Chapter 4
Preparing for Digital Disruption

4.1 Introduction

Prevention is better than cure, goes the adage. There is much to be said for prevention, especially when there is a chance to avoid the consequences of disruption altogether. But even if we take every preventive measure under the sun, we can never entirely exclude the possibility of serious disruption to the normal functioning of society. We therefore need to be prepared and to have early-warning mechanisms that can alert us when things are going awry. If disruption does occur, adequate follow-up action is vital. Recovery and reconstruction are key if society is to resume its normal functioning as rapidly as possible.

For physical risks such as major flooding or a severe flu epidemic, the government and other actors have identified measures to increase preparedness, detect early signs of disruption, minimize the impact and facilitate recovery. Probably more than any other event, the Covid-19 outbreak has underlined the importance of swift and coordinated responses. The Dutch government, however, has only recently recognized the risk of societal disruption due to the failure or disruption of digital infrastructure. Partly for this reason, we are unprepared. Extant policies focus on cyber security and prevention rather than on handling disruptive events as they unfold. This section discusses how our plans for digital disruption could be designed to include better preparation for its effects on society. We distinguish between four stages: preparedness, detection, mitigation, and finally, recovery and reconstruction.

E. Schrijvers et al., *Preparing for Digital Disruption*, Research for Policy,
https://doi.org/10.1007/978-3-030-77838-5_4

4.2 Preparedness

Detection, mitigation and, in particular, recovery and reconstruction largely depend on how well we are prepared to handle societal disruption. Unlike prevention, they involve measures that seek to limit the effects of the disruption and to facilitate recovery. They are comparable to the role played by firebreaks in a forest or artificial hills in flood defences, which do not prevent flooding but provide protection from the rising waters and limit the number of victims. Precautionary measures can likewise limit the societal disruption caused by 'digital fires'. The first stage is preparedness. Within this category, we distinguish between four areas: fall-back options, isolation, cyber security exercises, and the provision of information.

4.2.1 Fall-Back Options

Options for switching to different facilities come in many shapes. The most well-known is the back-up facility, a diesel generator to generate power in an emergency. A crucial issue is how long this type of facility would have to function. With back-up facilities for digital systems, one consideration is how long data needs to be retained, which would depend on the type of data involved. Following the *NotPetya* attack, Maersk was able to save much of its data by contacting data centres around the world. But what was missing was a back-up of how the company's own IT system – the digital core of the company – was set up.[1] The Maersk case shows the importance of companies to plan ahead. Some processes have become so large and complex that back-up facilities are practically impossible to implement, partly due to cost. In short, back-up facilities are important but are no longer the obvious solution for certain processes.

Another possibility when considering fall-back options is using multiple providers, applications or infrastructures so that contingency options are available. But this is not always feasible. There is no real alternative to the global internet, where the only realistic approach is a long-term joint effort by national governments, companies, non-governmental organizations and experts to make the internet more secure.[2] Another hurdle for having multiple contingency options is the poorly functioning market for digital services and products, particularly in the field of cyber security.[3] The result is that governments, companies and organizations worldwide must choose between a handful of large providers.[4] Precisely because of their size and importance, these providers are attractive targets for geopolitically motivated attacks. At the same time, they have become 'too big to fail' for major sections of the global economy.

---

[1] Maersk was able to restore this system through sheer chance. One of its terminals in Ghana had been down during the incident due to a local power outage. This terminal escaped the *NotPetya* attack, allowing Maersk to make a copy of the system. See Greenberg, 2018.

[2] WRR, 2015; Mueller, 2017.

[3] Overvest et al., 2018.

[4] The three largest Dutch banks depend on the services of the security company Akamai. See Overvest et al., 2018.

That said, concentration also has advantages when it comes to limiting disruption. Precisely due to their scale, large cloud providers are often better protected against cyber-attacks than the organizations that use them to host their data. With economies of scale, the services of these providers are often cheaper than those of smaller parties. At the same time, customers need to be confident that these giants are taking adequate measures to handle disruption. If many customers simultaneously face the same problem, questions will inevitably arise about who gets priority. The outage of Google Cloud (see Sect. 4.1) showed that Google had all kinds of contingency plans in place. The question is to what extent these plans are consistent with the public interests that the government represents.

An alternative fall-back option would be returning to more 'old-fashioned' ways of working. In the event of disruption or the failure of digital facilities, organizations are usually still able to temporarily revert to less efficient modes of working through paper-based methods or the manual operation of mechanical installations. But this assumes that employees are still *able* to work with these older systems, and that those systems remain available. The rise of digitization and robotics has meant that manual skills and 'old-fashioned' facilities (such as local bank branches), and even cash itself, are rapidly disappearing. Preparedness implies that alternative methods and skills to assure crucial societal functions remain available. An illustrative example comes from the US Navy, which has decided to teach recruits how to navigate by the stars again.[5]

4.2.2 Isolation

Firebreaks are used in forests to contain large fires. In the event of a nuclear disaster, the reactor is encased in a concrete shell to minimize radiation leaking into the environment. For every form of disruption, there are strategies for containing the incident and preventing the damage from spreading. For digital disruption, network separation could play this role. Network separation entails placing partitions between different systems and the digital processes that handle these systems. The most radical form of network separation is for an organization to disconnect from the global internet, known as 'islanding' among IT experts. But in a highly connected world, this is not always realistic.[6] After all, these systems are connected for a reason, and islanding deprives them of this connectedness.[7] The partial separation or temporary deactivation of specific networks are more attractive options.

When implemented properly, network separation can stop disruption in its tracks or prevent further contamination. Network separation is desirable for certain key societal functions, also because it reduces dependence on third parties. Nevertheless, most government organizations currently lack clear strategies for network separation and there is limited coordination. Organizations often independently decide on the form and extent of network separation. Departments are often reluctant to set requirements due to the additional costs.[8]

[5] Mentioned in Snyder, 2017.

[6] WRR, 2017: 21.

[7] Boin, 2017: 9–10.

[8] Geer et al., 2003.

4.2.3 Cyber Security Exercises

At the national level, within the European Union and in the context of NATO, cyber security exercises focus on critical infrastructure. There are also sectoral initiatives such as in the telecommunications, water, and financial sectors. Cyber security exercises give us a more realistic picture of the form disruption could take and its potential consequences.[9] They also enable parties to identify risks and hazards, familiarize themselves with emergency procedures and practise taking decisions under duress. An additional goal is strengthening mutual trust, essential when responding to an emergency.[10]

The number of cyber security exercises rose sharply worldwide between 2002 and 2015.[11] They increasingly involve a mixed group of private and public organizations (see inset).

Cyber Security Exercises for Financial Institutions[12]

The TIBER (Threat Intelligence-Based Ethical Red Teaming) initiative launched by the Netherlands' Central Bank (DNB) tests connectivity within the financial sector. It is a public-private partnership that includes, among others, the police, the National Coordinator for Security and Counterterrorism, banks, insurance companies, pension funds and the stock exchange.

TIBER focuses on simulating cyber-attacks on financial institutions, with ethical hackers copying the working methods of real hackers. Following the test, both the attacker and the bank provide crucial information about the resilience of digital security. Lessons learnt can be used to benefit the entire financial sector.

According to DNB, the TIBER test programme is an example of successful cooperation in the field of cyber security and could also be applied in other key sectors. A pilot programme is currently taking place in the energy sector in collaboration with the Cyber Security Alliance.

