Crime Law Soc Change (2017) 68:75–93
DOI 10.1007/s10611-017-9691-5

New governance of corporate cybersecurity: a case study of the petrochemical industry in the Port of Rotterdam

Judith van Erp[1]

Published online: 3 June 2017

Abstract The petro-chemical industry is a critical infrastructure that is vulnerable to cybercrime. In particular, industrial process control systems contain many vulnerabilities and are known targets for hackers. A cyberattack to a chemical facility can cause enormous risks to the economy, the environment, and public health and safety. This gives rise to the question how corporate cybersecurity has developed; how it is governed; and whether it should be subject to public oversight. This paper presents a case study of the governance of cybersecurity in the petrochemical industry in the Rotterdam Mainport area in the Netherlands, which reflects the 'new governance' view that cybersecurity can best be governed through voluntary public-private partnerships. The paper finds however that actual collaborative governance is not developing in the petrochemical industry in the port of Rotterdam; that corporate awareness and investment in cybersecurity stay behind standards, and that cybersecurity is not included in regulatory inspections. The paper places these findings in the context of three problems often associated with 'new governance' particularly pressing in cybersecurity governance: a weak role of government in public-private collaborative arrangements; an expectation that businesses will invest in self-regulation even in the absence of incentives to do so, and a lack of information exchange. In the port of Rotterdam, these problems result in a lack of obligations and accountability pressure on petrochemical corporations, leaving on of the most important chemical industrial hazards of today, largely unregulated.

✉ Judith van Erp
j.g.vanerp@uu.nl

[1] Faculty of Law, Economics and Governance, Utrecht University, Bijlhouwerstraat 6, 3511 ZC Utrecht, The Netherlands

Introduction

Chemical corporations as potential targets of cybercrime

The risk of becoming the target of a cyberattack is one of the most prominent security risks for corporate actors in the modern world. It is estimated that most companies face multiple cyberattacks every day; of which many of them remain unaware. One recent survey reports more than 40 million cyberattacks globally [1]. In the United States, in 2014 alone, prominent corporations such as Target, Home Depot, Yahoo, Google, and Apple are well-known targets of cyberattacks [2]. Many of these attacks involve identity theft – cybercriminals stealing digitally stored personal data, such as credit card data, of customers of these corporations, that they can sell online or capitalize in other ways. Another mode of cybercrime targets the internet itself, when corporate websites are attacked and rendered inaccessible for their clients. This happens, for example, when hackers execute DDOS attacks on banks, paralyzing the payment system or electronic banking. This paper deals with a third mode of cybercrime, which uses online access to firms as a weapon to disturb or take over their internal systems. The difference is that whereas DDOS attacks render companies websites or services inaccessible and thus block *access* to companies, this form of cybercrime enables cybercriminals to *enter* business processes and take control of them.

This third type of cybercrime generates a particular risk in so-called 'vital industries' or 'critical infrastructures': systems or actors providing products and services whose incapacity or destruction, would cause societal and economic disruption of (inter)national proportions, because they generate many victims and/or because there are no alternatives for these services and products, whereas they cannot be missed at the same time [3–5]. Examples of vital industries are health care, the financial sector, the chemical industry, defense systems, the prison system; the water management system; energy services; public transport and airlines. Clearly, cyberattacks to these vital industries form a major risk not only to the industry itself, but also to the public that depends on its services, and not only in terms of financial damage, but also in terms of health and safety. A particular risk exists in the chemical industry because of the hazard of toxic emissions. In a worst case scenario, an outsider entering the systems of a chemical plant could cause a serious chemical accident or an emission of a toxic substance, with health and environmental damage or even human casualties as a result [6].

This scenario is not entirely unlikely. A common denominator of many of these vital industries is that business processes are digitally managed through Industry Control Systems (ICS) or Process Control Systems (PCS); most commonly SCADA systems (Supervisory Control and Data Acquisition systems). These systems automatically monitor and control physical industry processes, often from a distance. For example, PCS systems monitor pipe pressure, temperatures, water levels, and other indictors, they receive signals of these indicators and react by adjusting processes by opening or closing valves or pipes; automatically generating warning signals and so on. They control the operation of technical processes in the physical world in almost all areas of life, from heart monitors in hospitals to ATMs to traffic lights, as well as the industrial processes in the chemical industry [7].

The security of PCS systems is generally assessed as low [3, 4, 8]. PCS systems currently in use, often date from the 1990s, a time in which the use of internet in the

corporate world was not widespread. Many of these systems are currently connected to the internet to allow connections with external data, for example from other PCS systems; and to allow for remote monitoring and control. Since they were designed for stand-alone use, rather than with the option of outside access in mind; they have no controls designed for the risks that come with connection to the outside world [7]. Research suggests that between 40 to 50% of the SCADA systems connected to the internet, have unresolved security issues or are vulnerable for hackers [9, 10]. The US National Vulnerability Database, an online database for software failures maintained by the National Institute of Standards and Technology, contained 90 SCADA vulnerabilities in June 2015.[1] Vulnerabilities of PCS systems are also regularly discussed on hacking fora; where special tools are available to search for and exploit vulnerabilities in SCADA systems. Various websites circulate 'recipes' for hacking SCADA systems, and search engines exist for targeted searches of vulnerable systems. One of them, SHODAN, is nicknamed 'Google for hackers'. These search engines enable potential wrongdoers to locate vulnerable systems without the need of very specific expertise.

Obviously, not all vulnerabilities result in a successful cyberattack. The US ICS-Cyber Emergency Readiness Team reports 245 incidents in critical infrastructure facilities in 2014 [11], with an increase in variation and sophistication of incidents. It is generally acknowledged that only a small fraction of incidents are reported since businesses are unwilling to do so. The best known example of a deliberate cyberattack against PCS systems is the Stuxnet virus in 2010 [12, 13]. Assumingly designed by the US and Israeli secret services against Iran's uranium production, this virus, after successfully incapacitating Iranian uranium centrifuges, unintendedly spread around the world affecting millions of computer systems until it eventually eliminated itself. A variety of other incidents with SCADA systems in vital infrastructures have been related to cyberterrorism, cyberespionage, and organized crime groups. Disgruntled (ex) employees; employees vulnerable to bribery or 'social engineering'; script kiddies and hacktivists have also been identified as SCADA systems attackers for an overview, see [7].

Together with the energy sector and water sector, the chemical sector is one of the vital industries in which cybercrime is considered a real and serious threat [14, 15]. Although cyber incidents in the chemical industry are frequently reported [6], no serious incidents with external victims are currently known. Nevertheless, cybersecurity in the chemical industry is considered to lag behind physical process safety. The US Roadmap to secure control systems in the chemical sector, which forms the basis for improvements of chemical cybersecurity in the US, identifies as main challenges that ICS systems are often not up to date with current standards; detailed analyses of potential threat and consequences are sometimes lacking, and that cyber risks are neither widely understood nor accepted in the chemical industry [14]; also see [4].

