Chapter 1

Fighting Digital Fires

Suppose a ‘fire’ breaks out in the digital realm. Which fire brigade would we call? Do we sufficiently understand the vulnerabilities? What should we prioritize in our fire-fighting efforts? What powers do the authorities have to minimize the number of victims and to limit the damage? Are their powers commensurate for our digital world? These questions take on renewed urgency when the ‘fire’ in question is not limited to the digital domain but, left unchecked, has the ability to disrupt the ‘real world’ and undermine confidence in public institutions. Answering these questions inevitably leads to fundamental questions about the role of government, citizens and businesses. These themes are the subject of this report.

1.1 Incidents – Large and Small – Are a Fact of Life

Incidents involving our digital infrastructure are to be expected in our rapidly digitizing society.¹ Governments and other public and private organizations around the world are warning us about the risks. Indeed, various types of disruption have already occurred.² The problems can usually be resolved quickly, with the effects limited to inconvenience – these are the minor blazes. But in recent years, we have also witnessed incidents with much more serious consequences:

- In the Netherlands, the 2011 DigiNotar crisis was the first to reveal our dependence on digital technology.³ Hackers released forged certificates from the certification authority, compromising the reliability of all DigiNotar certificates, which browser providers such as Microsoft threatened to declare invalid. This

¹ Section 1.2 discusses terms such as *incident*, *disruption*, *disaster*, *societal disruption* and *digital disruption* in more detail.

² Clarke & Knake, 2019 ; Schneier, 2018; Greenberg, 2018.

³ Prins, 2011.

meant that important functions of government, such as customs clearance for goods and the payment of surcharges, could no longer be carried out. The incident was resolved but made headlines around the world by revealing the vulnerability and importance of private certification authorities for secure communication over the internet.⁴

- In 2016, a DDoS attack targeted the American company Dyn, a Domain Name System (DNS) provider.⁵ Internet platforms such as Twitter, Netflix and Reddit could not be accessed in the United States and Europe for most of the day. The attack was carried out with the Mirai botnet, consisting of compromised consumer devices such as webcams and digital video recorders. DNS providers translate web addresses into IP numbers, enabling computers to access websites. Some described the attack on Dyn as an attack on the internet itself.⁶
- In 2017, *WannaCry* – which at the time was assumed to be ransomware but has since been attributed to North Korea – infected the computers of Chinese universities, Spanish electricity and gas companies, the French car company Renault and the rail transport company Deutsche Bahn, among others. The most prominent victim was the UK's National Health Service. The services of around 600 healthcare institutions were disrupted, including the cancellation of about 19,000 patient appointments; some accident and emergency locations were unable to provide care to patients and had to be relocated. It took the NHS about 1 week to return to normal. Estimated cost: £92 million.
- Also in 2017, hackers working for the Russian military distributed the *NotPetya* ransomware by exploiting vulnerabilities in Ukrainian accounting software, which they had previously hacked. The virus affected companies and organizations worldwide, with reports of damage running into the billions. The Rotterdam division of the Maersk container company fell victim to the cross-border chain of contamination. Like many other ports worldwide, container transport ground to a halt. So did the surrounding rail links and highways, causing congestion and long traffic jams. In the Dutch town of Oss, the production of medicines by the pharmaceutical company MSD came to a stop. MSD also lost a great deal of documentation.
- In March 2018, the US city of Atlanta fell victim to a digital attack. Months later, many basic municipal services were still unavailable. The city lost tens of millions of dollars; numerous data files, including police files, were lost for good.⁷ Many other municipalities, corporations and public institutions such as universities have since fallen victim to similar ransomware attacks, often paying the attackers to restore their systems and retrieve lost information.

⁴Van der Meulen, 2013.

⁵https://en.wikipedia.org/wiki/2016_Dyn_cyberattack

⁶See WRR, 2015 for the importance of basic protocols such as DNS for the internet's functioning.

⁷<https://nakedsecurity.sophos.com/2018/06/08/atlanta-ransomware-attack-destroyed-years-of-police-dashcam-video/>

- Human error, broken servers, software issues and external factors such as cable breaks and power failures can also jeopardize the functioning of digital infrastructure. In June 2019, Google Cloud suffered outages due to regular maintenance work⁸ and could no longer support one-third of its own traffic. In the event of disruption, Google prioritizes the data traffic which should remain available. But the slowdown also affected Google's own capacity to recover, which led to a longer outage than would otherwise have been the case. Like Amazon Web Services in 2017, Google Cloud had already suffered an outage in 2018 due to a simple typing error.⁹ In all of these cases, the outages did not last for more than a few hours; it remains unclear whether large cloud providers could cope with longer outages. The effects of such disruptions will grow as more and more companies switch to cloud-based services and more societal processes come to depend on these providers.

