilience at the Port of Rotterdam

4.1 Setting the scene: institutional arrangements for cyber resilience at the Port of Rotterdam

Understanding the governance of cyber risks at the PoR requires an overview of the laws, regulations and decision-making procedures that shape how port stakeholders interact and

Figure 1 Concept map of codes and themes



Source: The authors

make decisions about cyber security and resilience in a port context, which we obtained through desk research of policy documents and law and legislation. We limit this overview to currently relevant arrangements for attaining cyber resilience in a port context.

The International code for the security of ships and of port facilities (MSC.196(80)) (2009) defines mandatory requirements for the security of ships and port facilities. This code requires ports to design a security assessment and plan that addresses physical security, personnel protection, procedural policies and cyber security. Additionally, the International Maritime Organization (IMO) has elaborated a guideline (MSC-FAL.1-Circ.3) (IMO, 2017a) and resolution (MSC.428(98)) (IMO, 2017b) that encourages all stakeholders in the maritime industry to substantively address cyber risks. Furthermore, although not directed at the maritime sector, the European Directive (EU) 2016/1148 concerning Measures for a High Common Level of security of networks and information systems across the Union proposes that EU member states should develop and indicate a National Competent Authority for cyber security and oblige CIs to protect their ICT from incidents (EU, 2016). The Netherlands responded to the Directive by establishing the NCSC as the national authority; it acts as a central node in facilitating cyber security coordination across public and private organizations and providing information about cyber risks to governments and CIs. The

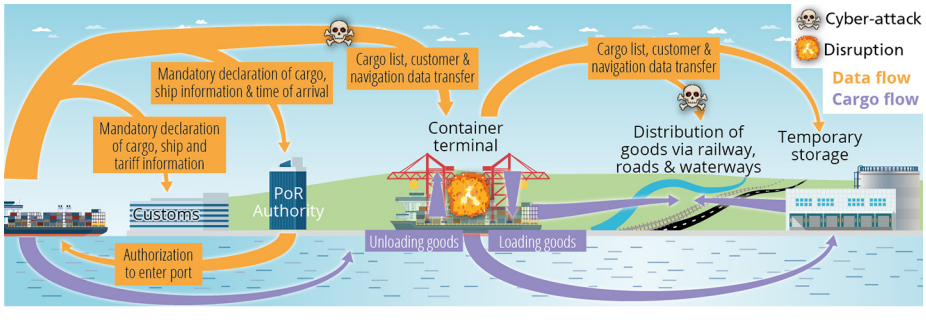
NCSC does not enforce any regulations; this is up to the sectoral inspections (Boeke, 2018). In addition, the Directive has been translated into the Security of Network and Information Systems Act (Government of the Netherlands, 2018a), under which the CI providers must implement measures to protect their ICT from incidents. The only maritime service named critical is the Harbor Master's Division of the PoR Authority, which is responsible for the smooth and safe handling of vessel traffic in the port.

These institutions are increasingly paying attention to cyber-related issues, but in general, they remain limited to protection measures (cyber security) and focus less on preparing for and recovering from cyberattacks (cyber resilience). Realizing that cyber resilience is critical to consider, the PoR Authority in recent years launched a Port Cyber Resilience Program that introduced a cyber resilience officer and a Port Cyber notification desk. The FERM foundation was set up to stimulate collaboration and raise awareness for cyber resilience. Cyber resilience at the PoR is incorporated voluntarily. Based on the current institutional landscape, we conclude that, as yet, cyber resilience awaits further institutionalization. In the following, we examine the challenges involved in enhancing cyber resilience.

4.2 Distributed responsibilities: shared responsibility, coordination and information sharing

Ports have highly interconnected and interdependent infrastructures (Figure 2). Figure 2, based on how respondents and policy documents (European Union Agency for Cybersecurity [ENISA], 2019) discussed the consequences of a cyberattack on port operations, shows how various port processes interconnect, including physical processes (e.g. transshipment procedures and the distribution and transfer of goods) and digital processes (e.g. declaration of cargo, ship and tariff information or the exchange of navigational data). The interconnectedness of port processes increases the shared risk of a cyberattack (Interviews 5, 7, 8, 12 and 14). Port services, such as vessel berthing, loading and unloading, temporary storage and distribution and transfer of goods, are provided by a diverse group of port stakeholders, including shipping companies, port industries, service providers, terminals and transport firms. Furthermore, many critical port processes are dependent on suppliers. These stakeholders and suppliers have their own IT and operating systems, each of which could be the target of a cyberattack. In particular, many respondents see the risk of cascading effects across the supply chain: if one part of the chain fails, then the entire port will have problems (Interviews 2, 5, 12 and 14). Furthermore, the rising number of suppliers makes it difficult to map interdependencies (Interview 2) and the risk of sensitive data leaks increases (Interview 5).

Figure 2 Vulnerability of port operations against cyberattacks



Source: The authors

In our research, we observed that port stakeholders feel a shared responsibility to collectively address cyber risks. For example, collective crisis exercises are being organized, and stakeholders help each other interpret risks (Interviews 3, 4, 9, 11, 12, 13 and 14). However, we also identified governance challenges associated with this notion of shared responsibility. According to our interviewees, port stakeholders are primarily responsible for protecting their systems against cyberattacks by taking cyber security measures such as patching vulnerabilities or introducing firewalls (Interviews 7, 9 and 11), but not all port stakeholders have enough resources to invest in cyber resilience (Interview 17). Furthermore, collective responsibility is not embedded in crisis management structures (Interviews 1, 2 and 6) and thus remains informal and based on networking (Interviews 3, 4 and 8).