Aim of this study

In the light of the potentially serious consequences of a cyberattack against chemical corporations for public safety and the environment, the question arises how and to what extent this risk is managed. Criminological theories on situational crime prevention

[1] https://web.nvd.nist.gov/view/vuln/search-results?query=SCADA&search_type=all&cves=on, last accessed June 22 2015.

have stressed the importance of 'target hardening' as a key strategy in the prevention of cybercrime [16]. Situational crime prevention theories place the responsibility for prevention of cybercrime with corporations as potential victims, an approach that is also taken in corporate crime literature about the prevention of environmental harm and industrial accidents [17–21]. In line with these approaches, this paper investigates what efforts corporate actors currently take to protect themselves, and what role public authorities should play in governing corporate cybersecurity.

Sociologists note how emerging technological risks are often met with the ´risk regulation reflex´ resulting in unnecessary regulation and high monitoring costs [22, 23]. Cybersecurity however, presents a different case. Since ownership of critical infrastructures is often in private hands, public-private partnerships are considered the adequate approach for cybersecurity governance across the globe, and the responsibility for cybersecurity lies mainly with the industry, with a facilitating approach by government agencies [24]; Tropina DSS. The underlying regulatory logic reflects characteristics of 'new governance', an approach in which public values are realized in bottom-up, decentered, horizontal and experimental networks rather than command-and control relations, and in which information exchange, best practices and pragmatic problem solving techniques are preferred over regulation and enforcement [25, 26]. New governance is considered particularly appropriate in complex, fast-operating and interconnected markets operating under uncertainty, such as cybersecurity [27]. However, failures of new governance in other sectors, most notably the financial sector, have given rise to a critique of 'new governance', in which intransparency and information problems; business short term self-interest, and a retreating government, are identified as key hindrances to effective governance of complex global risks [25]. This raises the question whether a 'new governance' approach results in an acceptable level of cybersecurity [28].

This paper addresses this question through a case study of the governance of cybersecurity of chemical corporations in the port of Rotterdam, the Netherlands. It describes the collaborate governance structure of cybersecurity in chemical industries, the efforts of chemical firms in the port of Rotterdam to prevent industrial hazards related to cybercrime, and the role of public authorities in ensuring corporate cybersecurity. Criminological scholarship on industrial hazards, corporate environmental harm and corporate negligence has frequently demonstrated how corporations fail to invest in adequate measures to protect their personnel and environment from accidents [18, 20, 29, 30]. This paper adds to this scholarship by studying how firms prevent industrial hazards and environmental harms caused by cybercrime. Research has also demonstrated that deterrence-based inspections and enforcement are often insufficient to activate firms into compliance or beyond-compliance behavior [31]. New governance forms of regulation are often suggested as better alternatives for command-and-control regulation, because collaboration between public authorities, businesses and external stakeholders is assumed to make better use of corporate knowledge, expertise and responsibility than traditional 'command and control' regulation [27]. The case of cybersecurity provides an opportunity to study collaborative modes of governance for the control of corporate industrial harm, and thus connects the literatures on new governance with those on cybercrime and corporate crime.

However, this paper demonstrates that these expectations are not fulfilled. Based on a survey and interviews with corporate cybersecurity managers within chemical firms in the port of Rotterdam; regulators, and external experts, the paper finds that a lack of accountability pressure on firm results in a level of prevention against breaches of cybersecurity within chemical firms in the port of Rotterdam that is below standard, and identifies several characteristics of cybersecurity governance that create obstacles for public authorities to effectively get involved. It therefore establishes several problems with the assumption that voluntary collaboration will increase the level of security sufficiently, and thus adds to emerging critiques of new governance of high-tech corporate activity in a globalized world.

This paper is built up as follows. Section 2 introduces the case study and presents the research approach. Sections 3, 4 and 5 analyze the governance structure of cybersecurity in the chemical industry in the port of Rotterdam in terms of three key characteristics of new governance: public-private collaboration; business self-regulation; and information disclosure and exchange. Section 6 presents the conclusions.

Research design and methods

Case study selection

Although cybercrime is a global problem, and many standards, codes and guidelines are developing on an international level, the implementation of these in actual corporate cybersecurity and translation to daily business practice eventually takes shape on a local level [4]. A case study of a local industrial network is therefore appropriate to study corporate security measures and business-government interactions and their translation in daily practice, because it allows for an in-depth analysis of the roles and activities of different actors and their relations. Studying a network in particular allows to take into account the interconnectedness of businesses: chemical facilities in industrial areas with a concentration of other facilities, such as a port, often share connections and services, such as pipelines and other transport facilities, and use each other's waste or energy. PCS systems of different facilities and corporations are connected to communicate with each other. Cybersecurity in these interconnected chains is not an individual business matter; but the security in production and transport chains depends on their weakest link.

The port of Rotterdam is one of the worlds largest ports, and the economic Mainport for the Netherlands. It hosts the largest concentration of petrochemical industry in Western Europe; in which most multinational oil corporations hold at least one refinery or plant; and also one of the world's largest container terminals for wet and dry bulk. A large variety of dangerous and toxic substances are being transported and processed every day. At the same time, Rotterdam and its surrounding port communities, the Rijnmond area, is one of the most densely populated areas in Western Europe. An accident in one of the ports chemical facilities can cause enormous risks to the European economy, the environment, and the health of more than one million people.

The port of Rotterdam is among the largest and the most technologically sophisticated; in one of the most advanced economies in the Western world. It is therefore not representative for industrial areas with a concentration of hazardous industry, which are often located in less advantageous areas. Grabosky [32] argues that states with weak economies may be less able to afford the IT security infrastructure to adequately protect information systems, and lack regulatory and enforcement resources to control cybercrime. Reversing this argument, if good governance of cybersecurity in the chemical industry exists anywhere, we could expect to find it in the port of Rotterdam. We therefore use the case of the port of Rotterdam as a 'most likely' case study [33] to investigate the validity of the claim of new governance theory that public-private collaboration will result in effective management of complex risks. In other words, if the case study demonstrates ineffective governance in a case where new governance is most likely to work, the effectiveness of 'new governance' should be reconsidered. Moreover, a European case-study permits to study collaborative governance more or less in its ideal type, since the US has recently seen a strengthening of binding public norms and standards with the adoption of the Chemical Facility Anti-Terrorism Standards DHS [15]. Last, this case study also contributes to the growing literature in corporate criminology outside Anglo-Saxon territories [34].