While the majority of cyber exercises take place in Europe, they do not cover all key sectors. Some exercises do not focus on digital infrastructure at all.[13] Exercises that involve multiple organizations, focusing on the complex chains and networks within which they operate, are few in number. But such exercises are vital, not only to identify dependencies, but to gain better insight into the various standards and protocols that organizations use. Cyber security exercises help organizations to learn how others respond and who should be approached in common situations.[14]

[9] Lawson, 2013; Bergstrom et al., 2016.

[10] Boeke, 2016.

[11] ENISA, 2015: 22–23.

[12] https://www.dnb.nl/en/news/news-and-archive/DNBulletin2018/dnb379565.jsp. See also: https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html

[13] See e.g. Netherlands Court of Audit, 2019: 9.

[14] EPSC, 2017.

4.2.4 Provision of Information

Another way of mitigating the effects of digital disruption is to provide information about what is happening and how to best respond. What constitutes useful information varies. Organizations affected by disruption need to know what actions they can take to limit the impact as much as possible. For instance, there are detailed communication requirements for the failure of electronic payment transactions, designed to help restore confidence.[15] Emergency services must have eyes on the ground; members of the public must know about first aid, emergency escape routes, and how to notify the authorities. The digital equivalent would include providing information about the installation of patches and about additional measures to reduce the risks of being affected.

The provision of information to citizens merits particular attention. During and immediately after societally disruptive events, citizens are often seen saving themselves and assisting others.[16] But the longer a disruptive situation lasts, the more it affects people's capacity to respond rationally. Little can be done about this. Research shows that citizens hardly ever prepare for disruptive events. They generally underestimate the likelihood of disruption or believe the consequences will be manageable. While people attach great importance to the government's response to crisis situations,[17] many governments prioritize asking citizens to take preventive measures. Information on coping with and responding to digital disruption is largely absent.[18]

Digital channels and social media can play key roles in crisis communication.[19] As almost everyone is connected to everyone else, people can be informed of disruptive events very quickly, even in real time, and be advised on how to get back to their normal daily business. Of course it is not only the government that uses social media: citizens communicate about incidents among themselves, sharing pictures and video clips, as happened during the attack on the Boston Marathon in 2013.[20] Social media can also be a highly disruptive factor in crisis communication. In the event of an incident, it is often members of the public who occupy 'front-row seats', broadcasting what they are witnessing to large numbers of other people and giving

[15] https://www.dnb.nl/binaries/Joint%20Forum%20High%20Level%20Principles%20for%20Businss%20Continuity_tcm46-145518.pdf?2019070914

[16] Helsoot & Ruitenberg, 2004.

[17] Donahue et al., 2014.

[18] Frerks, 2018. On https://crisis.nl/wees-voorbereid/cyberaanval/, the Dutch government advises citizens about what to do before, during and after a cyber-attack. The advice for before and after an attack mainly concerns IT-related measures such as the use of antivirus software and changing passwords. The European Commission states that 'Providing the public with information on how they can mitigate at user and organizational level the effects of an incident could be an effective measure to mitigate a large-scale cybersecurity incident or crisis', illustrating how the provision of information still needs work in member states.

[19] Simon et al., 2015.

[20] Cassa et al., 2013.

their own, often emotional, account of events. If an incident were to disrupt or take out digital channels of communication, this would – in a society accustomed to rapid digital communication – only exacerbate people's feelings of unease. It has become extremely challenging for governments to maintain the upper hand in providing information. In cross-border cyber incidents, EU member states only coordinate their public communications to a very limited extent.

4.3 Detection and Early-Warning Systems

The early detection of disruptive events is important because the longer the signs go unnoticed, the greater the potential for damage.[21] Early detection can take many possible forms, including the monitoring of networks and data flows; this approach is mainly technical in nature and will not be considered in detail here. We turn to the sharing of information between parties, an effective means to guarantee the performance and continuity of key sectors.[22] How this is organized and the development of a strategic information position are important factors.

4.3.1 Organizing the Exchange of Information

The exchange of information in many countries is organized through public-private partnerships. At the European level, the European Union Agency for Cyber Security (ENISA) and the European Computer Response Team (Cert-EU) are the primary information node and centre of expertise, representing the institutions of the European Union in numerous national and international forums. At the state level, National Cyber Security Centres fulfil similar functions, serving as the Computer Security Incident Response Team for national governments and critical service providers.

In the Netherlands, the exchange of information between government bodies and public and private actors has become much more comprehensive. Digital processes such as the government's electronic message service and the identification and authentication of citizens and companies wishing to use government services have been designated as critical services. The implementation of the Network and Information Security (NIS) Directive means that internet exchange points, top-level domain name registries and DNS service providers fall under this regime.[23] The NIS

[21] EPSC, 2017: 4.

[22] Settanni et al., 2017; Luiijf & Kernkamp, 2015; Choo, 2011.

[23] The NIS Directive applies to essential services rather than to key processes. Organizations that fall within these three categories provide a service essential to the continuity of critical and/or key economic activities. The provision of the service depends on network and data systems, and an incident would have a significant disruptive effect on the provision of that service.

Directive obliges major digital service providers to report incidents and to take measures to manage risks and reduce the consequences of incidents.[24] Although this extension of legislation is an important step, questions remain about the structure of the current system.[25] While the exchange of information is largely organized along sectoral lines, digitized societal processes are often interconnected, meaning any disruption could be accompanied by cascade effects between sectors. A quick and effective response to disruption would require the exchange of information not only within sectors but between them.[26]

The exchange of information is also hampered by the distinction between 'critical providers' and 'non-critical providers'. While critical providers exchange information with each other and with the government through Information Sharing Analysis Centres, many organizations classified as critical use the services of parties whose products and services are *not* classified as critical. The latter are not bound by the same reporting obligations as critical providers, although their operations may have a major impact on the continuity of critical processes (see inset).

Power Supply Under Pressure from Digitization[27]

The electricity system is classified as critical infrastructure in almost every country. Because this system increasingly relies on digital technology, any issues with digital technology could have a major impact on the supply of power. Yet the suppliers of digital technology are often not required to meet the same safety and security requirements as providers of critical services.

Advanced software and algorithms play a growing role in the supply, transport, and distribution of electricity. This trend is introducing new vulnerabilities. The risk of outages due to programming errors increases because processes in power plants and electricity networks are controlled by increasingly complex software programs. Disruption can also occur if autonomous digital systems behave in unexpected ways and/or respond to one another in unexpected ways – a risk with pre-programmed systems for energy production and supply from solar panels and wind turbines. Our digitized electricity system is also vulnerable to deliberate disruption, particularly now that many parts of the system are connected to the internet.

Because more and more societal functions depend on electricity, the consequences of incidents are likely to be more serious. And because the power supply of many European countries is now interlinked, vulnerabilities in the electricity system of one country also pose risks to the electricity systems of other countries.

[24] This includes online marketplaces, search engines and cloud service providers.

[25] For references to critical reports, see CSR, 2017: 3.

[26] Cf. CSR, 2017: 6.