Additionally, the distributed management suggests a need for coordination to manage the shared risk of a cyber-attack in the PoR. To that extent, initiatives like FERM and the Port Information Sharing and Analysis Centre have been introduced (Interviews 3, 4, 9, 11, 12, 13 and 14). Furthermore, regulatory authorities are increasingly interested and becoming involved in cyber resilience. For example, the Rijnmond Environmental Service, responsible for environmental safety, recently launched an investigation into the cyber resilience of organizations whose activities involve hazardous substances (Fox-IT Risk Management and Governance, 2021). The seaport police are increasingly involved in protection against cybercrime. The port authority wants to contribute to ideas about cyber resilience alongside the safety region Rotterdam–Rijnmond (Regional Risk Profile 2022–2025) (Safety Region Rotterdam-Rijnmond, 2021), the province of South Holland (Gijsbers, 2020) and the Municipality of Rotterdam (2022) (Cyberbeeld Rotterdam, 2022). However, these initiatives are not coordinated (Interview 9). As this interviewee noted: "Everyone is jumping on the bandwagon of the topic of cyber resilience. The question is if it is the role of regulatory authorities to step in or if they will become another entity that will draw up an assessment without having the expertise on the subject?" (Interview 9). The interviewee feels these assessments detract from what matters: "If I put myself in the position of one of our terminal managers, the regulatory authority is just another entity that comes by with an assessment. They are all slightly different, but they all consider themselves the most important. That distracts from what it is about: investing time and effort to become resilient against cyberattacks." (Interview 9). To improve the coordination between these initiatives, instances, such as the World Economic Forum, are developing preapproved, standardized cyber resilience assessments, but these have not yet become standard practice in assessing levels of cyber resilience of port stakeholders (Interview 9).

According to our interviewees, other governance challenges concern the lack of information exchange about cyber threats and vulnerabilities. For example, respondents indicated reluctance to exchange sensitive information. Even though many highlighted the importance of exchanging information about a vulnerability in their systems with suppliers, competitors and other parties, they were worried about this information falling into the hands of potential attackers or competitors (Interviews 9, 10, 15 and 18), as the following quote illustrates: "If I were to discuss with our clients that we were hit by a massive ransomware attack this week, there is a potential risk that they will unilaterally cancel the contract. Fortunately, that has not happened yet." (Interview 9). As a result, many stakeholders work with nondisclosure agreements or failed to share information about vulnerabilities (Interviews 10, 15 and 17).

Second, we can observe legal constraints for sharing information about cyber risks. The before-mentioned Network and Information Systems Security Act stipulates that the NCSC can only share cyber information with CI providers and governmental authorities because CI providers fall under the primary responsibility of the government, and an attack on one of these providers could have large-scale consequences (Interviews 13, 14 and 17). One interviewee expressed concern about the narrow definition of CI providers in

The Netherlands, which means information is only shared within a small group: "Less than 100 organizations have been deemed as CI providers and suppliers of these providers do not fall under that definition. That is a challenge because the CI provider receives information and support when something goes wrong. Still, the suppliers do not receive any information or support, even though the CI provider is dependent on those suppliers." (Interview 13). A representative from the NCSC explained that as a result, their role as a NCSC is criticized: "We often hear people say, 'you are not able to share information with everyone.' That is true because the law prevents that. As a result, the criticism is that information sharing is fragmented and slow." (Interview 17). Interviewees said that attempts to improve information exchange are primarily based on trust rather than on legislation because thresholds for notifications of cyberattacks and data leaks are generally high (Interviews 11 and 17).

Based on these findings, we found that responsibilities are distributed across a heterogeneous group of stakeholders, and there is a lack of information exchange about cyber risks and fragmentation of legislation, which makes governing cyber resilience at the PoR challenging. Furthermore, strategies remain informal and largely depend on trust or a sense of shared responsibility. There have been no financial or statutory incentives to collectively improve cyber resilience.

4.3 Uncertainty: perpetual knowledge gaps and a lack of awareness

The PoR is digitalizing, which has expanded the cyber risk landscape and introduced uncertainties, such as the difficulty of assessing across a large variety of stakeholders, assets and infrastructures when or where a cyberattack will occur and what the potential consequences are (Port of Rotterdam Authority, 2022; Municipality of Rotterdam, 2022). Our interviews indicated that uncertainties lead to various governance challenges for providing cyber resilience at the PoR. First, the ever more sophisticated cyberattacks and technical innovations have created perpetual knowledge gaps for port stakeholders (Interviews 2, 9, 11 and 14). For example, a Corporate Information Security Officer (CISO) from a logistics company at the PoR explained: "For other companies and us it feels like a rat race with always new risks that we have to deal with." (Interview 9). According to this interviewee, one way to fill these knowledge gaps is to keep up with daily risk reports (Interview 9). Other interviewees pointed to the importance of raising awareness of ports' insecurity against cyberattacks. For example, a digital relations manager from the Ministry of Economy, Trade and Industry said, "Many companies are unconsciously incompetent. They are not concerned with cyber issues. It is not something they read about or feel they should be concerned about. Many companies still think it will be okay and a cyberattack will not happen to them." (Interview 18). Furthermore, interviewees pointed to a lack of expertise in cyber security for critical operating systems (Interviews 14, 15, 16 and 18). According to one cyber expert, "there is a lack of understanding about the risk involved in coupling CI systems to the Internet and the solutions to this risk." (Interview 13). This lack of awareness was considered a major issue by many of our interviewees (Interviews 2, 13, 15 and 17). They plead for more financial resources for research and development of cyber security and resilience (Interviews 13 and 15).

Besides a lack of awareness, respondents discussed their limited knowledge of how to prepare for, adapt to and successfully recover from cyberattacks. This lack of knowledge stems from the general invisibility of cyberattacks. It is hard to pinpoint where a hacker entered a system, how long they were there, where they came from and what they have done (Interview 15). Not knowing these details means that "People cannot get beyond 'What should I do? So much stress, so much pressure, so scary.'" (Interview 15). This interviewee observed that people panicked if there was an incident. They felt there is time pressure to inform the relevant authorities immediately after an attack, inform customers who have directly experienced the consequences of the attack, and most importantly,

ensure the business processes are up and running again. These decisions would need to be made within hours by the people in charge. Part of the problem is that often organizations do not have incident response plans (Interviews 11 and 15).

Based on these findings, we argue that port stakeholders have limited information and lack awareness of cyber risks, which results in governance challenges when enhancing cyber resilience at the PoR. Keeping up with the rapid development of cyber risks is considered challenging. It is likely that the "defenders" against cyberattacks will always be one step behind the ever more innovative cyberattacks. Furthermore, we observed that cyber resilience strategies at the PoR remain focused on awareness, with as yet no developments that indicate preparation for infrastructure disruptions caused by cyberattacks.