Research methods

The case study makes use of a mixed method approach consisting of a survey; individual and group interviews; and a review of policy documents regarding cybersecurity in the chemical industry.

The survey investigated the technical level of cybersecurity within chemical corporations in the port of Rotterdam: it addressed the amount and nature of the PCS connections to other systems; PCS system updates and maintenance; the use of technological preventative instruments such as virus scanners and firewalls; the policies in use with regard to access and passwords; and staff awareness and training. The survey was based on two checklists for SCADA security developed by the Dutch National Cyber Security Centre (NCSC).[2] These checklists reflect emerging PCS security standards and best practices in PCS cybersecurity as they are being developed by public-private cybersecurity networks, in particular in the US but also in Europe [7]. Survey respondents were identified in all 56 hazardous petrochemical and bulk container firms in the port of Rotterdam. These 56 businesses were approached with a survey and invitation letter, co-signed by Deltalinqs, the Rotterdam Mainport industry association; DCMR, the Rotterdam port environmental regulator, and Erasmus University Rotterdam where the research was carried out, stressing the importance of the research and the confidentiality of data. 43 of these businesses provided the contact details of the most appropriate respondent in their organization, whom we then personally invited to participate in the research in the

[2] https://www.ncsc.nl/actueel/factsheets/checklist-beveiliging-van-ics-scada-systemen.html, accessed June 24 2015

summer of 2014. Eventually, 25 surveys were returned, filled in by IT managers, security analysts, process control supervisors and information security officers in 25 firms. All of the responding businesses used one or more PCS systems, sometimes more than ten different systems.[3] Since this paper focuses on cybersecurity governance, it only briefly summarizes the – primarily technical – survey findings.[4]

Group interviews were held in the form of two workshops with experts and representatives of corporations. A 'cybersecurity awareness workshop' for business IT managerswas organized by the Rotterdam Mainport industry association Deltalinqs, in collaboration with the author's university. Deltalinqs invited 10 chemical and bulk container corporations regarded as corporate leaders in the field of security in the port of Rotterdam. Despite their estimation that these selected firms would be open to discuss corporate cybersecurity in a collective workshop, only four corporations attended. It appeared that this was in fact the first time that representatives from chemical corporations in the port of Rotterdam discussed cybersecurity together. Two of them indicated that they primarily came to learn from others. Some of the absent corporations expressed their reluctance to participate in a seminar with competitors as well as officials from various government bodies, on such a sensitive issue. The seminar was further attended by experts from cybersecurity consulting firms; representatives of Deltalinqs; the Port Authority; and the cybersecurity unit of the police. A similar workshop was organized for representatives from various public safety authorities in the port of Rotterdam. This also appeared to be their first meeting on cybersecurity.

In addition to these group interviews, individual interviews were held with the chief safety strategist of DCMR; the safety officer of the Rotterdam Harbor business association Deltalinqs; and a representative of the city government of Rotterdam.

Public-private collaboration

The Dutch governance structure for the improvement of corporate cybersecurity reflects key characteristics of new governance, in the sense that it relies on public-private collaboration, self-regulation and information sharing. The national coordination of cybersecurity initiatives is in the hands of the National Infrastructure against Cybercrime (NICC) within the office of the National Coordinator for Terrorism Prevention and Safety, modeled after British and US equivalents such as the UK's Centre for the Protection of National Infrastructure.[5] The NICC performs facilitative roles such as to monitor; inform; develop preventative instruments; advise government and business; and coordinate action [35]. With regard to PCS security, the NICC publishes factsheets, information brochures and organizes information meetings to

[3] Corporations with more than one PCS system were asked to fill in the survey for their most important system.

[4] The survey was carried out by Laura Lormann-Zwartelé as part of her master's thesis research and supervised by the author.The full report (in Dutch) is available upon request.

[5] On the European level, a similar agency is the European Network and Information Security Agency ENISA, which undertook its first activities towards PCS systems in 2011 by undertaking an investigation into PCS security [4].

create awareness among businesses and to inform them about prevention strategies. Whether this advice is taken up, is the responsibility of the private owners of critical infrastructures.

In the port of Rotterdam, a variety of formal and more informal safety and security platforms and networks exist, such as BOOR, a safety coordinating group; the Platform for Port Integrity; the working group 'Safe Harbor'; 'Safety First', a network for high-risk corporations; and the Deltalinqs Safety and Security Contact Group. However, despite the fact that major problems with PCS security are common knowledge within the process industry, none of these platforms identifies PCS security as a specific problem. According to three respondents involved in several of these platforms, they tend to be very broad umbrella organizations with a large number of participants and no strings attached. As every business has its own special interest, and in order to keep them at the table, safety platforms tend to define security in a very broad manner enabling every involved business to take its pick, says a respondent. As became clear in the process of organizing the 'awareness workshop' for corporate IT experts, they were reluctant to engage in actual exchange on the subject of cybersecurity in chemical firms.

The informal, loose and broad governance network around cybersecurity in the port of Rotterdam reflects several problems with public private partnerships that have been identified in the Critical Infrastructure and cybersecurity literatures. Based on a comparison of several Critical Infrastructure Protection partnerships, May and Koski conclude that these partnerships tend to be vague about their goals and vision, and provide little guidance as to what action to take.[6] They tend to reflect the broad language of the national planning documents rather than offering a sector-specific course of action. Ambiguous container notions such as 'critical infrastructure protection' and 'cybersecurity', enable to avoid difficult choices and may result in less controversial and 'easier' forms of crime to be picked out first [28, 32]. This is illustrated in the port of Rotterdam by the prioritization of issues as container theft or drug smuggling, rather than confidential issues as firms internal cybersecurity, or collective hazards caused by interconnectivity between firms, such as the risk of a cyber incident. In Rotterdam as well as elsewhere, public private collaboration around cybersecurity tends 'to amount to conversations and consultations rather than genuine convergence. They assure that the wider community know each other well and are comfortable with each other but real public-private partnerships are underdeveloped [36] p.303. The result is that complex public-private governing networks have arisen in which 'no one knows how the increasingly complex ecology of cyberspace should be governed or who should own it' [36] p. 299, also see [24].

Industry associations and other intermediary 'third parties' are considered essential in collaborative networks for addressing public risks by private entities. Because of their expertise, legitimacy and information broker position, they are often appropriate organizations for leading networks; mobilizing participants and encouraging shared action [5]. The industry association for the port of Rotterdam Deltalinqs, has expressed

[6] The non-commital nature of public-private partnerships in the cybersecurity domain is also illustrated by a 2011 Enisa survey among various stakeholders in the ICS security domain, which shows that although most stakeholders view Public-Private Partnerships als useful, their actual participation is limited to only half of the stakeholders responding to the survey, with significantly less participation from industry than from government stakeholders.

its willingness to coordinate a bottom up process to stimulate corporate preventative action and has made a start by organizing the 'awareness workshop' for industry representatives. However, in the two years after this, Deltalinqs has not taken action to further increase the level of cybersecurity awareness and/or to start a process of voluntary collaboration. It thus demonstrates that 'the engagement of a professional industry association means little unless their involvement helps to foster a broader community of interest for addressing critical infrastructure risks' [5], p. 154.

