Chapter 2
Societal Disruption

2.1 Introduction

This section first explains the concept of 'societal disruption' to clarify what type of events we are addressing in this report. If events have a significant digital component, we speak of 'digital disruption'. Because societal disruption in policy practice is often linked to national security and 'critical assets', we also consider the classification of critical processes and critical infrastructure.

2.2 Societal Disruption

As societal disruption follows catastrophic events such as major floods or pandemics like Covid-19, it is intricately linked to the concept of risk. Risk is often defined in the literature as 'probability x consequence'.[1] Societal disruption concerns the consequences of that risk: the risk that damage will actually occur. While policy documents often refer to 'societal disruption', there is no clear definition of the term. Clearly, a major disaster would disrupt society. But it is more difficult to define a clear threshold as different types of events will differentially disrupt society, the market and government. Nor does disruption have to start at a clearly defined point. Like a smouldering peat fire, disruption may begin under the surface, its full extent only becoming apparent later. We explain the meaning and scope of the concept of societal disruption below by discussing: (1) 'normal' societal functioning; (2) the severity of disruption; (3) the role of perception; and (4) the duration of disruption.

[1] See WRR, 2008: 53–86 for an explanation of the 'classical' approach to risk.

E. Schrijvers et al., *Preparing for Digital Disruption*, Research for Policy,
https://doi.org/10.1007/978-3-030-77838-5_2

2.2.1 A Disruption of Everyday Life

Societal disruption implies the disruption of everyday societal processes. By 'everyday societal processes', we mean the regular functioning of the institutions of government, society and the market. If everyday societal processes can no longer function adequately – whether due to additional costs or inadequate public confidence – this counts as serious disruption, with consequences for society, economy and government, including justice, elections and the legislative process. We discuss the 'normal functioning' of society's institutions both in terms of verifiable damage to the continuity of society and people's perceptions of disruption.[2]

2.2.2 'Serious' Disruption: Failure of Core Processes

In the event of serious disruption, societal processes such as payments, the internet, public transport, healthcare, drinking water and electricity may stop functioning or switch to a less efficient mode. The continuity of society would no longer be guaranteed. Long traffic jams or queues could form, large quantities of goods could pile up, information and services could become inaccessible or unreliable, so that many everyday activities would no longer be possible. At this point, disruption would also lead to major economic damage. It may be direct damage, such as to flood defences, homes, computers and company installations, but also indirect damage due to business failures or the disruption of the activities of third parties. Finally, there may be physical casualties: human injuries and deaths.

2.2.3 Perceived Disruption

All of this can, in principle, be verified and quantified, and expressed in financial terms for compensation purposes, for instance. But alongside the material effects, there is also the risk that citizens lose confidence in the institutions of government, the market economy, or the society in which they live. Would they experience the disruption as an inconvenience or as a serious violation of their daily lives? The answer depends on people's value systems[3] as well as the extent of their self-reliance[4] during and after the disruption.

How people perceive the competence of private and public organizations, particularly that of the government, matters greatly. Did the government take adequate preventive measures? Was it able to take swift action to restore the normal

[2] Cf. PBL, 2014: 7–11.

[3] Douglas & Wildavski, 1982; Hood, 1998.

[4] Cf. WRR, 2017b.

functioning of society? If citizens, companies or organizations feel they can no longer rely on the continuity of normal societal functions, the foundations of the democratic constitutional state may be undermined. What makes digitization particularly problematic is the blurring of geographical boundaries; it may not always be in the power of national governments to quickly restore the normal functioning of society.[5]

The rule of law – which provides fundamental certainty in our society – is based on the premise that we live in a nation-state that can legitimately exercise a monopoly of violence within a clearly defined territory. If this principle is undermined, for example because the state can no longer successfully claim this monopoly, people may lose faith in society and the rule of law. In the event of serious digital disruption, it would also be unclear which resources the state can call on.[6] Such considerations would inevitably exacerbate the public perception of disruption.

Whether we are talking about an interruption to social services, economic damage, the number of victims, or the loss of confidence in society and government, these must reach a certain scale to merit the use of the term 'societal disruption'.

2.2.4 Duration of Disruption

A gradual, possibly unnoticed series of minor disruptions may have the same cumulative effect as an event that explodes onto our consciousness. In the former, the consequences of an event remain under the radar and only become clear gradually. The steady spread of disinformation, for example, undermines public confidence in institutions, which can harm the functioning of society over the long term. In the latter, cause and effect are largely indistinguishable; the seriousness of the situation is immediately obvious.