[27] Based on Council for the Environment and Infrastructure, 2018: 14–19. Cf. ENISA for further vulnerabilities to cyber-attacks: https://www.enisa.europa.eu/publications/power-sector-dependency

The question is to what extent the current distinction between 'critical' and 'non-critical' providers should be retained. The same question arises for the critical and non-critical parts of government, because information flows transcend the departmental boundaries and levels of government.[28]

The distinction between critical and non-critical processes also affects businesses and societal organizations. While companies and organizations deemed non-critical receive less information about vulnerabilities, they often fulfil key societal functions such as supplying medicines or checking the quality of drinking and swimming water.[29] To bridge this gap in the Netherlands, the Digital Trust Centre has been set up as a counterpart to the Information Sharing Analysis Centres for the private sector. But the companies served by the Digital Trust Centre vary enormously in the information they need, their ability to take remedial measures, and the potential impact on society of any disruption in their functioning. The same problem exists in other countries. The British Cyber Security Strategy identifies a number of 'preferential sectors' in addition to 13 vital sectors, on the grounds that 'other companies and organizations' also need more support.[30]

Although information sharing has improved significantly in recent years, the definition of society's core processes requires adjustment. As these processes are increasingly digitized and embedded in complex networks, clear distinctions between 'critical' and 'non-critical' processes can no longer be made; nor will measures solely targeting critical processes necessarily improve our security. There are so many 'unknown unknowns' that it is impossible to know in advance exactly which processes or outages would lead to disruption.[31] The cross-border chains and networks within which critical providers operate necessitate international information sharing. We need a more strategic approach to information to better understand the dependencies involved.

4.3.2 Strategic Information

Cyber risks are relatively new and remain difficult to identify and evaluate. Nevertheless, important steps have been taken in recent years to share information on digital security measures, vulnerabilities and incidents.[32] We know, for instance, that every piece of commercial software has many vulnerabilities, the majority of

[28] WRR, 2011a.

[29] For examples see: https://www.volkskrant.nl/nieuws-achtergrond/had-de-storing-van-112-voorkomen-kunnen-worden~b235b093/

[30] HM Government 2016. One criticism is that the more 'vital' processes are identified, the more complex the task of setting priorities becomes. See House of Lords, 2018.

[31] Boin, 2017; Carr, 2015.

[32] Hausken, 2007.

which have not yet been discovered.[33] In the meantime, vulnerabilities are also appearing in hardware (such as chips), meaning that it is possible to read the memory of computers without authorization.[34] The landscape of malicious actors is also constantly changing. All this means that the task of identifying potential issues and publicizing the available solutions is never finished. Given the global and sometimes geopolitical nature of the threats, robust international cooperation and the structural involvement of intelligence services are vital.

Our current level of information sharing on security measures, vulnerabilities and incidents is insufficient for an adequate detection system. There are too many gaps in our knowledge about the chains and networks through which digital disruption could spread. We need detailed insight into the interdependencies between companies and organizations involved in society's core processes, the importance of which are often underestimated.[35] The potential effects of disruption further down the chain currently remain outside of risk analyses and crisis plans.

Understanding these dependencies requires analysis from an international perspective.[36] While attacks often exploit generic vulnerabilities, incidents may affect European member states in different ways. The services of EU member states may be interdependent, meaning that incidents in one country can impact other countries, as seen for example in international payment traffic. Attackers' use of networks to achieve their goals also means disruptions will have wider reach.

More knowledge is also required about the government's strategic position. What crisis-management options are available? What dependencies would the government have to contend with? Most providers of critical services are privately owned and do not fall under direct government control; many are based overseas. What authority would the government have over such parties? The context in which the government must operate is affected by market concentration and foreign ownership. Although the risk of (foreign) share ownership is adequately contained in many sectors, it remains a key concern for critical infrastructure.[37] As critical processes are digitized, the same applies to dependence on (foreign) private digital service providers, such as cloud providers. Looking ahead, decisions will need to be made about investments in new digital technology. If the government does not anticipate developments early and seek to manage them, it may become more difficult to manage digital disruptions when they occur.

---

[33] According to Schneier (2015: 145–146), there are hundreds or even thousands of vulnerabilities. Pupillo et al., 2018 arrive at a much lower number (at least 14 vulnerabilities in an average software program).

[34] See for example: https://techcrunch.com/2018/05/01/what-do-meltdown-spectre-and-ryzenfall-mean-for-the-future-of-cybersecurity/?guccounter=1

[35] NCTV, 2018; Klaver et al., 2013: 56; CSR, 2017.

[36] ENISA, 2018: 21.

[37] Bulten et al., 2017: viii.

4.3.3 Responsibilities

Experience suggests that security within sectors does not improve unless the government takes a clear lead. But in complex, networked societies and economies, security also requires collective commitment from all parties involved.[38] Here the responsibility of the government is to create the conditions which ensure the effective sharing of information. At the same time, the government should encourage, and sometimes require, market actors to take their responsibilities seriously and to develop the necessary capabilities to do this. The government has traditionally played this role to ensure the continuity of core societal processes. Their digitization means that the government must play this role in the digital domain as well.

Sharing and analysing information is necessary to improve the cyber security of organizations, to make them more resilient to incidents, and to limit the damage when incidents occur. But not all parties currently participate in the Information Sharing Analysis Centres. Some are reluctant to share sensitive information in light of competition, legal restrictions, national security, and the government's ability to use it for law enforcement purposes.[39] Such reluctance may be greater during a crisis with reputational damage at stake.[40] Nevertheless, security must be everyone's priority.[41] The challenge is for the government to improve its position without jeopardizing security, confidentiality and the systematic sharing of information. The EU's Network and Information Security Directive provides the tools for this by imposing stricter requirements on critical providers for reporting incidents.[42] But we still do not know enough about how this will be supervised, or about the consequences for violating the trust on which the sharing of information is based.[43]

4.4 Responding to Incidents

Digital processes have been affected by incidents large and small in recent years. Incidents in the Netherlands have been handled successfully, in that they did not lead to widespread societal disruption. This may tempt us to conclude that current instruments and regulations are adequate. But the continuing march of

[38] WRR, 2012.

[39] Koepke, 2017.

[40] Bharosa et al., 2010.

[41] Van Vollenhoven, 2018: 80.

[42] There are a number of reporting obligations. See Sect. 4.5.

[43] Luiijf and Kernkamp (2015: 18) argue that relationships based on trust should be regulated through rewards (in the form of information from other parties) as well as sanctions (withholding information).

digitization – particularly the growing interconnectedness of the digital and physical realms – encourages us to rethink existing frameworks and procedures. There are three specific areas where we need to reassess our existing instruments. We discuss them in turn below: legal powers, cross-border mitigation, and setting priorities.

4.4.1 Legal Powers

In the physical realm, the government has emergency services such as the police, fire brigade, ambulance and rescue teams to respond to crises. These and other services have legal powers to carry out their duties, for example the ability to cordon off particular locations, enter a company's premises or initiate an evacuation. But what resources can the government call on in the event of a digital crisis? The hack at DigiNotar in 2011 painfully revealed the government's dependence on private actors to resolve problems in the digital realm.

The Acquisition of DigiNotar[44]

On 29 August 2011, the government received a report of problems at the DigiNotar certificate authority, responsible for securing electronic communications from and between government bodies (known as Public Key Infrastructure or PKI). Hackers had managed to release forged DigiNotar certificates. As a result, government certificates could no longer be relied on and were possibly even unusable. Goods at the Port of Rotterdam could no longer be accepted, social security payments were blocked, and the payments system compromised.

The immediate reason for the impending crisis lay with the major browser suppliers, including Microsoft, which were losing confidence in all DigiNotar certificates, including the PKI government certificates. This was a very real threat as Microsoft could have blocked the use of all DigiNotar certificates with its monthly security update to maintain confidence in its own systems. Regardless of the parties involved, Microsoft did not want to continue supporting potentially unsafe communications.