Strengthening the role of government?

An abundance of research has found that a strong regulatory environment is a necessary condition for really effective self-regulation of industries, in the sense that it moves beyond merely symbolic participation in self-regulation to actual changes in organizational behavior, such as in this case investments in ICS security [37]. Effective self-regulation may take place under the condition of economic and reputational self-interest, a credible 'shadow of hierarchy', and intervention capacity of government [38]. In the US, these insights seem to take root in the sense that a move from voluntary, bottom up collaboration towards more hierarchical regulation in the shape of binding standards and reporting obligations is visible [28, 39].[7] For example, in the chemical sector, cybersecurity is increasingly incorporated in the environmental license or industrial hazard inspections [39, 41]. In Europe, however, the EU agency for Network and Information Security Enisa observes a lack of leadership and coordination [4]; a remark that also applies to Enisa itself according to Herrington and Aldrich [36]. Enisa also observes a great heterogeneity in guidelines, good practices and standards that have evolved out of the variety of initiatives and partnerships [4]. Whereas in the US, private responsibility and government regulation are not perceived as mutually exclusive, the mixing of voluntary and binding aspects is considered more problematic in the EU. It is feared that the idea of a 'partnership' may erode with the introduction of reporting obligations and imposing duties on private parties [28].

The most recent Dutch national Cybersecurity Strategy seems to recognize that the voluntary approach may have its limitations where it concerns protecting vital infrastructures. It advises regulatory enforcement authorities to formulate norms and standards, and to expand their supervising role to cybersecurity [42]. When it comes to practice however, in the port of Rotterdam, attempts to strengthen the role of public authorities with regard to ensuring corporate cybersecurity, are complicated by demarcation and authority problems between the various government agencies responsible

[7] For example, the voluntary Framework for Improving Critical Infrastructure Cybersecurity developed by the US National Institute for Standards and Technology is based on a presidential order. Despite its non-binding nature and the absence of enforcement, it is now advised as a standard for due diligence in potential litigation and may be used by courts to hold institutions accountable for failures in their cybersecurity ([40]; cf. [41]). An example specific for the chemical industry is the Chemical Sector Coordinating Council, which works in partnership with the Department of Homeland Security and has established a national control systems security programme to specifically address the cybersecurity issues within PCS systems in critical infrastructures ([4], p.22; [8]). Last, the Chemical Facility Anti-Terrorism Standards (CFATS) requires chemical facilities designated by DHS to comply with Risk-Based Performance Standards, including the standard that regulated facilities must deter cyber sabotage, including preveting remote access to critical PCS and ICS systems (DHS [14, 15]). DHS also monitors compliance with these standards through onsite inspection visits.

for oversight in the chemical sector [24, 28]. Three public supervising agencies monitor the risk of a chemical accident in the Rijnmond area: the Occupational Safety and Health Agency, a national inspectorate entrusted with occupational health and safety; the regional 'Safety Region Board', which includes the specialized regional Fire Brigade for ex post crisis management, and DCMR, the regional environmental protection agency mandated for licensing and inspecting major hazard facilities.[8] Together, these three agencies monitor compliance to the European Seveso regulation for industrial safety, implemented in the Netherlands in the Major Accidents Hazards Decree, and in the environmental license. Although each of these agencies carries out frequent inspections of chemical facilities in the Rijnmond area, none of them currently includes cybersecurity in their inspections; nor is it part of the licensing requirements. Although inspectorates have a detailed insight in the physical safety of hazardous chemical facilities in the port of Rotterdam, they completely lack insight in whether corporate cybersecurity levels are adequate to prevent industrial hazards.

As part of this research, a workshop was organized for representatives from public supervising authorities in the port of Rotterdam to discuss the need for a stronger involvement of public authorities in the governance of cybersecurity of chemical corporations in the port of Rotterdam. The participants in this workshop acknowledged the potential risk of a cyber incident, and realized that in the face of a collapse of critical infrastructure, the public will hold government to account for the failure, even when it is corporate-owned [36]. However, none of the agencies present were ready to take up a coordinating or supervising role. In an internal memo discussing whether the agency should take responsibility for monitoring cybersecurity, DCMR takes the position that the absence of an explicit assignment of the regulatory responsibility for corporate cybersecurity leaves no room for taking up this task. Although it realizes that the public will hold DCMR accountable for a serious cyber incident in a chemical facility, it resists the idea of taking responsibility for monitoring corporate cybersecurity, since it interprets its mandate as limited to physical safety. As DCMR's chief strategist attempts to put the issue of cybersecurity on the agenda within in his agency, he reports encountering reactions such as 'Should we become the secret service'? and 'Where to draw the line, where does it end?' within DCMR.

DCMR's position can be better understood when it is realized that no incentives exist for the agency to take up an additional responsibility on a subject for which it lacks expertise and capacity. DCMR staff have no expertise on cybersecurity, nor has DCMR any specific budget allocated to cybersecurity, whereas it operates within general resource constraints. The interviews and workshop also demonstrate that a 'new governance' network role does not come easily for a primarily rule-based inspectorate as DCMR is. In the actual governance of cybersecurity of chemical corporations in the port of Rotterdam, public authorities rely on self-regulation and voluntary information sharing between businesses, without actively directing or orchestrating that meaningful exchange actually takes place.

[8] Since environmental licensing and supervision is the primary task of the municipal and provincial governments in the Netherlands, and the local governments in the Rijnmond area consider themselves insufficiently capable to monitor and enforce the safety procedures in multinational chemical corporations individually, the local and provincial governments have collectively decentralized their supervising task to a specialized regional environmental protection agency.

Mills and Koliba [43] have argued that the increased reliance on voluntary and collaborative governance with regard to complex technical industrial processes, sometimes serves to mask regulatory weakness, lack of resources and professional capacity. Their analysis of the failure of regulatory oversight of deep-water drilling in the Deepwater Horizon case demonstrates that it was not a conviction that a public-private partnership would result in better compliance, but a lack of understanding of the complex technology in combination with diminishing resources for the regulatory agency, that led to a collaborative regulatory regime [43]. 'Faced with the reality that it could no longer sustain effective inspection techniques, the MSS decided to (…) shift the risk and responsibility for oversight from the agency to industry'. ([43] p.10). In the case of cybersecurity in the port of Rotterdam, a similar process can be observed, in the sense that the preference for voluntary public private collaboration might be interpreted not as a deliberate choice for the best regulatory arrangement, but as the best available option in terms of resources and agency risk aversion. The public private arrangements that actually have developed are more 'thin' than 'thick' versions of the ideal model of collaborative governance [44].