The passage of time is an important factor in the costs of disruption. Longer disruptions mean higher costs.[7] Ultimately, the adverse consequences of an event and assessments of damage will unfold over time.[8] More broadly, this also applies to the reputation of companies, organizations and governments. Inadequate detection systems and sluggish responses will impact the public's confidence in government, which by definition is expected to respond to serious situations swiftly and effectively.

[5] Bovens, 1998; WRR, 1998.

[6] Digitization poses anew what constitutes violence; it no longer only involves physical violence, but also new forms of 'digital violence'.

[7] Jocqué, 2016. For the costs of 'cyber breaches' relative to time of detection, see e.g. EPSC, 2017: 4.

[8] Lindenbergh & Hebly, 2016.

2.3 Critical Infrastructure and Critical Processes

Governments often view societal disruption through the lenses of national security and critical infrastructure. For the Dutch government, national security encompasses various 'critical' interests: territorial integrity, economic security, ecological security, physical security and social and political stability. The definition of national security has recently been extended to include 'other situations that (may) have a major impact on society'.[9] These include 'critical' processes that are so crucial that their failure or disruption would lead to immediate societal disruption or undermine national security. Together, these processes form the Netherlands' 'critical infrastructure'.[10]

Critical infrastructure denotes a range of services upon which society depends. Critical infrastructure must be protected from natural and technological disasters (e.g. floods and nuclear accidents). More recent understandings of critical infrastructure, however, transcend the traditional focus on national defence and military considerations. The focus of security policy has expanded beyond hostile actors, their capacity and motivations, to include the general vulnerabilities of society as a whole. Underlying this broader definition is the more diffuse spectrum of threats since the end of the Cold War, and new societal vulnerabilities due to our dependence on information systems.[11]

2.3.1 Critical Processes

The broader definition of critical infrastructure has led to a different approach to risk. In the absence of reliable data on the likelihood and impact of the risks society now faces, the focus has shifted from the potential causes to the potential consequences of the failure of processes critical to society's functioning. A classification of critical processes provides guidance for politicians, policymakers and other stakeholders to determine whether a particular situation should be considered serious – and thus whether the government should take action and, if so, how. After all, it is impossible to protect all societal functions against every possible threat all of the time, and we need to distinguish critical from non-critical processes. Assessments by the Dutch government have quantified the consequences of failure of each process as it bears on potential economic, physical and social harm. Consideration of

[9] NCTV, 2016: 8. These include 'a local or regional incident or accident with many casualties, an incident or accident abroad with a large number of Dutch casualties, or international events which affect the Netherlands'.

[10] See Parliamentary Papers II 2014/15, 30 821, no. 23 and Parliamentary Papers II 2015/16, 30 821, no. 32.

[11] Dunn Cavalty, 2007: 16; WRR, 2017a; Nationale Veiligheid Strategie 2019. [National Security Strategy 2019].

cascade effects resulted in two categories of critical processes, based on the seriousness of the impact of their failure.

The 'critical' nature of societal processes also depends on their organization and the risk of disruption.[12] This includes the presence of back-up options and recovery time – decisive factors for the extent of damage or the number of victims if things go wrong. Impact is not a fixed measure; it depends on the resilience of the actors responsible for the critical process in question.

Overviews of critical processes therefore differ, both over time and from country to country. Governments compile different lists or add new areas to reflect the latest threats. In 2017, the United States reclassified elections infrastructure as critical.[13] Germany includes the media and certain cultural goods.[14] While healthcare regularly features in international overviews of critical infrastructure, Dutch hospitals and other healthcare institutions have recently been dropped from the list.[15] As in the DigiNotar case, the critical importance of certain processes often only becomes clear after they suffer disruption. We will return to the implications of these national differences in the next section.

2.4 Digital Disruption

Digitization means that societal functions and processes are vulnerable in new and unexpected ways. This vulnerability applies to both regular processes and processes classified as critical by the government, since most critical processes are already bound up with digital infrastructure. By 'digital infrastructure', we mean all facilities for the storage, exchange and processing of digital data. Until about 10 years ago, the risk of the disruption or failure of these facilities was absent from almost all national and international risk analyses. This has changed over the past decade. The risk of the disruption or failure of digital infrastructure has risen rapidly through the ranking of risks that would have disruptive consequences for society.[16]

The disruption or failure of digital infrastructure can have many causes, from accidental (errors) or deliberate human actions (often of a criminal or at least unlawful nature) to the spontaneous failure of systems or the semi-autonomous behaviour of machines. There are also more indirect causes such as fires, power failures or floods that damage servers. These causes can occur separately or in combination and can result in both acute and gradual disruption. Where societal disruption has an important digital component, we refer to 'digital disruption'.

---

[12] Sharma, 2017: 33–36.