4.4 Interpretative and normative ambiguity

Governing cyberattacks at the PoR can be seen as a political undertaking subject to inherent subjectivity. Stakeholders can interpret risks differently based on limited observations available (i.e. interpretative ambiguity) or they can have different priorities for technical developments and investment for cyber resilience strategies (i.e. normative ambiguity). Investing in cyber resilience is very costly, and we noted a distinct variation in who was willing to invest what based on different acceptance levels for cyber risks. We also observed a variation in how cyber risks are perceived.

Our findings show that there are interpretative ambiguities regarding cyberattacks on critical operating systems versus data management systems. Even if stakeholders have access to the same information about a cyberattack, they are likely to set different priorities for decision-making depending on the potential target (Interviews 13, 14, 15 and 16). As one interviewee explained, in the case of a failure of an electrically operated fence around a data center or factory, "someone from the IT world will say that the gate must be locked to protect the information and data located there, whereas someone from the industrial world will say that the gate must remain open to ensure people will be able to enter or leave when something goes wrong in the operational process." (Interview 16). That leads to different priorities in cyber security measures. The interviewee went on to explain: "a common security measure is that if you have entered a password three times you are not allowed to log in for a certain amount of time. Imagine you have an operating system for a storm surge barrier. A storm is coming. Maybe that storm surge barrier needs to be repaired, and you must log in. If you have a complicated password and make a typo, the system says you can't log in for 3 hours. That is a huge safety risk." (Interview 16). This shows us that fundamental cyber security measures required for a data system's security might restrict operational systems. Conventional cyber security strategies are targeted toward data systems rather than critical operating systems because the latter have traditionally been considered low risk (Interviews 13 and 15).

We also identified normative ambiguity, where stakeholders showed different acceptance levels of risks based on their background, expertise and economic interests. This normative ambiguity was demonstrated in two ways. First, distinct variation in acceptance of cyber risks could be identified between cyber experts and those responsible for business operations. For example, one interviewee noted that "from a business economics perspective it is very interesting to connect sensors in the port to central operating systems to increase efficiency. However, from a perspective of security, you increase the connections you make to the Internet, creating more vulnerability to cyberattacks" (Interview 13). Those responsible for business operations make decisions based on cost efficiency, i.e. the systematic approach to estimating the strengths and weaknesses of alternatives and the value at risk, i.e. the possible financial losses within a firm over a specific time frame. Risk assessments are considered essential. However, according to the interviewee, what is not well-developed is how to translate cyber risks into financial risks for the company: "It is very difficult for cyber guys to identify which cyber risks are also

business risks and why security measures need to be taken. For example, every month, hundreds of software vulnerabilities need to be patched. Where do you start? You should start with the systems that influence the business value most. However, there is a lack of communication between cyber guys and the business side to identify those processes." (Interview 13).

The second manifestation of normative ambiguity was between cyber security and cyber resilience. The difference between accepting the risk of an infrastructure disruption occurring versus making a system impregnable can lead to alternative decisions about where to invest and which measures should receive priority. According to some interviewees, you can improve the safety of systems with relatively cheap and simple measures, such as software patching, network separation and good access control (Interviews 12 and 18). At the same time, other interviewees noted that 100% security does not exist (Interview 5) and that "security is relative, difficult. It is wiser to focus on making sure you are resilient. However, then you must be aware that you are not digitally secure right now." (Interview 18) while many advanced cyber security measures that are marketed are judged to be unnecessary and expensive (Interview 15).

Based on these findings, we argue that interpretative and normative ambiguities of how cyber risks are interpreted can result in competing priorities for governing seaports toward cyber resilience. Often, multiple interpretations are valid, such as when a cyberattack hits data management systems and critical operating systems that require different coping strategies, which can result in conflicts of interest and make it challenging to achieve cyber resilience.

5. Conclusion

Using the example of the PoR, this article has explored the governance of cyber risks in seaports. We have identified governance strategies for dealing with cyberattacks in seaports and discussed which challenges stakeholders face in building cyber resilience. Our analysis revealed that to some extent port stakeholders have developed strategies that focus on preparing for disruptions. For example, collective crisis exercises that simulate a disruptive cyberattack are organized by FERM on a regular basis. Furthermore, there is much discussion about how to raise awareness of the insecurity of port infrastructure against cyberattacks and the need to be prepared. These findings can be placed in a broader trend of moving away from *ad hoc* arrangements for responding to emergency situations to a more permanent governance of preparedness that focuses on building resilience (Medd and Marvin, 2005). However, we identified that the strategies of preparedness remain informal, incremental and noninstitutionalized. In the event of an actual cyberattack, stakeholders often do not know what to do because they do not have incident response plans in place, or it is unclear which legal obligations they have.

Other governance challenges we identified include a lack of information exchange about cyber risks, insufficient knowledge regarding cyber risks and, as a result of ambiguous risk perceptions and economic interests, disagreement about how to govern seaports toward cyber resilience. These findings highlight how characteristics of distributed responsibilities, uncertainty and ambiguity reinforce each other and lead to various governance challenges. We can also conclude that aligning stakeholders' perceptions, values and interests has proven difficult, which complicates governing cyber resilience in a context where responsibilities lie with a broad range of stakeholders (Heilig and Voß, 2017). Yet, coordination between governmental and nongovernmental organizations has become increasingly necessary to provide cyber security and resilience for CI systems (Carr, 2016; Dunn-Cavelty and Suter, 2009). Furthermore, we found a mandatory legal framework for building cyber resilience is missing, which means building resilience largely depends on the creativity and agency of stakeholders. As a result, informal factors such as trust, personal networks and a sense of shared responsibility, emerge as key components of the current governance of cyber resilience. These findings are in line with Boholm *et al.* (2012),

who advocate a practice-near approach to resilience. However, we also argue that without a comprehensive legal framework for cyber resilience, the scope of action of these stakeholders remains limited. Furthermore, the price of resilience should be considered. We identified a lack of economic incentive among port stakeholders to invest in cyber resilience. Boin and van Eeten (2013) point out that resilience is often described in terms of redundancy and slack, but these components usually come at a cost, which creates challenges for implementing resilience strategies.