Self-regulation

The belief in collaborative cybersecurity governance and business self-regulation relies on the assumption that businesses are willing to invest in cybersecurity, and that market pressure will stimulate private firms to resolve public risks. Through a workshop with business representatives and a survey among cybersecurity experts in chemical corporations, we investigated whether businesses have taken actual responsibility to prevent cyberincidents. The survey investigated the actual level of protection of chemical businesses against the most common cybersecurity risks, to assess whether businesses actually regulate themselves. Although most responding businesses ($n = 25$) had taken a variety of protective measures against a breach of cybersecurity, there is also considerable variation between firms, with some firms' security procedures in conformity with current standards on most levels; to firms that are slow in updating their software; lacking virus scanners; are insufficiently aware of the risks of connectivity; or paying attention to cybersecurity infrequently. The following survey results stand out.

PCS systems are known to have many vulnerabilities, which can be repaired through software updates. A problem noted by experts is that necessary system maintenance and updates are carried out less frequent than desirable because of attempts to save costs [35, 42]. Eight of the 25 surveyed businesses indicated that cybersecurity received attention annually or in one case, never. For the others, this was a daily or weekly, or sometimes monthly concern. Only two facilities carried out updates of their systems as soon as an update is available. The majority of businesses did this when the production process was put to a halt because of physical maintenance. This means that physical maintenance is prioritized over digital maintenance and that vulnerabilities in the PCS systems are only repaired when a facility is temporarily shut down for other reasons. Two businesses indicated that they had never carried out an update of their system.

Another problem frequently mentioned by PCS experts is that virus-scanners are absent or outdated. Although half of the facilities had a virus scanner on their PCS system; nine did not and four of the respondents did not know. Among the facilities

without virus scanner were several businesses who indicated that their PCS systems were connected to the internet; office network; or other corporations. These connections are currently perceived as one of the main challenges to ICS security; because they enable unauthorized access to the business process [4, 7]. It is often noted by PCS experts that the main threat for PCS security is human; not technical; and that most security breaches are personnel security problems caused by a lack of attentiveness or by social engineering [36]. Weak passwords, such as 'welcome' or 'admin' are still frequently used across a variety of industries. Most of the surveyed companies within the Rijnmond chemical industries however employed various protocols preventing unauthorized access to their systems. 20 businesses therefore indicated that it was impossible that their PCS system could be entered through a successful attack on collaborating businesses. One however, admitted that this was possible, and four businesses responded that this had never occurred to them.

These survey findings provide the first indication of the level of cybersecurity of chemical corporations in the port of Rotterdam. Although a survey fails to take into account the specific system architecture of a facility and may overlook tailor-made solutions, the results show several firms being unaware of risks, particularly on the risks associated with connectivity between firms. The survey results also indicate that economic considerations sometimes result in postponing system maintenance. IT security officers of chemical plants in the Rijnmond area attending the awareness workshop, as well as safety experts from Deltalinqs, confirmed that the level of awareness for cybersecurity within corporations was low in comparison to the awareness of physical security. In their positions, they also found it difficult to create awareness, because economic pressure on industry is high; and ongoing operations are prioritized over security. This is consistent with a large scale Enisa investigation into cybersecurity awareness in the PCS area (2011) which identifies as one of the main challenges that top management shows a lack of involvement in cybersecurity and considers cybersecurity more of a cost than an investment and have the impression that they are already doing enough. Also, managers are not aware of the cascading effects that a cybersecurity breach in a connected business may have. The specific risks associated with connectivity may be hard to imagine and may also limit incentives to invest in vulnerability reduction as the security of one actor depends on the investments of others [45].

A condition underlying effective self-regulation is that firms face economic and reputational incentives to invest in security and that market transparency exists to allow stakeholders to discipline firms who underperform [25, 38]. Moreover, businesses tend to invest more in risk prevention measures when economic incentives are combined with pressure from the social environment of businesses [46]. Currently, however, cybersecurity is not subject to market incentives or accountability pressure for shareholders [4, 5, 24], as is confirmed by the business representatives attending the workshop. The cybersecurity experts interviewed for this research add that firms fail to realistically assess the potential financial damage of a successful cyberattack see also [8]. Temporarily shutdown of business processes; system replacement and hardware replacement can cause immense financial damage alone. This damage is often not calculated in the cost-benefit analysis of cybersecurity investments.

With regard to pressure from the social environment, firms internal cybersecurity is a difficult topic to monitor externally. In general, the high technological complexity of

the process industry, a lack of transparency, and a collective illusion of invulnerability after years of incident-free living contribute to a low risk perception within the Rijnmond community, as is a general problem of high risk communities [5, 47]. Political pressure; normative consensus about the level of protection that is demanded from firms, or active demands to protect the community against environmental hazard, are infrequent. The Rijnmond area is a relatively low-income community with a strong economic dependency on the industries in the port, resulting in a pro-industry political environment in which economic development and environmental protection are regarded as opposite. Illuminating in this respect is the fact that in the municipal council of Rotterdam, industrial safety is assigned to the council committee ´Economy and Port´ rather than the Safety committee, which deals with street crime.

Information sharing

Given the complexity of PCS systems and the uncertainty about the nature of cyber threats, information exchange between private corporations, external experts, and public agency representatives, is an essential feature of effective cybersecurity governance. Disclosure and sharing of information enable a form of dialogue known to benefit 'secondary learning': insights in how existing systems work; common problems and ways to solve them, in particular about 'on the ground' practices that may remain otherwise invisible on a higher management level unless reported [48, 49]. Disclosure also enables dialogue and collaboration on the design of solutions to problems [50]. Systematic analysis of incidents helps to create a better understanding of the nature of threats, as well as the specific circumstances and vulnerabilities that led to a security incident [4]. The sharing of information is particularly important to assess the nature and size of systemic risks caused by interconnectedness, such as the risk of a 'domino effect' associated with interconnected systems [45].

The function of information exchange in cybersecurity governance is performed in Information Sharing and Analysis Centers ISACs; [24]. ISACs - an international format for cybersecurity information exchange - are network organizations formed by corporate representatives; police; various government agencies including the national security agency coordinators and specialists. ISACs serve to confidentially share information and report incidents, to learn, and to coordinate collective action on a wide variety of cybersecurity issues, sometimes including PCS depending on the particular cyber-related risk in a sector. ISACs have been established for the nuclear sector, financial institutions, water, multinationals, energy, ports, the airport, among others. ISACs can be useful platforms to informally share information and to systematically investigate incidents, and thus facilitate mutual learning.