The severity of these incidents continues to be debated. The global financial damage caused by *WannaCry* was enormous and human lives were endangered. The same was true of the *NotPetya* attack, the effects of which had similar cross-border patterns. But did these attacks truly disrupt society? Although the DigiNotar incident in the Netherlands revealed unforeseen problems, they were resolved. The record thus far has muddled efforts to place the threat of digital disruption on the political agenda and generally accept the seriousness and urgency of this problem. Nevertheless, we would be amiss to downplay the potential of such incidents or to imagine that a major disruption is unrealistic.

1.2 Disruptions at the Heart of Society

The potential scale of disruption has grown enormously in recent years. According to the OECD project 'Future Global Shocks' back in 2011, few cyber-related events had the potential to cause a global shock.¹⁰ But the authors were already pointing to the growing risk of financial damage due to compromised computers and telecommunications services. They also added that digital services would be essential for recovery operations following other types of large-scale disasters.¹¹ Almost a decade later, both observations have been proven prescient. Crisis management and disaster

⁸ See: [https://www.wired.com/story/google-cloud-outage-catch-22/?CNDID=53898727&CNDID=53898727&bxid=Mjc0Mzg0ODIwMDk5S0&hasha=100c13df07dc1abb3dd77f24de416e4d&hashb=c00c411b0670ffa64b106b13483864092cbfb5d4&mbid=nl_060819_daily_list1_p4&source=DAILY_NEWSLETTER&utm_brand=wired&utm_mailing=WIREDD%20NL%20060819%20\(1\)&utm_medium=email&utm_source=en](https://www.wired.com/story/google-cloud-outage-catch-22/?CNDID=53898727&CNDID=53898727&bxid=Mjc0Mzg0ODIwMDk5S0&hasha=100c13df07dc1abb3dd77f24de416e4d&hashb=c00c411b0670ffa64b106b13483864092cbfb5d4&mbid=nl_060819_daily_list1_p4&source=DAILY_NEWSLETTER&utm_brand=wired&utm_mailing=WIREDD%20NL%20060819%20(1)&utm_medium=email&utm_source=en). For Google's own report on the outage see: <https://status.cloud.google.com/incident/cloud-networking/19009>

⁹ See: <https://www.geekwire.com/2017/amazon-explains-massive-aws-outage-says-employee-error-took-servers-offline-promises-changes/>

¹⁰ Sommer & Brown, 2011.

¹¹ Cf. Prins, 2010.

relief today are unthinkable without digital tools, the Covid-19 crisis being a case in point. And the potential impact of incidents involving digital infrastructure has only grown: in geographical scope as well as how they affect real-world infrastructure and the daily lives of citizens.

Digital disruptions can now jeopardize the core processes of society. *WannaCry* caused parts of the UK's healthcare system to fail; DigiNotar threatened to disrupt the Dutch government's digital services and parts of the payment system; the hack in Atlanta led to the loss of important public data. In the meantime, we have already moved into the next phase: the taking out of facilities. In 2016, hackers infected a power station in Kiev with malware, knocking out one-fifth of the capital's power-generating capacity¹² – an incident that will go down in history as the first time malicious actors managed to remotely switch off a public utility. Things have only accelerated since then. In 2017, hackers succeeded in gaining control of software in US power plants.¹³ June 2019 saw media reports of disruptive malware that the US had placed in the Russian electricity grid.¹⁴

The costs for society are also rising. Lloyd's estimates the damage that would be caused by the failure of cloud services in the United States at 5 to 53 billion US dollars.¹⁵ The IMF reports that the potential damage to financial institutions caused by cyber-attacks could run into the hundreds of billions of dollars. These are estimates; there have been too few incidents to calculate potential damage with any degree of certainty. Nor is there consensus over what losses different types of incidents could generate.¹⁶ What is clear is that the potential for human victims and material damage is growing as society becomes ever more reliant on digital technologies. The US cyber expert Bruce Schneier explains:

With smart homes, attacks can mean property damage. With banks, they can mean economic chaos. With power plants they can mean blackouts. With waste treatment plants they can mean toxic spills. With cars, planes and medical devices, they can mean death. With terrorists and nation-states, the security of entire economies and nations could be at stake.¹⁷

Digital attacks have become an instrument of geopolitical conflict as the traditional struggle for control over land, sea and airspace has been extended to the digital realm.¹⁸ The struggle here is not about defining boundaries, but about sabotaging societal and economic processes and the strategic position of other countries. All in all, the question is no longer if – but *when* – we will need to deal with the consequences of a large-scale cyber-attack.

¹² Cf. Sanger, 2018, chapter 7.