We conclude that, for the time being, resilience is no more than an ideal at the PoR that some stakeholders are trying to incrementally translate into action(s). Yet resilience and a culture of preparedness will likely become increasingly important in the face of global, interconnected risks. For example, a proposed EU directive (EU, 2020a) that should update the EU Directive (EU, 2016) could result in statutory requirements to improve the resilience of CIs against cyberattacks. Future research is needed into how procedural standards and future legislation can cope with the continuous innovation of cyberattacks and the digitalization of seaports and how they can contribute to building cyber resilience. Furthermore, since our research is based on a single case study, it would be relevant to compare the different challenges and processes for cyber resilience in various seaports. Gaining insight into how seaports can better prepare for infrastructure disruptions as a result of cyberattacks is important for introducing new technological solutions to guarantee the socioeconomic function of seaports.

References

Ahokas, J., Kiiski, T., Malmsten, J. and Ojala, L. (2017), "Cybersecurity in ports: a conceptual approach", *Proceedings of the Hamburg International Conference of Logistics (HICL). Hamburg International Conference of Logistics (HICL), Hamburg*, doi: 10.15480/882.1448.

Atkinson, R., Crawford, L. and Ward, S. (2006), "Fundamental uncertainties in projects and the scope of project management", *International Journal of Project Management*, Vol. 24 No. 8, pp. 687-698, doi: 10.1016/j.ijproman.2006.09.011.

Boeke, S. (2018), "National cyber crisis management: different European approaches", *Governance*, Vol. 31 No. 3, pp. 449-464, doi: 10.1111/gove.12309.

Boholm, Å., Corvellec, H. and Karlsson, M. (2012), "The practice of risk governance: lessons from the field", *Journal of Risk Research*, Vol. 15 No. 1, pp. 1-20, doi: 10.1080/13669877.2011.587886.

Boin, A. and van Eeten, M. (2013), "The resilient organization", *Public Management Review*, Vol. 15 No. 3, pp. 429-445, doi: 10.1080/14719037.2013.769856.

Bonfanti, M.E. (2022), "Artificial intelligence and the offense-defense balance in cyber security", in Dunn-Cavelty, M. and Wenger, A. (Eds), *Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation*, 1st ed., Routledge, pp. 64-79, doi: 10.4324/9781003110224.

Bowen, G.A. (2009), "Document analysis as a qualitative research method", *Qualitative Research Journal*, Vol. 9 No. 2, pp. 27-40, doi: 10.3316/QRJ0902027.

Carr, M. (2016), "Public–private partnerships in national cyber-security strategies", *International Affairs*, Vol. 92 No. 1, pp. 43-62, doi: 10.1111/1468-2346.12504.

Carr, M. and Lesniewska, F. (2020), "Internet of things, cybersecurity and governing wicked problems: learning from climate change governance", *International Relations*, Vol. 34 No. 3, pp. 391-412, doi: 10.1177/0047117820948247.

Cedergren, A., Johansson, J. and Hassel, H. (2018), "Challenges to critical infrastructure resilience in an institutionally fragmented setting", *Safety Science*, Vol. 110, pp. 51-58, doi: 10.1016/j.ssci.2017.12.025.

Collier, S.J. and Lakoff, A. (2008), "Distributed preparedness: the spatial logic of domestic security in the United States", *Environment and Planning D: Society and Space*, Vol. 26 No. 1, pp. 7-28, doi: 10.1068/d446t.

Cyber Security Council (2021), "Recommendation: integrated approach to cyber resilience", available at: https://open.overheid.nl/documenten/ronl-f8f86125-0635-47a7-b669-7b54011cd073/pdf

de Bruijne, M. and van Eeten, M. (2007), "Systems that should have failed: critical infrastructure protection in an institutionally fragmented environment", *Journal of Contingencies and Crisis Management*, Vol. 15 No. 1, pp. 18-29, doi: 10.1111/j.1468-5973.2007.00501.x.

de Bruijne, M., Boin, A. and van Eeten, M. (2010), "Resilience: exploring the concept and its meanings", in Comfort, L.K., Boin, A. and Demchak, C.C. (Eds), *Designing Resilience: Preparing for Extreme Events*, University of Pittsburgh Press, pp. 13-32.

de la Peña Zarzuelo, I. (2021), "Cybersecurity in ports and maritime industry: reasons for raising awareness on this issue", *Transport Policy*, Vol. 100, pp. 1-4, doi: 10.1016/j.tranpol.2020.10.001.

Digital Trust Center (DTC) (2020), "De five basisprincipes van veilig digitaal ondernemen", available at: www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen

Dunn-Cavelty, M. and Suter, M. (2009), "Public–private partnerships are no silver bullet: an expanded governance model for critical infrastructure protection", *International Journal of Critical Infrastructure Protection*, Vol. 2 No. 4, pp. 179-187, doi: 10.1016/j.ijcip.2009.08.006.

Dunn-Cavelty, M. and Wenger, A. (2020), "Cyber security meets security politics: complex technology, fragmented politics, and networked science", *Contemporary Security Policy*, Vol. 41 No. 1, pp. 5-32, doi: 10.1080/13523260.2019.1678855.

Dunn-Cavelty, M. and Wenger, A. (Eds) (2022), *Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation*, 1st ed., Routledge, doi: 10.4324/9781003110224.

Dunn-Cavelty, M., Kaufmann, M. and Søby Kristensen, K. (2015), "Resilience and (in)security: practices, subjects, temporalities", *Security Dialogue*, Vol. 46 No. 1, pp. 3-14, doi: 10.1177/0967010614559637.

Egloff, F.J. (2020), "Contested public attributions of cyber incidents and the role of academia", *Contemporary Security Policy*, Vol. 41 No. 1, pp. 55-81, doi: 10.1080/13523260.2019.1677324.