The demarcation issues and non-binding nature of collaborative platforms as discussed in section 3, also influence the exchange of information on PCS security in the chemical industry. The Rotterdam Port ISAC is mainly concerned with types of cybercrime that threaten short term business financial interest or safety, such as container theft or drugs smuggling through organized cybercrime. Second, the composition of the ISAC reflects the general problem of participation of agencies with an enforcement task in ISACs: corporations often perceive public-private collaboration on the basis of mutual trust irreconcilable with an enforcement perspective [51]. The

environmental regulator in the port of Rotterdam, DCMR, notes in an internal memo that it was not welcome to participate in the port ISAC, because corporations fear that DCMR will use its licensing and enforcement powers to coerce corporations into investments or to issue sanctions.

It is increasingly acknowledged that despite the creation of ISAC's in some industry sectors in the Netherlands, voluntary disclosure has not provided the level of learning and exchange that is considered adequate. This is also illustrated by the fact that another exchange platform, Deltalinqs university, has received 37 voluntary incident reports over the course of 15 years according to one of the respondents. A reporting duty for security breaches of electronic systems in vital industries to the NICC is currently proposed in the Dutch parliament. However, this proposal reflects the tension between coercion and trust that is inherent to collaborative governance, as corporations are expected to comply voluntary and enforcement of the reporting duty is not foreseen. In the stakeholder consulting round in the lawmaking process, business associations have expressed their opposition to the reporting duty's the obligatory character, which will in their view negatively influence the current practice of collaboration, information sharing and trust between business and government. Internet service providers on the other hand have pointed out that a safety culture will not develop without guarantees for compliance of the reporting duties [52]. The latter seems a more adequate assessment of current business attitude, since one of the respondents reports in an interview that businesses in the port ISAC did not support the reporting duty: 'They clearly expressed that they were not going to report everything to the authorities'. One of the experts interviewed for this research mentions an incident that later proved unknown with the regulatory agency, in which a petrochemical facility operating in the Rijnmond area shut down for 2 days because of a virus. He adds that if corporations report such incidents at all, they attribute it to technical failure rather than to a cyber incident. These remarks indicate that despite the importance of information disclosure and exchange, businesses face no incentive to actually disclose sensitive information, even with a reporting duty because of its difficulty to enforce [24, 49].

The role of ICT security consultants in information sharing

With regard to information sharing, ICT security consultants or private intelligence firms play a crucial yet ambiguous role in cybersecurity networks. Because of their sophisticated and elaborate knowledge on cybersecurity threats, they are often called in by government agencies for advice, since they are considered more knowledgeable than public authorities with regard to cyber risk. They thus play an important role in defining and framing cybersecurity problems [53]. In their role as experts, they are able to increase awareness and thus push for more efforts into risk reduction [5]. In this research, this was illustrated when several private intelligence firms were invited to give a presentation in the workshop that served to increase firms cybersecurity awareness. Much more than the regulatory agencies present in the workshop or even the NICC representative, these consultants were able to speak to the corporate representatives' imagination with examples of actual cyber incidents and to frame the risks from a business perspective, for example by sketching the financial recovery costs of a cyber incident for businesses.

But although these consultants contribute to business risk awareness, their contribution to information sharing is at the same time ambiguous. Since their actual activities and clients remain confidential, their involvement does not actually contribute to more transparency and learning [53]. For example, the mission statement of one of the most important ICT security consultants in the port of Rotterdam, FOX IT, includes a core value 'secrecy': '*Working with secrets, producing secrets and having trust from our clients to work with their secrets'*.[9] The security officer of DCMR comments: 'These consultants know far more than the government. They constantly communicate about new developments. We depend on their knowledge, but we deliver ourselves to the gods. They come up with problems that aren't urgent, and we cannot assess whether we're sold rubbish. They are very intransparent. They make a profit because governments have no knowledge. By remaining blurry, they are able to orchestrate. They can direct us to every corner of the room. Secrecy is their revenue. It is in their interest to keep us in the unknown'.

Conclusion

Experts agree that there is a considerable risk that a cyberattack against process control systems of chemical facilities may result in chemical incidents causing harm to people, the economy, and the environment. This paper asked how the risks of industrial hazards related to cybercrime are governed and controlled by corporations and public authorities. It is common practice that public risks of private corporate activity which involve globalized crime against national infrastructures are regulated in multilevel governance arrangements rather than command-and-control regulation. Likewise, policies with regard to corporate cybersecurity rest on the idea that voluntary collaborative arrangements, and informational instruments such as guidelines, checklists, information sharing and voluntary disclosure, are most suitable to provide adequate prevention of cybercrime. These new governance arrangements are assumed to provide the necessary flexibility to deal with complex risks and uncertainty; make best use of corporate expertise and collaborative learning; and enable pragmatic problem solving rather than imposing top-down solutions, in particular in a situation of interdependency. Through a case study of collaborative governance of corporate cybersecurity in the chemical industry in the port of Rotterdam, the Netherlands, this paper aimed to investigate how new governance operates in practice and whether it indeed contributes to an adequate level of corporate cybersecurity.

This study finds that despite the fact that a need for governance of cybersecurity in the chemical sector is considered necessary by many parties, in practice, actual collaborative governance with regard to corporate cybersecurity has not developed in the chemical industry in the port of Rotterdam. Information exchange, collaborative learning, or voluntary reporting of chemical cyber incidents is hardly nonexistent. A survey presented in this paper has demonstrated that the level of prevention against

[9] https://www.fox-it.com/nl/over-ons/manifest/, accessed June 30 2015. An illustration is the practice as revealed by ICT security consultants to always drive in white, unidentifyable vans, rather than arriving at the scene of a security incident in cars with recognizable logos which might raise suspicion from the media; shareholders; or inspectors.

breaches of cybersecurity within chemical firms in the Rijnmond area is below standard on some points. Regulatory agencies monitoring industrial safety struggle with the question whether the monitoring of corporate cybersecurity should be seen as part of their regulatory responsibility; and how this task can best be fulfilled. As collaborative governance is lacking, firms cybersecurity is purely left to individual firms willingness and capacity to invest, whereas expertise, awareness and knowledge may lack and interdependency may make individual firms security measures less adequate.

The findings of this study thus provide further support for scholarship on the risks and limitations of 'new governance' in practice, in particular, criticisms of 'hollowing out of the state' and soft, unenforceable obligations [26]. First, even though information exchange is key in new governance approaches, partnerships in practice are often hindered by intransparency and reluctance to share corporate information. In the port of Rotterdam, this results in broad and informal deliberation networks in which actual commitment and sensitive issues can be avoided. In the absence of a community of interest in which parties trust each other, it is unlikely that a reporting duty will change this.