¹³ <https://www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems/>

¹⁴ See <https://www.google.nl/amp/s/www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.amp.html> and <https://www.google.nl/amp/s/www.nytimes.com/2019/06/17/world/europe/russia-us-cyberwar-grid.amp.html>

¹⁵ Lloyd's & Cyence, 2017.

¹⁶ OECD, 2017.

¹⁷ Schneier, 2018: 16.

¹⁸ WRR, 2017.

1.3 There Is No Such Thing as 100% Security – But Are We Sufficiently Prepared for Disruption?

The growing scale, distribution and impact of incidents are partly due to the rapid pace at which the world is embracing digital technology.¹⁹ Digital technology is also becoming ever more complex with the exponential growth of data, computing power, and the exchange of data between devices, between people and devices, and between technology and the physical environment. We are now adding chips and sensors to almost everything, while everything is being connected to the internet. The next phase of this development – the ‘Internet of Things’ and artificial intelligence – will make all kinds of processes even faster and smarter. The result is that interaction between the digital world and the physical world is becoming ever more intense. In some sectors, the digital realm and the physical realm are already difficult to distinguish.

Alongside countries like Denmark, Estonia, Singapore, Finland, the US, Norway, the UK and Sweden, the Netherlands is at the forefront of the digital evolution. It has high connectivity, a digitally adept population, and highly digitized public services. Actively supported by the government, consumers and companies are embracing all kinds of digital activities. But every technological development has its flip side: advantages (the ‘highway to efficiency’) as well as disadvantages (the ‘highway to failure’).²⁰ Digitization is no exception.²¹ Digitization creates prosperity, individual freedom and convenience; countless nations are fully committed to these aspirations. But digitization also brings new vulnerabilities and dependencies,²² to the economy and core societal processes as well as to the safety of people and their property.²³ Although the stakes are presumably higher for highly digitized countries, countries lower on international indexes of digitization are not immune.

Many governments are well aware of society’s growing vulnerability to digital disruption.²⁴ The UK government expects that the country, measures notwithstanding, will suffer a major cyber-attack.²⁵ In Austria, there is discussion of a ‘Digitalen

¹⁹ Schwab, 2016.

²⁰ Turner, 1978; Perrow, 1983; Boin, 2017.

²¹ Pupillo, 2018: 1.

²² Schneier, 2018; World Economic Forum, 2017: 6; NCTV, 2018a, b: 5.

²³ Internet Society, 2017: 10.

²⁴ There has been no systematic international comparison of cyber security policies and institutions. See Van der Zwan and Spit (2015) for a cursory comparison of efforts to protect vital infrastructure; Janczewski and Caelli (2016) for the position of some smaller countries in cyber-attacks; Boeke (2016) for the role of the defence ministry in cyber-attacks in Denmark, the Netherlands, Estonia and the Czech Republic.

²⁵ For the British cyber strategy see: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

For parliamentary deliberations and reports: <https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/1708/1708.pdf>

Stillstand’ scenario caused by cascade effects.²⁶ The United States and France have developed systems of categorization for cyber incidents to determine the appropriate time to take direct action. The European Union has various initiatives to ensure that digital disruption can be adequately addressed.²⁷

All of these cyber-security measures aim to *prevent* major incidents. But there is no such thing as total information security – an inconvenient truth that is often forgotten. Whether inside or outside the digital domain, incidents can and will occur, leading to real-world disruption. Countries have contingency plans as well as legislation and regulation to deal with major disruptions due to natural and industrial disasters. But when it comes to cyber security, contingency planning has been much more limited. While many policy documents include sections on the possibility of serious disruption, their primary focus is achieving a higher level of protection or measures to reduce risks.²⁸ The scenario of major disruption thus serves to encourage people to take prevention more seriously. Only rarely are concrete measures set out for dealing with the consequences of incidents that do occur.²⁹

1.4 Structure of This Report

Cyber security and the prevention of digital disruption are not the focus of this report. We begin with the premise that we must face the real possibility of a scenario in which digital disruption leads to societal disruption. In short, we have to think about our response in concrete terms.³⁰ This report thus inquires: *How can government better prepare itself for societal disruption in a digitizing society?*

The report is structured as follows. Section 2 defines societal disruption to clarify the type of events we are addressing. Section 3 analyses how digitization is changing the context in which these events occur. Section 4 discusses the challenges that the government faces in terms of preparedness, detection, combating, and

²⁶ <http://www.darc-c12.de/system/files/Projektbericht-Digitaler-Stillstand-final.pdf>

²⁷ For example: <http://ec.europa.eu/transparency/regdoc/rep/3/2017/NL/C-2017-6100-F1-NL-MAIN-PART-1.PDF> and <http://ec.europa.eu/transparency/regdoc/rep/3/2017/NL/C-2017-6100-F1-NL-ANNEX-1-PART-1.PDF>

²⁸ Cyber security is defined in Dutch policy as ‘the entirety of measures to prevent damage due to the disruption, failure or misuse of information and communication technology and, where damage does occur, to rectify this’.