EU (2016), "Directive (EU) 2016/1148 concerning measures for a high common level of security of networks and information systems across the Union, 2016/1148 352", available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

EU (2020a), "Proposal for a directive (EU) on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM (2020) 823", available at: www.nis-2-directive.com/Proposal_for_a_directive_on_measures_for_a_high_common_level_of_cybersecurity_across_the_Union.pdf

EU (2020b), "The EU's cybersecurity strategy in the digital decade", available at: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

European Union Agency for Cybersecurity (ENISA) (2019), "Port cybersecurity–good practices for cybersecurity in the Maritime sector", available at: www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector

Fox-IT Risk Management and Governance (2021), "Cybervolwassenheidsbeeld", available at: www.dcmr.nl/sites/default/files/2021-10/Eindrapportage%20Cybervolwassenheidsonderzoek%20DCMR%20v1.1.pdf

Gijsbers, K. (2020), "Cybergereedheid economie provincie Zuid-Holland: een strategische luchtfoto en handelingsperspectief", available at: www.zuid-holland.nl/publish/pages/26859/provincie_zuid-holland_-_overzicht_cybergereedheid_final.pdf

Goerlandt, F. (2020), "Maritime autonomous surface ships from a risk governance perspective: interpretation and implications", *Safety Science*, Vol. 128, p. 104758, doi: 10.1016/j.ssci.2020.104758.

Government of the Netherlands (2000), "Defensienota 2000", available at: https://zoek.officielebekendmakingen.nl/kst-26900-2.html

Government of the Netherlands (2001), "Beleidsnota Kwetsbaarheid op het internet", available at: https://www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vi3ajv92kxri

Government of the Netherlands (2011), "National cyber security strategy", available at: https://zoek.officielebekendmakingen.nl/blg-101635.pdf

Government of the Netherlands (2018a), "Wet beveiliging netwerk- en informatiesystemen", available at: https://wetten.overheid.nl/BWBR0041515/2021-08-01

Government of the Netherlands (2018b), "Besluit meldplicht cybersecurity", available at: https://wetten.overheid.nl/BWBR0040368/2018-01-01

Government of the Netherlands (2021a), "Kamerstuk: Bijlage Voortgangsrapportage NCSA 2021", available at: https://open.overheid.nl/documenten/ronl-737b69e1-d8a0-4a4c-99a8-453b0ad5f10d/pdf

Government of the Netherlands (2021b), "Kamerbrief over diverse onderwerpen digitale weerbaarheid", available at: https://open.overheid.nl/documenten/ronl-cc6a27a6-0b2f-44d7-bbd6-9d51cc08c712/pdf

Government of the Netherlands (2022), "Wetsvoorstel tot wijziging van de wet beveiliging netwerk- en informatiesystemen", available at: www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?cfg=wetsvoorsteldetails&qry=wetsvoorstel%3A36084

Greenberg, A. (2018), "The untold story of NotPetya, the most devastating cyberattack in history", Wired.Com, p. 12, available at: www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Harrison, H., Birks, M., Franklin, R. and Mills, J. (2017), "Case study research: foundations and methodological orientations", *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research*, Vol. 18 No. 1, pp. 1-17, doi: 10.17169/fqs-18.1.2655.

Heilig, L. and Voß, S. (2017), "Information systems in seaports: a categorization and overview", *Information Technology and Management*, Vol. 18 No. 3, pp. 179-201, doi: 10.1007/s10799-016-0269-1.

International code for the security of ships and of port facilities (MSC.196(80)) (2009), MSC.196(80) ISPS, 87, available at: https://puc.overheid.nl/nsi/doc/PUC_2396_14/

International Maritime Organisation (IMO) (2017a), "Guidelines on maritime cyber risk management MSC-FAL.1-Circ.3", available at: wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf

International Maritime Organization (IMO) (2017b), "Resolution maritime cyber risk management in safety management systems MSC.428(98)", available at: wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf

Kapalidis, P. (2020), "Cybersecurity at sea", in Otto, L. (Ed.), *Global Challenges in Maritime Security: An Introduction*, 1st ed., Springer, Cham, doi: 10.1007/978-3-030-34630-0_8.

Klinke, A. and Renn, O. (2012), "Adaptive and integrative governance on risk and uncertainty", *Journal of Risk Research*, Vol. 15 No. 3, pp. 273-292, doi: 10.1080/13669877.2011.636838.

Kuerbis, B. and Badiei, F. (2017), "Mapping the cybersecurity institutional landscape", *Digital Policy, Regulation and Governance*, Vol. 19 No. 6, pp. 466-492, doi: 10.1108/DPRG-05-2017-0024.

Lakoff, A. (2007), "Preparing for the next emergency", *Public Culture*, Vol. 19 No. 2, pp. 247-271, doi: 10.1215/08992363-2006-035.

Lam, J.S.L., Liu, C. and Gou, X. (2017), "Cyclone risk mapping for critical coastal infrastructure: cases of East Asian seaports", *Ocean and Coastal Management*, Vol. 141, pp. 43-54, doi: 10.1016/j.ocecoaman.2017.02.015.

Linkov, I. and Kott, A. (2019), "Fundamental concepts of cyber resilience: Introduction and overview", in Kott, A. and Linkov, I.(Eds), *Cyber Resilience of Systems and Networks*, Springer International Publishing, pp. 1-25, doi: 10.1007/978-3-319-77492-3_1.

Mayring, P. (2000), "Qualitative content analysis", *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research*, Vol. 1 No. 2, p. 10, doi: 10.17169/fqs-1.2.1089.

Medd, W. and Marvin, S. (2005), "From the politics of urgency to the governance of preparedness: a research agenda on urban vulnerability", *Journal of Contingencies and Crisis Management*, Vol. 13 No. 2, pp. 44-49, doi: 10.1111/j.1468-5973.2005.00455.x.

Ministry of Transport, Public Works and Water Management (1999), "De digitale Delta", available at: www.kennisvandeoverheid.nl/documenten/beleidsnotas/1999/06/01/de-digitale-delta

Molavi, A., Lim, G.J. and Race, B. (2020), "A framework for building a smart port and smart port index", *International Journal of Sustainable Transportation*, Vol. 14 No. 9, pp. 686-700, doi: 10.1080/15568318.2019.1610919.