At this point, the Dutch government had every interest in clarifying how many certificates had been manipulated or compromised. But despite urgent investigations, it was unable to retrieve this information. On 3 September, the government decided to take over the management of DigiNotar. There was no specific legal basis for this, but the Dutch government was able to count on the 'voluntary' cooperation of its American parent company Vasco. Microsoft then postponed its security update in the Netherlands for 1 week, which bought enough time to replace the certificates.

[44] Based on reports from the Dutch Safety Board 2012 and the Inspectorate of Justice and Security 2012 that evaluated the Diginotar incident.

Estonian Government and Gemalto[45]

The vulnerability in the chip of Estonian ID cards is a more recent example of the dependence of governments in solving problems in the digital realm. In September 2017, a vulnerability was discovered in a certificate that affected laptops and PCs as well as authentication to cloud applications. The vulnerability also affected ID cards in Estonia and eID cards in Slovakia, Spain and other countries. In Estonia, the ID card is used to authenticate one's person and to digitally sign documents. In theory, hackers were able to steal users' digital identity and access sensitive personal information, manipulate the results of e-voting, and hack into the state's information systems.

In November, the Estonian government decided to suspend all certificates of approximately 800,000 ID cards. Intensive users such as doctors were able to update their certificates at several government locations while the remote updating of certificates was disabled. Gemalto, the company that produced the chips, and the Estonian government, seeking €152 million in damages, traded accusations. The government was unhappy with Gemalto's handling of the security breach, especially its failure to notify the government of the problem.

At first glance, the Dutch decision-making structure for granting legal powers for crisis decision-making appears in good order. If societal disruption occurs, decisions are made through structures set out in the National Guide for Crisis Decision-Making (NHC). There is also a National ICT Crisis Plan, currently under review. In the NHC, the government has three roles: facilitation, management, and coordination. The latter, including the deployment of the police and fire brigade, and requisitioning resources, requires legal authority. The NHC also refers to 'measures in the event of a major IT incident' which are not set out in detail.[46]

The national IT Crisis Plan describes an IT crisis as 'a threat or crisis that originates in the field of information technology, which places one or more vital interests in jeopardy and for which the regular structures are not adequate.'

In the event of an (imminent) IT crisis, the IT Response Board (IRB) is activated. The IRB – a flexible public-private partnership – analyses the crisis and, if necessary, advises the Interdepartmental Crisis Management Committee, the official communication channel for the Ministerial Crisis Management Committee, chaired by the Minister of Justice and Security or the Prime Minister.

[45] See Ventsel and Madisson 2019 for a reconstruction of the Estonian case.

[46] The Dutch National ICT Crisis Plan includes nothing on this subject either.

Private actors can be required to cooperate if (imminent) disruption or the failure of their systems could undermine the public interest. They are required to keep the government informed about the situation and to cooperate in tackling the causes and consequences of the disruption.[47] But the interests of private organizations are not always consistent with the public interest that government represents; nor does the government have the means to force private parties headquartered overseas to cooperate. The government's role in cyber security is often limited to providing advice or assistance to the private organizations that form the critical infrastructure. Such was the case when, partly due to the lack of powers to intervene, the municipal crisis response team in Rotterdam was unable to access information about the terminals and systems of the container company Maersk as they were being hit by the *NotPetya* attack (see inset).

NotPetya and the Municipality of Rotterdam

In June 2017, hackers working for the Russian military distributed the *NotPetya* ransomware. One of the most prominent victims was Maersk, which runs container terminals around the world. The gates to ports could not be used, cranes ceased to work, trucks were unable to unload their cargo and new cargo shipments could not be booked. Maersk, an ultramodern shipping company, was forced to revert to a paper-based system.[48]

The terminals in the port of Rotterdam were affected by the attack. Container transport via the port as well as the surrounding highways and rail links ground to a halt, causing congestion and long traffic jams. The city authorities were unprepared. They had difficulty gathering the relevant actors; the municipal crisis response organization responsible for public order was initially denied information about Maersk's terminals and systems. The city authorities were thus unable to assess the situation's seriousness and whether, for example, there was a risk to public order.

Formal assistance from the National Coordinator for Security and Counterterrorism was impossible because Maersk's APM terminals, unlike the Port of Rotterdam itself, were not part of the 'critical infrastructure'.

A great deal of sector-specific legislation outlines the powers of the government in exceptional circumstances. During a crisis, parties are obliged to cooperate and to follow government instructions. The legislation, however, is lengthy and complex.[49] Extensive explanation would be needed for relevant parties to understand the implications. Although sectoral legislation can provide useful starting points for government intervention, the question is whether these powers are sufficiently comprehensive and suited to the problems of a digital world.

[47] Luiijf and Klaver (2015: 266) argue for direct access to the relevant IT systems of producers.

[48] Greenberg, 2018.

[49] Muller, 2014: 45.

The government can also act without making use of sector-specific provisions. In a crisis, and if circumstances warrant, the law could simply be broken in a case of 'needs must'. This is not a desirable course of action.[50] It would require a degree of improvisation, better minimized for maintaining the rule of law.[51] Government actions – especially interventions by authorities such as the police and the public prosecution service – should be predictable and subject to accountability.[52] A crucial question is whether interventions would be justified if they did not also serve the purposes of an investigation or prosecution.

The problem extends to who takes the relevant decisions and initiates the required actions. As in the physical realm, the primary responsibility of companies operating in the digital realm is to ensure their own security and to draw up contingency plans for emergencies. Large companies need to arrange for their own cyber security departments, sector-specific Computer Emergency Response Teams or employ the services of private cyber security companies.[53] The government will only step in when circumstances involve (the risk of) societal disruption.

It is often not immediately clear who or what caused an incident, and in the case of deliberate disruption, the motive.[54] It can thus be unclear whether government bodies such as the Ministry of Defence, the national cyber security authorities, the police or the intelligence services should take action. As each body has its own sets of powers and interests, the government's approach could well depend on who responds to the incident: the police are primarily concerned with identifying perpetrators so that the public prosecutor can take action; the intelligence services are more inclined to protect their information position; the national cyber security agency, given its remit to ensure information security, openness and stability, focuses on remedial action. While the police also have the powers to provide assistance and to prevent escalation, public order and security must be at stake.[55] A national cyber security authority would not always be bound by this requirement.

In conclusion, legal powers for the digital domain and for mitigating disruption are not always sufficiently clear and well defined. The emphasis is currently on advising and supporting parties within infrastructure categorized as critical. But if parties refuse to cooperate, it is unclear what powers the government has to intervene, and on what grounds. Given the limited powers of the national cyber security authority, which focuses on technical expertise and assistance, previous interventions have largely been ad hoc.

---

[50] Within the modernization of state emergency law, consideration is currently being given to supplementing existing emergency powers with specific powers over certain IT services. See: https://www.rijksoverheid.nl/documenten/kamerstukken/2018/07/03/tk-modernisatie-staatsnoodrecht

[51] See Kortmann, 2009.

[52] To obtain information, the Public Prosecutor can initiate a search warrant process in accordance with art. 96c Sv. See Prins, 2019: 721.

[53] For a similar argument, see Prins, 2012: 44–45.

[54] Prins, 2012: 45.

[55] Prins, 2019: 578.