²⁹ An example is the letter from the Dutch State Secretary of the Interior and Kingdom Relations addressing information security in government. It states that ‘Citizens, businesspeople and other organizations must be able to continue to rely on the government, including in the digital age’ (Ministry of the Interior & Kingdom Relations, 2018: 6). Measures include ‘ensuring that important digital facilities of government are sufficiently able to withstand failure or outage.’ But except for the capacity to generally communicate about responses to incidents, the measures do not concern responding to incidents once they have happened.

³⁰ Cf. Prins, 2017.

recovering from major digital incidents. Section 5 presents our conclusions and recommendations.

We conclude that digitization has led to new forms of societal disruption and thus to a new set of tasks for government. Our recommendations concern policies regarding dependencies, critical infrastructure, competencies, priorities in combating the consequences of incidents, and compensation for victims, including the insurability of damages

References

- 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.
- Clarke, R.A. & Knake R.K. (2019). *The fifth domain. Defending our country, our companies, and ourselves in the age of cyber threats*. Penguin Press.
- 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/>
- Internet Society. (2017). *Global internet report 2017. Paths to our digital future*. <https://future.internetsociety.org/2017/wp-content/uploads/sites/3/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf>
- Janczewski, J., & Caelli, W. (Eds.). (2016). *Cyber conflicts and small states*. Ashgate.
- Lloyd's and Cyence. (2017). *Counting the cost: Cyber exposure decoded*. Lloyd's.
- Ministry of the Interior and Kingdom Relations. (2018, October 16). *Brief inzake verhogen informatieveiligheid bij de overheid* [Letter on increasing information security in the government]. Ministry of the Interior and Kingdom Relations.
- NCTV. (2018a). *Cybersecuritybeeld Nederland 2018* [Cyber security assessment Netherlands 2018]. NCTV.
- NCTV. (2018b). *Nationale veiligheid bij overnames en investeringen of inkoop en aanbesteding* [National security in take-overs and investments or service provision and tenders]. NCTV. https://www.nctv.nl/binaries/WEB_113154_NCTV_Veiligheid_bij_overnames_tcm31-334520.pdf
- OECD. (2017). *Enhancing the role of insurance in cyber risk management*. OECD.
- Perrow, C. (1983). The organizational context of human factors engineering. *Administrative Science Quarterly*, 28(4), 521–541.
- Prins, J. E. J. (2010). Digital tools: risks and opportunities for victims: Explorations in e-victimology. In J. van Dijk & R. Letschert (Eds.), *The new faces of victimhood. Studies in global justice*. Springer.
- Prins, J. E. J. (2011). Een hack bij DigiNotar [A hack at DigiNotar]. *Nederlands Juristenblad*, 86(30), 1585.
- Prins, J. E. J. (2017). Schadelijke beestjes [Damaging bugs]. *Nederlands Juristenblad*, 92(8), 507.
- Pupillo, L. (2018). EU cybersecurity and the paradox of progress. *CEPS Policy Insights 2018/06*.
- Sanger, D. A. (2018). *The perfect weapon: War, sabotage and fear in the cyber age*. Crown.
- Schneier, B. (2018). *Click here to kill everybody: Security and survival in a hyper-connected world*. W.W. Norton & Company.
- Schwab, K. (2016). *The fourth industrial revolution*. Crown.
- Sommer, P., & Brown, I. (2011). *Reducing systemic cybersecurity risk*. OECD.
- Turner, B. A. (1978). *Man-made disasters*. Wykeham.

- Van der Meulen, N. (2013). DigiNotar: Dissecting the first Dutch digital disaster. *Journal of Strategic Security*, 6(2), 44–58.
- Van der Zwan, E., & Spit, M. (2015). De internationale stand van zaken in de bescherming van vitale infrastructuur [The international state of affairs in protecting vital infrastructure]. *Magazine Nationale Veiligheid en Crisisbeheersing*, 3, 32–33.
- World Economic Forum. (2017). *The global risks report 2017*. <https://www.weforum.org/reports/the-global-risks-report-2017>
- 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://www.wrr.nl/publicaties/rapporten/2015/03/31/de-publieke-kern-van-het-internet>
- WRR [Netherlands Scientific Council for Government Policy]. (2017). *Veiligheid in een wereld van verbindingen* [Security in a connected world]. WRR. <https://www.wrr.nl/publicaties/rapporten/2017/05/10/veiligheid-in-een-wereld-van-verbindingen>

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

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