Municipality of Rotterdam (2022), "Cyberbeeld Rotterdam 2022", available at: www.ferm-rotterdam.nl/sites/default/files/2022-02/Cyberbeeld%20Rotterdam%202022.pdf

National Coordinator for Security and Counterterrorism (NCTV) (2013), "National cyber security strategy 2", available at: https://zoek.officielebekendmakingen.nl/blg-259104.pdf

National Coordinator for Security and Counterterrorism (NCTV) (2018), "Nederlandse cybersecurity agenda", available at: www.rijksoverheid.nl/documenten/rapporten/2018/04/21/nederlandse-cybersecurity-agenda-nederland-digitaal-veilig

National Coordinator for Security and Counterterrorism (NCTV) (2020a), "Nationaal crisisplan Digitaal", available at: www.rijksoverheid.nl/documenten/rapporten/2020/02/21/tk-bijlage-1-nationaal-crisisplan-digitaal

National Coordinator for Security and Counterterrorism (NCTV) (2020b), "Cybersecuritybeeld The Netherlands CSBN2020", available at: www.nctv.nl/documenten/publicaties/2020/06/29/cybersecuritybeeld-nederland-2020

National Coordinator for Security and Counterterrorism (NCTV) (2021), "Cybersecuritybeeld The Netherlands CSBN2021", available at: www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021

National Cyber Security Center (NCSC) (2020), "Handreiking OKTT: Aansluiting bij NCSC", available at: www.ncsc.nl/documenten/publicaties/2021/maart/29/handreiking-oktt

National Cyber Security Center (NCSC) (2021), "Leerpunten cyberoefening ISIDOOR", available at: www.ncsc.nl/documenten/rapporten/2021/september/14/evaluatierapportage-isidoor-2021

Paté-Cornell, M.-., Kuypers, M., Smith, M. and Keller, P. (2018), "Cyber risk management for critical infrastructure: a risk analysis model and three case studies", *Risk Analysis*, Vol. 38 No. 2, pp. 226-241, doi: 10.1111/risa.12844.

Port of Rotterdam Authority (2016), "Annual report Port of Rotterdam 2015", available at: www.portofrotterdam.com/sites/default/files/2021-06/havenbedrijf-rotterdam-jaarverslag-2015.pdf

Port of Rotterdam Authority (2017), "Annual report Port of Rotterdam 2016", available at: https://reporting.portofrotterdam.com/FbContent.ashx/pub_1011/downloads/v230308163521/Jaarverslag-2016-Havenbedrijf-Rotterdam.pdf

Port of Rotterdam Authority (2018a), "Annual report Port of Rotterdam 2017", available at: https://reporting.portofrotterdam.com/FbContent.ashx/pub_1011/downloads/v230308163521/Jaarverslag-2017-Havenbedrijf-Rotterdam.pdf

Port of Rotterdam Authority (2018b), "Beleidsdocument Haven cybermeldpunt", available at: https://www.portofrotterdam.com/sites/default/files/2021-05/beleidsdocument_haven_cybermeldpunt.pdf

Port of Rotterdam Authority (2019), "Annual report Port of Rotterdam 2018", available at: https://reporting.portofrotterdam.com/FbContent.ashx/pub_1011/downloads/v230308163522/Jaarverslag-2018-Havenbedrijf-Rotterdam.pdf

Port of Rotterdam Authority (2020), "Annual report Port of Rotterdam 2019", available at: https://reporting.portofrotterdam.com/FbContent.ashx/pub_1011/downloads/v230308163523/Jaarverslag-2019-Havenbedrijf-Rotterdam.pdf

Port of Rotterdam Authority (2021), "Annual report Port of Rotterdam 2020", available at: https://reporting.portofrotterdam.com/FbContent.ashx/pub_1011/downloads/v230308163525/Jaarverslag-Havenbedrijf-Rotterdam-2020.pdf

Port of Rotterdam Authority (2022), "Annual report port of Rotterdam 2021", available at: https://reporting.portofrotterdam.com/FbContent.ashx/pub_1006/downloads/v220308113811/Jaarverslag-2021-Port-of-Rotterdam.pdf

Priyadarsini, A. and Kumar, A. (2022), "A literature review on IT governance using systematicity and transparency framework", *Digital Policy, Regulation and Governance*, Vol. 24 No. 3, pp. 309-328, doi: 10.1108/DPRG-09-2021-0114.

Renn, O., Laubichler, M., Lucas, K., Kröger, W., Schanze, J., Scholz, R.W. and Schweizer, P.-J. (2020), "Systemic risks from different perspectives", *Risk Analysis*, Vol. 42 No. 9, doi: 10.1111/risa.13657.

Research and Documentation Centre (WODC) (2021), "Eindrapport informatie-uitwisseling Landelijk Dekkend Stelsel", available at: https://repository.wodc.nl/handle/20.500.12832/2484

Safety Region Rotterdam-Rijnmond (2017), "Regionaal risicoprofiel 2017-2020", available at: https://raad.albrandswaard.nl/Vergaderingen/Gemeenteraad/2016/19-september/20:00/Hamerstukken/g-1122029-rv-Regionaal-Risicoprofiel-2017-2020-Veiligheidsregio-Rotterdam-Rijnmond.pdf

Safety Region Rotterdam-Rijnmond (2021), "Regionaal risicoprofiel 2022-2025", available at: https://vrrr.nl/over/rc/crisisbeheersing/regionaal/

Saldaña, J. (2013), *The Coding Manual for Qualitative Researchers*, 2nd ed., SAGE.

Sanchez-Gonzalez, P.-L., Díaz-Gutiérrez, D., Leo, T. and Núñez-Rivas, L. (2019), "Toward digitalization of maritime transport?", *Sensors*, Vol. 19 No. 4, p. 926, doi: 10.3390/s19040926.

Sanderson, J. (2012), "Risk, uncertainty and governance in megaprojects: a critical discussion of alternative explanations", *International Journal of Project Management*, Vol. 30 No. 4, pp. 432-443, doi: 10.1016/j.ijproman.2011.11.002.

Tam, K., Hopcraft, R., Moara-Nkwe, K., Misas, J.P., Andrews, W., Harish, A.V., Giménez, P., Crichton, T. and Jones, K. (2022), "Case study of a cyber-physical attack affecting port and ship operational safety", *Journal of Transportation Technologies*, Vol. 12 No. 1, pp. 1-27, doi: 10.4236/jtts.2022.121001.