4.4.2 Combating Cross-Border Crises

Digital disruption will unlikely be confined within national borders. Research shows that cross-border crises are by definition challenging.[56] Nevertheless, some steps have already been taken at the international level. For example, the EU has put various crisis management provisions in place, some specifically for cyber security.[57]

> The most important initiative is the Cyber Security Strategy of the European Union which dates from 2013, on which the 2016 Network and Information Security Directive and the 2018 Cyber Security Act are based. The NIS Directive obliges member states to establish a national centre for cyber security and establishes European level cooperation between these centres. The Cyber Security Act strengthens ENISA, the EU agency for cyber security.
>
> The EU has a number of specialist cyber security organizations, including ENISA, the European Centre for Cyber Crime (EC3), which falls under Europol, the European Defence Agency (EDA), and the European Computer Emergency Response Team (CERT-EU).
>
> A number of countries, including the Netherlands, have signed a letter of intent for a European Cyber Rapid Response Force to respond quickly in the event of a large-scale digital incident.[58]
>
> The Forum of Incident Response and Security Teams (FIRST) is a worldwide partnership of CERTs.

The capacity of these facilities has improved in recent years.[59] While cross-border initiatives have been initiated to improve cyber security in critical sectors, such as energy and transport,[60] existing mechanisms for dealing with cross-border crises are fragmented across a range of institutions. Their functions are not always clearly defined and, according to experts, their effectiveness is at best limited.[61] Although the NIS Directive should lead to improvements, it still does not provide a framework for EU-level cooperation in the case of major cyber incidents.[62] EU

[56] Boin & Lodge, 2018.

[57] Backman & Rhinard, 2018.

[58] https://eeas.europa.eu/topics/eu-international-cyberspace-policy/47525/new-tool-address-cyber-threats-eus-rapid-response-force_en. Compare the proposal for a European cyber agency in CEPS, 2018. This agency also has the authority to attribute attacks.

[59] https://www.enisa.europa.eu/news/enisa-news/csirts-and-incident-response-capabilities-in-europe

[60] European Commission, 2016.

[61] Boin & Lodge, 2018; cf. European Commission, 2016: 2.

[62] Implemented in the Netherlands through the Network and Information Systems Security Act (17 October 2018, Bulletin of Acts and Decrees 2018, 387). https://wetten.overheid.nl/BWBR0041515/2018-11-09

member states have therefore asked the European Commission to produce plans for responding to a major cyber incident involving multiple member states. In the meantime, the 'blueprint'[63] outlines what a timely and effective response would look like. Practice exercises are needed, and since the blueprint does not provide any new legal powers, combating incidents will still fall on national crisis management mechanisms. The question is whether these are still fit for purpose.

4.4.3 Setting Priorities

Not all instruments and resources can be deployed simultaneously. Some areas will have to be prioritized, again pointing to the importance of clearly defined decision-making powers. There are questions about when the government should deploy which instruments, the most effective use of resources, and the relationship between detecting and counteracting incidents on the one hand and legal powers on the other. Many governments are also working to improve the categorization of cyber incidents.

France is considering classifying cyber-attacks according to specific response options.[64] The United States has had such a system since 2014, where The National Cyber Security and Communications Integration Center (NCCIC) reports incidents and assesses risks by assigning a score between 1 and 100 based on 8 criteria:
actual impact on an organization;
observed activity;
location of detection;
actors involved;
type of information that has been lost, compromised or corrupted;
recovery options;
cross-sectoral dependencies;
extent of societal disruption.[65]

The United Kingdom has recently developed a system of six categories of incidents, covering the entire spectrum from local incidents to national emergencies. The British National Cyber Security Centre links each category to a party responsible for responding to the incident.[66]

[63] See http://ec.europa.eu/transparency/regdoc/rep/3/2017/NL/C-2017-6100-F1-NL-MAIN-PART-1.PDF. A blueprint is also attached to the document. See: http://ec.europa.eu/transparency/regdoc/rep/3/2017/NL/C-2017-6100-F1-NL-ANNEX-1-PART-1.PDF

[64] Secrétariat général de la défense nationale, 2018: 140.

[65] https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System and https://grants.nhisac.org/BackgroundData/Cyber_Incident_Severity_Schema.pdf

[66] https://www.ncsc.gov.uk/news/new-cyber-attack-categorisation-system-improve-uk-response-incidents

Following the EU blueprint for preventing incidents, the European NIS cooperation group[67] has drawn up a taxonomy of large-scale cyber incidents.[68] Alongside malicious acts, it includes spontaneous system failure, natural phenomena such as fires, floods and earthquakes, human error, and failures by third parties. The aim is to link this taxonomy to integrated EU political crisis response (IPCR) regulations.

While the Dutch government's assessment of incident severity is linked to its list of critical infrastructure, the examples above show the usefulness of additional criteria for combating digital incidents. For starters, the national government would not have to be involved in all incidents. A more differentiated classification system could form the basis for a more clearly defined division of responsibilities, both within the various layers of government (such as the national cyber security authority, government departments, safety regions, and municipal information security services) and between government bodies and the business community. A more nuanced classification system for cyber incidents would allow for more effective responses, as action by the central government would no longer have to be directly linked to incidents involving critical infrastructure.

Prioritization also needs to occur on the spot. In the event of a major fire, the fire brigade can choose to put out the fire or to minimize damage by keeping nearby buildings wet; adjacent buildings may suffer water damage, but would be salvaged. Something similar may apply to disconnecting digital systems, requiring the assessment of the risks of acute interruption to operations and the risks of problems spreading further, possibly leading to broader damage. Because many digital systems are in the hands of private parties, the considerations the government will consider when intervening must be clear in advance.

Prioritization involves both technical and substantive aspects. On the technical side, the logic of the systems will play a role. This means that decisions regarding connecting and disconnecting networks will be based on a particular sequencing; here it is essential to know how the various systems and organizations in a network are connected. In terms of content, there is the question of which processes should be kept operating the longest and be restarted first in the event of failure. The government's choices will not always be self-explanatory to all parties. Private actors may want to safeguard their own systems and those of their clients first, rather than prioritizing the public interest.

In the Netherlands, the continuity of critical processes is given priority in the event of an incident. Critical processes that fall under category A (the disruption of which would have severe economic and societal impact) are prioritized over those in category B (the disruption of which would have a more limited, but still

[67] The NIS cooperation group consists of representatives of EU member states, ENISA and the European Commission. It was established on the basis of Article 11 of the NIS Directive.

[68] http://ec.europa.eu/information_society/newsroom/image/document/2018-30/cybersecurity_incident_taxonomy_00CD828C-F851-AFC4-0B1B416696B5F710_53646.pdf

substantial economic and societal impact). Digitization challenges this categorization. For digital facilities, the current list of critical infrastructure focuses mainly on traditional telecommunications services and their role in for instance the deployment of emergency services and communication between emergency services. The telecoms/IT sectors, however, fall under category B. Whether this is sustainable is doubtful. Second only to the power supply, the failure of digital facilities would likely lead to the most significant cascade effects. There are detailed shutdown and recovery plans for electricity companies, with the restoration of public order and safety being priorities. No such plans are in place for digital disruption, again underlining the importance of rethinking our definition of critical processes.

4.5 Recovery & Reconstruction

The final phase in dealing with digital disruption concerns recovery and reconstruction – the resumption of normal functioning. If normal everyday life is seriously disrupted, various steps will be required to get things working normally again. Often things will not return to how they were before the disruption because people and organizations learn from the incident. Companies and organizations affected by a computer virus or ransomware, or which have experienced system and process failures for other reasons, often alter their policies (for example staff only using USB sticks under strict conditions). To learn from such incidents, we must analyse what went wrong. The recovery and reconstruction process also requires adequate facilities. This means, for example, that victims are compensated for damages. Learning lessons and providing compensation are to some extent related. Those who wish to redesign core societal processes must have the resources to do this.