Second, the belief in business self-regulation neglects the economic and organizational context within firms, where economic pressure puts constraints on businesses to invest in cybersecurity. On a cognitive level, managers, and even security personnel, are often unaware of the risk and implications of becoming victim to a cyber-incident, and of suitable preventative measures. As corporate crime literature on industrial hazards [18, 29, 30, 44] has already demonstrated, the assumption that firms will take sufficient measures to protect not only themselves and their personnel, but also their wider environment from harm in the absence of external pressure is often problematic. This paper adds to this scholarship an analysis of the emerging risk of cybersecurity, in particularly in highly connected industries. As these risks are more intangible and unpredictable; changing faster; more global; and more complex to understand than 'traditional' physical security, it will be even more difficult to hold firms to account.

Third, new governance in practice is often characterized by a retreating and weak role of the government, whereas in fact a strong involvement of public actors is an important condition for governance in the public interest. 'New governance' does not imply less government, but a different role for government. More active orchestration of networks; stimulating standard setting and certification; increasing knowledge and awareness at all levels of corporations, including top management, and organizing resilience and post-incident crisis control, can all be imagined as alternatives to traditional inspections. Often, these stretch beyond the regional or even national level. The point is that in imagining new and collaborative governance, it is too easily assumed that industry will prevent environmental harm or accidents without adequate incentives, and the role of government agencies in representing and protecting the public interest is not enough thought through [44]. These findings relate to a development in which deregulation and budget cutbacks make it less likely that public authorities can keep up with industries that are generally more powerful and have more knowledge, capacity and resources in the field of cybersecurity than governmental actors (cf. [27]). Without the means and professional capacity to effectively oversee complex industrial and technological processes, and a clear mandate to do so, public authorities will increasingly be unable to respond to technological innovations.

Regulatory authorities supervising industrial risk, should therefore develop an understanding of the meaning and consequences of globalized, internet-based and interconnected industrial processes, and the related risk that these processes become a target for cybercrime. Striking enough, in one of the most technologically advanced and densely populated regions in Europe, this process is just beginning.

Acknowledgments The author expresses thanks to Laura Lormann-Zwartele for assisting in data collection and to colleagues at Utrecht School of Governance for valuable comments to an earlier version of this paper.

References

1. Shackelford, S., & Bohm, Z. (2015). Securing north American critical infrastructure: A comparative case study in cybersecurity regulation. *Canada-US Law Journal*, forthcoming.http://papers.ssrn.com/sol3/Jeljour_results.cfm?form_name=journalBrowse&journal_id=231161&Network=no&lim=false.
2. Walters, R. (2015). Cyberattacks on US companies in 2014, the Heritage foundation issue brief no. 42890, October 2014. https://thf_media.s3.amazonaws.com/2014/pdf/IB4289.pdf. Accessed 12 Apr 2015.
3. Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection, 8*, 53–66.
4. Enisa (2011). Protecting industrial control systems. Recommendations for Europe and Member States. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states. Accessed 19 Nov 2015.
5. May, P., & Koski, C. (2013). Addressing public risks: Extreme events and critical infrastructures. *Review of Policy Research, 30*(2), 139–159.
6. Chemical Sector Coordinating Council (2012). Securing industrial control systems in the chemical sector. *Roadmap awareness initiative a case for action*. September 2012. Accessible through. https://www.dhs.gov/sites/default/files/publications/securing-ics-case-for-action-508.pdf. Accessed May 13 2017.
7. Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). Scada security in the light of cyber-Warfare. *Computers & Security, 31*(4), 418–436.
8. Knowles, W., Prince, D., Hutchison, D., Disso, J., & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection, 9*, 52–80.
9. Gritsai, G., Timorin, A., Goltsev, Y., Ilin, R., Gordeychik, S., & Karpin, A. (2012). *SCADA safety in numbers v1.1*. London: Positive Technologies.
10. NICC. (2012). *Cybersecuritybeeld Nederland*. Den Haag: Ministerie van Veiligheid en Justitie.
11. ICS-CERT (2015). ICS-CERT year in review – 2014. https://ics-cert.us-cert.gov/Year-Review-2014. Accessed 15 Nov 2015.https://ics-cert.us-cert.gov/sites/default/files/documents/Year_in_Review_FY2014_Final.pdf"
12. Langner, R. (2011). Stuxnet: Dissecting a Cyberwarfare Weapon. Security & Privacy. *IEEE, 9*(3, May–June 2011), 49–51.
13. Zetter, K. (2014). *Countdown to zero day, Stuxnet and the launch of the World's first digital*. Random House USA: Weapon.
14. Department of Homeland Security, Chemical Sector Roadmap Working Group (2009a). Roadmap to Secure Control Systems in the Chemical Sector. https://scadahacker.com/library/Documents/Roadmaps/Roadmap%20to%20Secure%20Control%20Systems%20in%20the%20Chemical%20Sector.pdf. Accessed 19 Nov 2015.
15. Department of Homeland Security (2009b). Risk-Based Performance Standards Guidance; Chemical Facility Anti-Terrorism Standards. http://www.dhs.gov/sites/default/files/publications/CFATS-Risk-Based-Performance-Standards-508.pdf. Accessed 19 Nov 2015.