The Human Environment and Transport Inspectorate (ILT) (2019), "Meerjarenplan 2020-2024", available at: www.ilent.nl/documenten/rapporten/2019/09/17/meerjarenplan-2020-2024-inspectie-leefomgeving-en-transport

The Netherlands Scientific Council for Government Policy (WRR) (2021), "Voorbereiden op Digitale Ontwrichting", available at: www.wrr.nl/publicaties/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting

TNO (2020), "Handvaten cybersecurity in de logistieke keten", available at: www.digitaltrustcenter.nl/sites/default/files/2021-01/Handvatten_Cybersecurity_in_de_Logistieke_Keten.pdf

Tonn, G., Kesan, J.P., Zhang, L. and Czajkowski, J. (2019), "Cyber risk and insurance for transportation infrastructure", *Transport Policy*, Vol. 79, pp. 103-114, doi: 10.1016/j.tranpol.2019.04.019.

van Eeten, M. (2017), "Patching security governance: an empirical view of emergent governance mechanisms for cybersecurity", *Digital Policy, Regulation and Governance*, Vol. 19 No. 6, pp. 429-448, doi: 10.1108/DPRG-05-2017-0029.

Verschuur, J., Koks, E.E. and Hall, J.W. (2020), "Port disruptions due to natural disasters: insights into port and logistics resilience", *Transportation Research Part D: Transport and Environment*, Vol. 85, p. 102393, doi: 10.1016/j.trd.2020.102393.

von Solms, R. and van Niekerk, J. (2013), "From information security to cyber security", *Computers and Security*, Vol. 38, pp. 97-102, doi: 10.1016/j.cose.2013.04.004.

Voß, J.-P., Newig, J., Kastens, B., Monstadt, J. and Nölting, B. (2007), "Steering for sustainable development: a typology of problems and strategies with respect to ambivalence, uncertainty and distributed power", *Journal of Environmental Policy and Planning*, Vol. 9 Nos 3/4, pp. 193-212, doi: 10.1080/15239080701622881.

Walker, J. and Cooper, M. (2011), "Genealogies of resilience: from systems ecology to the political economy of crisis adaptation", *Security Dialogue*, Vol. 42 No. 2, pp. 143-160, doi: 10.1177/0967010611399616.

Wassens, R. (2022), "There is a real chance of a targeted cyber attack on the port of Rotterdam (Translated from Dutch: 'Kans op gerichte cyberaanval op Rotterdamse haven is reëel')", NRC, available at: www.nrc.nl/nieuws/2022/03/24/roep-de-haven-maar-uit-tot-crisisgebied-a4104937

World Economic Forum (WEF) (2021), "Advancing supply chain security in oil and gas: an industry analysis", available at: www3.weforum.org/docs/WEF_Advancing_Supply_Chain_Security_in_Oil_and_Gas_2021.pdf

Yadav, N.N.M. and Banerjee, P. (2022), "Exploring governance issues between online food delivery platforms and restaurant partners in India", *Digital Policy, Regulation and Governance*, Vol. 24 No. 3, pp. 292-308, doi: 10.1108/DPRG-06-2021-0074.

Author affiliations

Eline Punt is based at the Department of History and Social Sciences, TU Darmstadt, Darmstadt, Germany and Department of Human Geography and Spatial Planning, Utrecht University, Utrecht, The Netherlands.

Jochen Monstadt is based at the Department of Human Geography and Spatial Planning, Utrecht University, Utrecht, The Netherlands and Laboratoire Techniques, Territoires et Sociétés (LATTS), Université Gustave Eiffel, Marne la Vallée, France.

Sybille Frank is based at the Department of History and Social Sciences, TU Darmstadt, Darmstadt, Germany.

Patrick Witte is based at the Department of Human Geography and Spatial Planning, Utrecht University, Utrecht, The Netherlands.

Appendix. Data material

Table A1 Desk research of policy documents and law and legislation overview

No.	Document	Type	No.	Document	Type
1	Guidelines on Maritime Cyber Risk Management (IMO, 20170a)	Guideline	24	Nationaal Crisisplan Digitaal (NCTV, 2020a)	Policy document
2	Resolution MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems (IMO, 2017b)	Resolution	25	Cybersecuritybeeld The Nederland CSBN2020 (NCTV, 2020b)	Policy document
3	Wet beveiliging network- en informatiesystemen (Government of the Netherlands, 2018a)	Dutch law	26	Handreiking Objectief Kenbaar Tot Taak (OKTT): Aansluiting bij NCSC (NCSC, 2020)	Guideline
4	Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (EU, 2016)	EU Directive	27	Voorbereiden op Digitale Ontwrichting (WRR, 2021)	Research report
5	Overzicht vitale processen (NCTV, 2018)	Factsheet	28	Adviesrapport Integrale Aanpak Cyberweerbaarheid (CSR, 2021)	Advice
6	Regionaal risicoprofiel Rotterdam-Rijnmond, 2017-2020 (Safety Region Rotterdam-Rijnmond, 2017)	Policy document	29	Cybersecuritybeeld The Nederland CSBN2021 (NCTV, 2021)	Policy document
7	Regionaal risicoprofiel Rotterdam-Rijnmond 2022–2025 (Safety Region Rotterdam-Rijnmond, 2021)	Policy document	30	Cyberbeeld Rotterdam CB010 2022 (Municipality of Rotterdam, 2022)	Policy document
8	The Untold Story of NotPetya, the Most Devastating Cyberattack in History (Greenberg, 2018)	Newspaper article	31	Cybervolwassenheidsonderzoek (Fox-IT Risk Management and Governance, 2021)	Research report
9	Confidential document	Report	32	Cybergereedheid Economie Provincie Zuid-Holland: een strategische luchtfoto en handelingsperspectief (Gijsbers, 2020)	Policy document
10	Advancing Supply chain Security in Oil and Gas: an industry analysis (WEF, 2021)	White paper	33	Wijziging van de wet beveiliging netwerk- en informatiesystemen (Government of the Netherlands, 2022)	Wetswijzigingsvoorstel
11	Bijlage Voortgangsrapportage NCSA, 2021 (Government of the Netherlands, 2021a)	Kamerstuk	34	Besluit meldplicht cybersecurity (Government of the Netherlands, 2018b)	Decision
12	Meerjarenplan 2020–2024 Inspectie Leefomgeving en Transport (ILT, 2019)	Policy document	35	The EU's cybersecurity strategy in the digital decade (EU, 2020b)	Policy document
13	Proposal for a Directive (EU) on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (EU, 2020a)	EU Directive	36	Handvaten cybersecurity in de logistieke keten (TNO, 2020)	Research report
14	Kans op gerichte cyberaanval op Rotterdamse haven is reeel (Wassens, 2022)	Newspaper article	37	Leerpunten cyberoefening ISIDOOR 2021 (NCSC, 2021)	Policy document
15	Port Cybersecurity – Good practices for cybersecurity in the maritime sector (ENISA, 2019)	Report	38	Kamerstuk informatie trajecten digitale weerbaarheid (Government of the Netherlands, 2021b)	Kamerstuk
16	De five basisprincipes van veilig digitaal ondernemen (DTC, 2020)	Poster	39	Eindrapport informatie-uitwisseling Landelijk Dekkend Stelsel (WODC, 2021)	Research report
17	Defensienota 2000 (Government of the Netherlands, 2000)	Kamerstuk	40	Port of Rotterdam annual report 2015 (Port of Rotterdam Authority, 2016)	Annual report
18	De Digitale Delta (Ministry of Transport, Public Works and Water Management, 1999)	Policy document	41	Port of Rotterdam annual report 2016 (Port of Rotterdam Authority, 2017)	Annual report
19	Beleidsnota Kwetsbaarheid op het internet (Government of the Netherlands, 2001)	Kamerstuk	42	Port of Rotterdam annual report 2017 (Port of Rotterdam Authority, 2018a)	Annual report
20	National Cyber Security Strategy (Government of the Netherlands, 2011)	Policy document	43	Port of Rotterdam annual report 2018 (Port of Rotterdam Authority, 2019)	Annual report
21	National Cyber Security Strategy 2 (NCTV, 2013)	Policy document	44	Port of Rotterdam annual report 2019 (Port of Rotterdam Authority, 2020)	Annual report
22	Nederlandse cybersecurity Agenda (NCTV, 2018)	Policy document	45	Port of Rotterdam annual report 2020 (Port of Rotterdam Authority, 2021)	Annual report
23	Beleidsdocument Haven cybermeldpunt (Port of Rotterdam Authority, 2018b)	Policy document	46	Port of Rotterdam annual report 2021 (Port of Rotterdam Authority, 2022)	Annual report