4.5.1 Evaluating and Learning Lessons

The recovery and reconstruction phase must be used to reflect on how new digital facilities are to be embedded. This may extend to rethinking the balance between economic interests and political and administrative authority in the organization of the digital society. Changing priorities may mean developing facilities that privilege security over speed, efficiency, and low prices.

We need more than reorientation; past incidents must lead to concrete learning.[69] This often does not happen, even in the aftermath of major incidents such as *NotPetya* and *WannaCry*.[70] The availability of historical data on cyber incidents is limited; there is currently no generally accepted definition of what constitutes an incident.[71] An additional problem is that most data on incidents does not concern

[69] Van Vollenhoven, 2018.

[70] Van Tiel, 2019.

[71] Valeriano & Maness, 2018.

vulnerabilities that could lead to societal disruption. Public data on incidents tends to focus on data breaches because legal disclosure requirements focus on them.[72] The Network and Information Security Directive will change this by introducing a reporting obligation for problems that affect the continuity of 'essential services'. The European Payment Directive will also require payment service providers to report major incidents that jeopardize the financial interests of their users. As both reporting obligations have been introduced very recently, it is too early to draw meaningful conclusions.

As for the supervision of digital security, the Netherlands still lacks a designated supervisor.[73] Several organizations are active in specific, limited areas: the Data Protection Authority registers data breaches; De Nederlandsche Bank (the central bank) protects electronic payment transactions; the Telecommunications Agency monitors network providers. Several government departments are also involved as their remits cover critical sectors. The incident data that each of these organizations collects is only haphazardly shared and not always analysed, let alone in a coordinated manner.[74] This is a missed opportunity. Because digital disruptions always involve multiple organizations and sectors, it would be extremely useful to compare data on incidents.

4.5.2 Compensation

An important aspect of recovery and reconstruction is compensation to victims, whether through liability insurance or government payments. Adequate compensation reduces risks and damages to society[75] and contributes to the recovery of the economy, social stability and trust in institutions.[76] In principle, it is possible to insure against cyber risks.[77] As the market for cyber insurance is a fraction of the market for other risks, we may see considerable growth in this area.

Risks are insurable if they can be quantified in terms of their probability and impact. It must also be possible to draw on a sufficiently large group of individuals affected by the risk, who would therefore be willing to share it. Finally, risks need to be unpredictable in terms of when and where they materialize, and be beyond the control of the insured parties. Otherwise, each party would insure itself individually.

---

[72] OECD, 2017: 34. For an indication of the number of data breaches, see: https://autoriteitpersonaldata.nl/nl/onderwerpen/security/meldplicht-datalekken/Digits-datalekken-2018. The Dutch Data Protection Authority received more than 20,000 reports of data breaches in 2018. In 2017, there were 10,009 reports; in 2016, 5849 reports.

[73] This is a more general problem. See Van Vollenhoven, 2018.

[74] One exception is the National Coordinator for Security and Counterterrorism, which provides an overview of reports and incidents in an appendix to the Netherlands Cyber Security Assessment. See NCTV, 2019: 43–46.

[75] Bruggeman & Faure, 2018: 11; WRR, 2011b: 16, 53.

[76] Kuipers & Tjepkema, 2017.

[77] OECD, 2017; Biener et al., 2015.

Cyber risks are difficult to quantify due to lack of historical data. We have no clear method for classifying incidents and no insight into the resilience of companies and the types of losses they incur.[78] Cyber risks are also constantly evolving, complicating quantification. Insurers could face massive losses due to the accumulation of risks.[79] If many parties depend on the same infrastructure or suppliers, or use the same basic software, insurers will have difficulty pooling the risks across sectors or regions. Lloyd's and Cyence have estimated a cloud software service outage, depending on its duration, to cause between $4.6 billion and $53 billion in damages.[80] The accumulation of risks is a major reason the market for cyber insurance is growing so slowly. The extensive damage (see table below) and damage claims resulting from *NotPetya* are additional reasons for large insurers to limit their coverage of cyber incidents.

Impact of Interruption to Business Operations Due to the NotPetya Incident[81]

Organisation	Commercial Impact	Financial Components	Source
A.P. Moller – Maersk	$250-300 million	Earnings Reduction	Q4 2017 Financials
Beiersdorf AG	Minimal sales impact €15 million	€35 million sales shifted Q2 to Q3 Additional expenses	Q2 2017 Financials Q4 2017 Earnings Call
FedEx (TNT Express)	$400 million	Earnings Reduction	Q4 2018 Financials
Merck & Co.	$410 million $380 million	2017, 2018 Sales Reduction Additional Expenses	Q4 2017 Financials Q3 2018 Financials
Mondelez International	-$104 million $84 million	2017 Sales Reduction Additional Expenses	Q4 2017 Earnings Call Q4 2017 Earnings Release
Nuance Communications	$68 million $31.2 million	2017 Sales Reduction Additional Expenses	Q3 2018 Financials
Reckitt Benckiser	-£114 million	2% Q2 Sales Reduction 2% Q3 Sales Reduction	Press Release Q2 2017 Financials Q3 2017 Financials
Saint-Gobain	-€220-250 million €80 million	2017 Sales Reduction 2017 Earnings Reduction	Q3 2017 Earnings Release Q1 2018 Earnings Release

These insurance companies felt emboldened by the United States' attribution of the cyber-attack to Russia.[82] They also explicitly excluded alternative cover from their policies, for example through liability for or damage to company equipment (so-called 'silent cyber').

[78] OECD, 2017; ENISA, 2017; Nieuwesteeg et al., 2017. Many insurance policies focus on the loss of customer data and not on the cost of repairing digital infrastructure and losses due to disruption of business.

[79] OECD, 2017: 123.

[80] Lloyd's & Cyence, 2017.

[81] AON, 2019: 8. Based on corporate quarterly figures.

[82] https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html

Damage due to armed conflicts cannot be insured by law, due to the excessive financial risk. This causes few problems when war remains a distant prospect and there is a clear definition of 'armed conflict'. But cyber-attacks, which enable countries to harm each other's interests without ever setting foot on their soil, cannot be placed in this category so easily. A further question is whether and when computer code can be considered a 'weapon', particularly given the rapid evolution of malware. Most problematically, it is unclear when cyber-attacks merit retaliation; there are no international rules or definitions to determine this.[83] Now that insurers see cyber-attacks as a form of armed conflict and companies are protesting against this move, it is up to the legal system to determine the extent to which a cyber-attack carried out by a foreign state is, in fact, an act of war.[84]

The handling of other major incidents shows that solutions exist. After the 9/11 attacks, insurers withdrew because they no longer wanted to compensate clients for losses due to terrorist incidents. It is likewise almost impossible to insure against flooding in the Netherlands, although a public-private arrangement now provides insurance against terrorism, for which insurers are not required to compensate all losses and for which the government acts as the guarantor of last resort.[85] Similar public-private arrangements are found in Belgium and Germany. Such constructions enable insurers to offer insurance products without unacceptably high financial risks for themselves. Applied to digital disruption, it would mean that the government provides compensation for damages exceeding a certain limit. Once this guarantee has been provided, insurers could expand the market for cyber security risks and companies would, in principle, be liable for the costs of smaller incidents.