16. Benson, M., & Simpson, S. (2015). *Understanding white-Collar crime, an opportunity perspective*. New York: Routledge.
17. Bisschop, L. (2015). Facilitators of environmental crime: Corporations and governments in the port of Antwerp. In J. van Erp, W. Huisman, & G. Vande Walle (Eds.), *The Routledge Handbook of white-Collar and corporate crime in Europe* (pp. 246–259). Abingdon: Routledge.
18. Pearce, F., & Tombs, S. (1998). *Toxic capitalism: Corporate crime and the chemical industry*. Aldershot: Dartmouth.
19. Passas, N. (2005). Lawful but awful. 'legal corporate crimes'. *Journal of Socio-Economics, 34*(6), 771–786.
20. Ruggiero, V., & South, N. (2013). Toxic state -orporate crimes, neo-liberalism and green criminology: The hazards and legacies of the oil, chemical, and mineral industries. *International Journal for Crime, Justice and Social Democracy, 2*(2), 12–16.
21. van Wingerde, K. (2015). The limits of environmental regulation in a globalized economy: Lessons from the Probo koala case. In J. van Erp, W. Huisman, & G. Vande Walle (Eds.), *The Routledge Handbook of white-Collar and corporate crime in Europe* (pp. 260–274). Abingdon: Routledge.
22. Furedi, F. (2002). Culture of Fear. Continuum.
23. Wildavsky, A. (1995). *But is it true? A citizen's guide to environmental health and safety issues*. Cambridge: Harvard University Press.
24. Rosenzweig, P. (2010). The Organization of the United States Government and Private Sector on achieving cyber deterrence. In *In: Proceedings of a workshop for deterring cyberattacks: Informing strategies and developing options for US policy*. National Academies: Press.
25. Ford, C. (2010). New governance in the teeth of human frailty: Lessons from financial regulation. *Wisconsin Law Review, 07*(2010), 101–146.
26. Levi-Faur, D. (2012). From 'big government' to 'big governance'. In D. Levi-Faur (Ed.), *The Oxford Handbook on governance*. Oxford: Oxford University Press.
27. Abbott, K. (2013). Introduction: The challenges of oversight for emerging technologies. In G. Marchant, K, Abbott and B. Allenby (eds.), *Innovative Governance Models for Emerging Technologies*. Edward Elgar, Cheltenham, pp 1-16.
28. Tropina, T. (2015). *Public-private collabortion. Cybercrime, cybersecurity and national security*. In T. Tropina & C. Callanan (eds.), Self and Co-regulation in Cybercrime, Cybersecurity and National Security (p. 1–41). Springer: Dordrecht.
29. Katz, R. (2010). The corporate crimes of Dow chemical and the failure to regulate environmental pollution. *Critical Criminology, 18*(4), 295–306.
30. Kluin, M. (2014). *Optic compliance, enforcement and compliance in the Dutch chemical industry (dissertation, TU Delft, The Netherlands)*. The Hague: Eleven International Publishing.
31. Kagan, R., Gunningham, N., & Thornton, D. (2011). Fear, duty, and regulatory compliance: Lessons from three research projects. In C. Parker & V. Lehman Nielsen (Eds.), *Explaining Compliance* (pp. 37–57). Business responses to regulation: Edward Elgar.
32. Grabosky, P. (2013). *Organized Cybercrime and National Security* (pp. 19–30). Korean Institute of Criminology, Korea: World Crime Forum.
33. Levy, J. (2008). Case studies, types, designs, and logics of inference. *Conflict management and peace science, 25*(1), 1–18.
34. van Erp, J., Huisman, W., & VandeWalle, G. (2015). *Routledge Handbook on White-Collar and Corporate Crime in Europe*. Abingdon: Routledge.
35. Luijff, E., Ali, M., & Zielstra, A. (2008). Assessing and improving SCADA security in the Dutch drinking water sector. In R. Setola & T. Geretshuber (Eds.), *Critical Information Infrastructure Security, Third International Workshop Revised Papers, CRITIS 2008*. Berlin: Springer.
36. Herrington, L., & Aldrich, R. (2013). The future of cyber-resilience in an age of global complexity. *Politics, 33*(4), 299–310.
37. Short, J., & Toffel, M. (2010). Making self-regulation more than merely symbolic: The critical role of the legal environment. *Administrative Science Quarterly, 55*(3), 361–396.
38. Saurwein, F. (2011). Regulatory choice for alternative modes of regulation: How context matters. *Law & Policy, 33*(3), 334–365.
39. Department of Homeland Security (2015). Chemical Facilities Anti-Terrorism Standards Factsheet. http://www.dhs.gov/sites/default/files/publications/cfats-fact-sheet-11-15-508.pdf. Accessed 19 Nov 2015.
40. Shackelford, S. and Z. Bohm (2016). Securing North American critical infrastructure: A comparative case study in cybersecurity regulation. *Canada-United States Law Journal, 40*(1).
41. Lunn, B. (2014). Strengthened director duties of care for cybersecurity oversight: Evolving expectations of existing legal doctrine. *Journal of Law and Cyber Warfare, 4*, 109.

42. NICC. (2013). *Cybersecuritybeeld Nederland*. Den Haag: Ministerie van Veiligheid en Justitie.
43. Mills, R., & Koliba, C. (2014). The challenge of accountability in complex regulatory networks: The case of the Deepwater horizon oil spill. *Regulation & Governance, 9*(1), 77–91.
44. Almond, P. (2015). Revolution blues: The reconstruction of health and safety law as 'common-sense' regulation. *Journal of Law and Society, 42*(2), 202–229.
45. van Eeten, M., Nieuwenhuis, A., Luijff, E., Klaver, M., & Cruz, E. (2011). The state and the threat of cascading failure across critical infrastructures: The implications of empirical evidence from media incident reports. *Public Administration, 89*(2), 381–400.
46. Haines, F. (2011). Facing the compliance challenge: Hercules, Houdini or the charge of the light brigade? In C. Parker & V. Lehman Nielsen (Eds.), *Explaining compliance* (pp. 287–303). Business responses to regulation: Edward Elgar.
47. 't Hart, P. (2013). After Fukushima: Reflections on risk and institutional learning in an era of mega-crises. In: Public Administration, p. 1–13.
48. Lajili, K., & Zeghal, D. (2005). A content analysis of risk management disclosures in Canadian annual reports. *Canadian Journal of Administrative Sciences, 22*(2), 125–142.
49. Smyth, S. (2014). The Greening of Canadian Cyber Laws: What Environmental Law can Teach and Cyber Law can learn. *International Journal of Cyber Criminology, 8*(2), 111–155.
50. Mills, R., & Reiss, D. (2013). Secondary learning and the unintended benefits of collaborative mechanisms: The federal aviation administration's voluntary disclosure programs. *Regulation & Governance, 8*(4), 437–454.
51. Enisa (2013). *Can we learn from Scada Security Incidents* (white paper). www.enisa.europa.eu. Accessed 15 May 2015.
52. Dutch Ministry of Safety and Justice (2015) Explanatory Note to Proposal of Law regulating the data processing and reporting duty for Cybersecurity (Toelichting bij wet gegevensverwerking en meldplicht cybersecurity), the Hague. https://www.internetconsultatie.nl/cybersecurity. Accessed 19 Nov 2015.
53. O'Reilly, C. (2015). The pluralization of high policing: Convergence and divergence at the public-private interface. *British Journal of Criminology, 55*(4), 688–710.
54. Fox-IT (2011). Fox-IT Manifest. https://www.fox-it.com/nl/over-ons/manifest/. Accessed 30 June 2015.
55. Nationaal Cyber Security Centrum. (2012). *Beveiligingsrisico's van on-line SCADA-systemen. Factsheet FS-2012-01*. Den Haag: Ministerie van Veiligheid en Justitie.
56. NIST (2013). National Vulnerability Database. http://web.nvd.nist.gov/view/vuln/search. Accessed 10 Oct 2013.