Source: The authors

Table A2 Participatory observation

No.	Event	Date	No.	Event	Date
O1	FERM Port Cyber Café: digital Disruptions	02.06.2020	O9	NCSC Knowledge Event Cybersecurity for Industrial Systems (Part 2)	17.11.2021
O2	FERM Port Cyber Café: legacy Systems	17.09.2020	O10	FERM Port Cyber Café: cybersecurity and resilience about hazardous substances	18.11.2021
O3	FERM Port Cyber Café: FERM is growing up	19.11.2020	O11	NCSC Knowledge Event Cybersecurity for Industrial Systems (Part 3)	23.11.2021
O4	FERM Port Cyber Café: cybersecurity in the logistics chain	02.18.2021	O12	Webinar Digital resilience in the Rotterdam port area: a mutual responsibility	23.02.2022
O5	FERM Port Cyber Café: drones and safety/security	22.04.2021	O13	Webinar NCSC and DTC: digital impact situation Ukraine	09.03.2022
O6	FERM Port Cyber Café: OKTT and threat information	01.07.2021	O14	FERM Port Cyber Café: cyber insurance	10.03.2022
O7	FERM Port Cyber Café: cyber crisis exercise	16.09.2021	O15	FERM Port Cyber Café: cybersecure chain	14.04.2022
O8	National Cyber Security Center (NCSC) Knowledge Event Cybersecurity for Industrial Systems (part 1)	10.11.2021			

Source: The authors

Table A3 List of stakeholder interviews

No.	Position	Date	No.	Position	Date
1	Independent Administrative Body: researcher and program coordinator	28.07.2020	10	CI provider: strategy advisor	21.09.2021
2	Safety region: head of crisis management	22.09.2020	11	PoR Authority: CISO	21.09.2021
3	Municipality Rotterdam: strategic advisor	25.09.2020	12	FERM: director	11.10.2021
4	Municipality Rotterdam: program manager	25.09.2020	13	Cyber consultant	12.10.2021
5	Ministry of Justice and Security: policymaker	15.10.2020	14	Municipality Rotterdam: cyber security strategist	15.10.2021
6	Safety region: policy advisor	16.10.2020	15	Cyber consultant	16.02.2022
7	PoR Authority: senior advisor	09.09.2021	16	CI provider: senior advisor cybersecurity	18.02.2022
8	Port company: managing director	10.09.2021	17	Ministry of Justice and Security: digital relations manager	22.02.2022
9	Logistics company: corporate information security officer (CISO)	16.09.2021	18	Ministry of Economy: digital relations manager	28.02.2022

Source: The authors

About the authors

Eline Punt is a PhD candidate at the Research Training Group KRITIS and Institute for Sociology, Technical University of Darmstadt, and the Department of Human Geography and Spatial Planning, Utrecht University. Previously, she obtained a master's degree in urban and economic geography at Utrecht University. Her PhD project, "Seaports as nested infrastructure systems: governing risks at the Port of Rotterdam," aims to understand how systemic risks are governed at the Port of Rotterdam and how seaports can become resilient against infrastructure disruptions. Eline Punt is the corresponding author and can be contacted at: punt@kritis.tu-darmstadt.de

Jochen Monstadt is a Professor of Governance of Urban Transitions and chairs the Spatial Planning section at Utrecht University and visiting professor at the Université Gustave Eiffel, France. His research revolves around the transformation patterns of cities and how these are mediated by technical infrastructures. His specific interest is the socio-technical design and governance of those critical systems.

Sybille Frank holds the Chair of Urban Sociology and Sociology of Space at the Institute for Sociology at the Technical University of Darmstadt. Her research examines the city and urban spaces on the micro-, meso- and macro-levels with a thematic focus on conflicts in the areas of housing, tourism, heritage, technical infrastructures and the commemoration of violence.

Patrick Witte is an Associate Professor at the Department of Human Geography and Spatial Planning at Utrecht University with broad expertise and background in spatial planning. He is specialized in the interconnection of land use and transportation planning, with a particular focus on integrated corridor development and inland port development. His current research interests revolve around integrated spatial planning, transport infrastructure systems, transformations of cities and the smart city debate (smart governance and smart mobility).