4.6 Conclusion

The government and other parties have always taken steps to minimize the potential consequences of societal disruption. Digitization adds a new form of disruption to the list of risks we are already familiar with. This section has focused on contingency measures in anticipation of digital disruption. Our main conclusion is that these measures have yet to be adequately implemented and that the government and other parties are insufficiently prepared. A number of steps are required:

- There is currently no coherent policy for critical infrastructure: for back-up options, the isolation of chains and networks, for cyber exercises, and for providing information on how to respond to urgent incidents. While regulations diverge between sectors and organizations, other factors undermine our preparedness as a society. Back-up options disappear as analogue systems are decommissioned

[83] Mačák, 2017.

[84] Several companies currently have legal cases against insurance companies, which may require judges to decide whether cyber-attacks are in fact a form of 'armed conflict'.

[85] For an extensive discussion of both attempts to insure against the risk of flooding and the terrorism pool, see Bruggeman & Faure, 2018: 61–62, 70–72.

and organizations outsource important facilities to third parties, further increasing the interdependence between processes and sectors.

- Information sharing has recently improved and become much more comprehensive. But it is still hampered by sectoral divisions and a partly outdated distinction between critical and non-critical providers. This means that signals may not be picked up (or picked up too late) by the relevant actors. A broader perspective is needed for gathering and sharing knowledge. While the current focus is on digital security measures, vulnerabilities and incidents, there is much less clarity for service providers and governments when it comes to chains, networks and the dependencies they create. This kind of knowledge is essential if we want to be able to classify the severity of incidents and manage the spread of digital disruption.
- In combating digital disruption, the government depends on information and cooperation from private actors (many of them based overseas). But the government lacks any clearly defined authority to intervene on the basis of specific categories of digital incidents; there is also little clarity about which public bodies should take action for which type of incident. Greater powers for the government should be accompanied by adequate protection for private parties, as interventions based on coercion may have adverse financial effects.
- Digital disruption can cross national borders, calling for international coordination. The current approach relies on partly inadequate national mechanisms, which is particularly risky in light of the spill-over effects into critical infrastructure elsewhere in Europe and attacks on European institutions. The need for European and international cooperation is urgent due to the geopolitical dynamics that surround digital disruption.
- Recovery and reconstruction would currently be difficult to achieve. The funds required for recovery would be in short supply now that insurers seem to be withdrawing from the cyber insurance market. But other major incidents of damage show that solutions are possible. While learning from incidents requires wide-ranging reflection and analysis, this is currently limited by various supervisory authorities processing the available data on incidents in isolation, precluding the benefits of potential learning effects.

References

AON. (2019). *Cyber perils in a growing market. Helping EMEA organizations better understand the interconnectivity among multiple lines of insurance*. https://www.aon.com/unitedkingdom/insights/cyber-perils-in-a-growing-market.jsp

Backman, S., & Rhinard, M. (2018). The European Union's capacities for managing crises. *Journal of Contingencies and Crisis Management, 26*(2), 261–271.

Bergström, J., Uhr, C., & Frykmer, T. (2016). A complexity framework for studying disaster response management. *Journal of Contingencies and Crisis Management, 24*(3), 124–135.

Bharosa, N., Lee, J., & Janssen, M. (2010). Challenges and obstacles in sharing and coordinating information during multi-agency disaster response: Propositions from field exercises. *Information Systems Frontiers, 12*(1), 49–65.

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risks: An empirical analysis. *Geneva Papers, 40*, 131–158.

Boeke, S. (2016). *First responder or last resort? The role of the ministry of defence in national cyber crisis management in four European Countries*. Leiden University.

Boin, R. A. (2017). *De grenzeloze crisis: Uitdagingen voor politiek en bestuur* [Crisis without borders: Challenges for politics and management]. Inaugural lecture, Leiden University.

Boin, R. A., & Lodge, M. (2018). *Enhancing the EU's transboundary crisis management capacity: Recommendations for practice*. TransCrisis.

Bruggeman, V., & Faure, M. (2018) Compensation for victims of disaster in Belgium, France, Germany and the Netherlands. *WRR Working Paper* 30. https://www.verzekeraars.nl/media/5662/compensation_for_victims_of_disasters_working_paper_30.pdf

Bulten, C., de Jong, B., Breukink, E., & Jettinghoff, A. (2017). *Vitale vennootschappen in veilige handen* [Vital companies in safe hands]. Radboud Business Law Institute. https://www.wodc.nl/binaries/2609_Volledige_Tekst_tcm28-250320.pdf

Carr, N. (2015). *De Glazen Kooi: Wat automatisering met ons doet* [The glass cage: What automation does to us]. Maven.

Cassa, C. A., Chunara, R., Mandl, K., & Brownstein, J. S. (2013). Twitter as a sentinel in emergency situations: Lessons from the Boston marathon explosions. *PLOS Currents Disasters*. https://currents.plos.org/disasters/index.html%3Fp=8687.html

CEPS (Centre for European Policy Studies). (2018). *Strengthening the EU's cyber defence capabilities. Report of a CEPS task force.* CEPS.

Choo, K. (2011). The cyber threat landscape: challenges and future research directions. *Computers & Security, 30*(8), 719–731.

Council for the Environment and Infrastructure. (2018). *Stroomvoorziening onder digitale spanning* [Electricity network under digital pressure]. The Hague.

CSR (Cyber Security Raad) [Cyber Security Council]. (2017). *Naar een landelijk dekkend stelsel van informatieknooppunten, advies inzake informatieuitwisseling met betrekking tot cybersecurity en cybercrime* [Towards a nationally comprehensive system on information nodes. Advice on information exchange regarding cyber security and cyber-crime]. https://www.cybersecurityraad.nl/binaries/CSR_Advies_Informatieuitwisseling_NED_DEF_tcm107-314535.pdf

Donahue, A. K., Eckel, C. C., & Wilson, R. K. (2014). Ready or not? How citizens and public officials perceive risk and preparedness. *American Review of Public Administration, 44*(4), 89–111.

Dutch Safety Board. (2012). *Het DigiNotar-incident. Waarom digitale veiligheid de bestuurstafel te weinig bereikt* [The DigiNotar incident. Why digital security is not reaching the board room enough]. The Hague.

ENISA. (2015). *The 2015 report on national and international cyber security exercises. Survey, analysis and recommendations*. ENISA.

ENISA. (2017). *Commonality of risk assessment language in cyber insurance. Recommendations on cyber insurance*. https://www.enisa.europa.eu/publications/commonality-of-risk-assessment-language-in-cyber-insurance

ENISA. (2018). *Good practices on interdependencies between OES and DSPs*. ENISA.

EPSC [European Political Strategy Centre]. (2017). *Building an effective European Cyber Shield. Taking EU cooperation to the next level.* https://ec.europe.eu/epsc/publications/strategic-notes/building-effective-european-cyber-shield_en#-1

European Commission. (2016). *Strengthening Europe's cyber resilience system and fostering a competitive and innovative cybersecurity industry*. https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-410-EN-F1-1.PDF

Frerks, G. (2018). Citizen engagement and resilience in Dutch disaster management: A black hole in *policy* and practise? In J. Bohland, J. Harrald, & D. Brosnan (Eds.), *The disaster resiliency challenge*. Charles C. Thomas.

Geer, D., Bace, R., Gutmann, P., Metzger, P., Pfleeger, C., Querterman, J., & Schneier, B. (2003). CyberInsecurity: The cost of monopoly – How the dominance of Microsoft's products poses a risk to security. *Computer & Communications Industry Association Report*. https://www.schneier.com/essays/archives/2003/09/cyberinsecurity_the.html

Greenberg, A. (2018). *The untold story of NotPetya, the most devastating cyberattack in history*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Hausken, K. (2007). Information sharing among firms and cyber attacks. *Journal of Accounting and Public Policy, 26*(6), 639–688.
Helsloot, I., & Ruitenberg, A. (2004). Citizen response to disasters: A survey of literature and some practical implications. *Journey of Contingencies and Crisis Management, 12*(3), 98–111.
HM Government. (2016). *National cyber security strategy 2016–2021*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf
House of Lords. (2018). *Cyber security of the UK's critical national infrastructure*. https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/1708/1708.pdf
Inspectorate of Justice and Security. (2012). *Evaluatie van de rijkscrisisorganisatie tijdens de DigiNotar-crisis* [Evaluation of the national organizational crisis during the DigiNotar crisis]. The Hague.
Klaver, M. H. A., Verheesen, B., & Luiijf, H. A. M. (2013). *Intersectorale afhankelijkheden: buitenlandse methoden en mogelijke toepasbaarheid in Nederland* [Intersectoral dependencies: Methods from abroad and their possible application in the Netherlands]. TNO.
Koepke, P. (2017). *Cybersecurity information sharing incentives and barriers*. Sloan School of Management, MIT. https://cams.mit.edu/wp-content/uploads/2017-13.pdf
Kortmann, C. A. J. M. (2009). *Staatsrecht en raison d'État* [The rule of law and raison d'état]. Valedictory lecture, 27 February. Kluwer.
Kuipers, G. M., & Tjepkema, M. K. G. (2017). 'Public management' in Groningen. Publiekrechtelijke schadeafhandeling en het vertrouwen in de overheid [The settlement of public law claims and trust in the government]. *Nederlands Juristenblad, 29*(1576), 2058–2067.
Lawson, S. (2013). Beyond cyber-doom: Assessing the limits of hypothetical scenario's in the framing of cyber-threats. *Journal of Information Technology and Politics, 10*, 86–103.
Lloyd's and Cyence. (2017). *Counting the cost: Cyber exposure decoded*. Lloyd's.
Luiijf, E., & Kernkamp, A. (2015). *Sharing cyber security information: Good practice stemming from the Dutch public-private participation approach*. TNO.
Luiijf, E., & Klaver, M. (2015). Governing critical ICT: Elements that require attention. *European Journal of Risk Regulation, 2*(6), 263–270.
Mačák, K. (2017). From cyber norms to cyber rules: re-engaging states as law-makers. *Leiden Journal of International Law, 30*(4), 877–899.
Mueller, M. (2017). *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace*. Polity Press.
Muller, E. R. (2014). Crisis en recht: Naar een integrale Crisisbeheersingswet? [Crisis and the law: Towards an integral Crisis Management Act?]. In E. R. Muller, T. Hartlief, B. F. Keulen, & H. Kummeling (Eds.), *Crises, rampen en recht* [Crisis, disasters and the law]. Kluwer.
NCTV. (2018). *Cybersecuritybeeld Nederland 2018* [Cyber security assessment Netherlands 2018]. NCTV.
NCTV. (2019). *Cybersecuritybeeld Nederland 2019* [Cyber security assessment Netherlands 2019]. NCTV.
Netherlands Court of Audit. (2019). *Digitale dijkverzwaring: Cybersecurity en vitale waterwerken* [Digital flood defences: Cyber security and vital defences]. The Hague.
Nieuwesteeg, B., Visscher, L., & de Waard, B. (2017). De rechtseconomie van cyberverzekeringen [The law and economics of cyber insurance]. *Het Verzekerings-archief, 3*, 155–160.
OECD. (2017). *Enhancing the role of insurance in cyber risk management*. OECD.
Overvest, B., Braam, A. M, Windig, R., & Bartels, E. (2018). *Knelpunten op de markt voor cyberveiligheid* [Bottlenecks in the market for cyber security]. *CPB Policy Brief 2018/01*. CPB.
Prins, R. (2012). Een veilige cyberwereld vraagt nieuw denken [Safe cyber requires new thinking]. *Veiligheid in Cyberspace, Justitiële Verkenningen, 1*(12), 40–51.
Prins, J. E. J. (2019). Digitaal binnentreden om escalatie te voorkomen [Digital search warrants to prevent escalation]. *Nederlands Juristenblad, 578*.
Pupillo, L., Ferreiora, A., & Varisco, G. (2018). *Software vulnerability disclosure in Europe. Technology, policies and legal challenges*. Centre for European Policy Studies. https://www.ceps.eu/wp-content/uploads/2018/06/CEPS%20TFRonSVD%20with%20cover_0.pdf

Schneier, B. (2015). *Data and goliath: The hidden battles to collect your data and control your world*. W.W. Norton & Company.

Secrétariat général de la défense nationale. (2018). *Revue stratégique de cyberdéfense, 12 février 2018.* http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf

Settanni, G., Skopik, F., Shovgenya, Y., Fiedler, R., Carolan, M., Conroy, D., et al. (2017). A collaborative cyber incident management system for European interconnected critical infrastructures. *Journal of Information Security and Applications, 34*, 166–182.

Simon, T., Goldberg, A., & Adini, B. (2015). Socializing in emergencies: a review of the use of social media in emergency situations. *International Journal of Information Management, 35*(5), 609–619.

Snyder, C. (2017). *Too connected to fail. How attackers can disrupt the global internet, why it matters and what we can do about It.* Cyber Security Project, Belfer Center for Science and International Affairs.

Valeriano, B., & Maness, R. C. (2018). How we stopped worrying about cyber doom and started collecting data. *Politics and Governance, 6*(2), 49–60.

Van Tiel, B. (2019). *Kritische waakhond, vergeet de digitale veiligheid niet* [Critical watch dog, do not forget digital security]. https://www.pwc.nl/nl/themas/blogs/kritische-waakhond-vergeet-de-digitale-veiligheid-niet.html

Van Vollenhoven. P. (2018). *Oproep van een waakhond* [Appeal from a watchdog]. Balans.

Ventsel, A., & Madisson, M. (2019). Semiotics of threats: Discourse on the vulnerability of the Estonian identity card. *Sign Systems Studies, 47*(1/2), 126–151.

WRR [Netherlands Scientific Council for Government Policy]. (2011a). *iOverheid* [iGovernment]. Amsterdam University Press. https://english.wrr.nl/latest/news/2011/11/29/igovernment-available-in-english

WRR [Netherlands Scientific Council for Government Policy]. (2011b). *Evenwichtskunst. Over de verdeling van verantwoordelijkheid voor fysieke veiligheid* [Balancing act. On the division of responsibility for physical security]. Amsterdam University Press. https://english.wrr.nl/latest/news/2012/10/09/evenwichtskunst-available-in-english

WRR [Netherlands Scientific Council for Government Policy]. (2012). *Publieke zaken in de marktsamenleving* [Public affairs in the market society]. Amsterdam University Press. https://www.wrr.nl/publicaties/rapporten/2012/04/12/publieke-zaken-in-de-marktsamenleving

WRR [Netherlands Scientific Council for Government Policy]. (2015). *De publieke kern van het internet. Naar een buitenlands internetbeleid* [The public core of the internet. Towards a foreign internet policy]. Amsterdam University Press. https://english.wrr.nl/publications/reports/2015/10/01/the-public-core-of-the-internet

WRR [Netherlands Scientific Council for Government Policy]. (2017). *Veiligheid in een wereld van verbindingen* [Security in a connected world]. WRR. https://www.springer.com/gp/book/9783030376055