[13] https://fas.org/sgp/crs/misc/IF10677.pdf

[14] https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis.pdf?__blob=publicationFile&v=3

[15] https://zoek.officielebekendmakingen.nl/kst-27529-158.html

[16] The World Economic Forum scores the same risks each year, giving us an idea of how digital disruptions rank relative to other risks.

The scope of this report does not extend to the exact likelihood and consequences of digital disruption. Recent studies have already addressed these questions, both in the Netherlands[17] and abroad.[18] The potential of digital disruption leading to significant economic damage and social unrest is real, and is the premise of our analysis in the following sections. Our aim is to formulate an agenda for measures that could be taken to prepare society for such disruption, focusing specifically on what government can do.

2.5 Conclusion

We use the term 'societal disruption' to refer to serious disruptions to the regular functioning of society. What constitutes 'regular' societal functioning and 'serious' disruption will depend not only on the interruption of core processes in society but on the confidence that citizens, companies and public and private organizations have in them. The two feed into one another: a major disruptive event will inevitably undermine public confidence in society as well. At the same time, a series of smaller events may exacerbate the sense of threat and undermine confidence in the government, even if the event's actual significance is limited.

By identifying critical processes, the government seeks to set priorities and ensure that not all disruptions are classified as 'major'. This helps to direct scarce resources to where they can be used most effectively and legitimately. The list of critical processes is the result of an assessment of their importance and vulnerability to disruption and failure. That the disruption and failure of digital infrastructure can also have socially disruptive effects is now widely recognized. In the following sections, we use the concept of digital disruption to describe these effects.

References

ANV (Analistennetwerk Nationale Veiligheid) [National Security Analysts Network]. (2018). *Horizonscan Nationale Veiligheid 2018*. https://www.thehaguesecuritydelta.com/media/com_hsd/report/216/document/ANV-Horizonscan-Nationale-Veiligheid-2018.pdf

Bovens, M. A. P. (1998). *De digitale rechtstaat. Beschouwingen over informatiemaatschappij en rechtstaat* [The digital nation state. Reflections on the information society and the rule of law]. Samsom.

DeNardis, L. (2014). *The global war for internet governance*. Yale University Press.

Douglas, M. & Wildavski, A. (1982). *Risk and culture.* University of California Press.

[17] E.g. ANV, 2018: 22.

[18] E.g. World Economic Forum, 2017; Sommer & Brown, 2011; Lloyd's & Cyence, 2017. For the relationship between cyber security governance and national security, see DeNardis, 2014: 86, 104–106.

Dunn Cavalty, M. (2007). Critical information infrastructure: Vulnerabilities, threats and responses. *ICTs and International Security, 3*. https://www.peacepalacelibrary.nl/ebooks/files/UNIDIR_pdf-art2643.pdf

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

Hood, C. (1998). *The art of the state. Culture, rhetoric and public management*. Oxford University Press.

Jocqué, G. (2016, 2016). Tijdsverloop en schadevergoeding [Damage compensation over time]. *Tijdschrijft voor Privaatrecht*, (4), 1375–1434.

Lindenbergh, S. D., & Hebly, M. R. (2016). Schadebegroting en tijdsverloop. In *Preadviezen 2016* (pp. 301–361) http://hdl.handle.net/1765/95657

Lloyd's and Cyence. (2017). *Counting the cost: Cyber exposure decoded*. Lloyd's.

Ministerie van Justitie en Veiligheid [Ministry of Justice and Security]. (2019). *Strategie nationale veiligheid* [Strategy national security]. https://www.rijksoverheid.nl/documenten/rapporten/2019/06/07/tk-bijlage-nationale-strategie-2019

NCTV [National Coordinator for Security and Counterterrorism]. (2016). *Nationaal handboek crisisbesluitvorming* [National handbook for crisis decision making]. NCTV.

PBL (Netherlands Environmental Assessment Agency). (2014). *Maatschappelijke ontwrichting en overstromingen* [Societal disruption and flooding]. PBL.

Sharma, M. (2017). *Securing critical information infrastructure: Global perspectives and practices*. Institute for Defence Studies and Analyses. https://idsa.in/system/files/monograph/monograph60.pdf

Sommer, P., & Brown, I. (2011). *Reducing systemic cybersecurity risk*. OECD.

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]. (1998). *Staat zonder land: een verkenning van bestuurlijke gevolgen van informatie- en communicatietechnologie* [State without a nation: an exploration of the administrative consequences of Information and Communication Technology]. Sdu Uitgevers. https://www.wrr.nl/publicaties/rapporten/1998/03/09/staat-zonder-land-een-verkenning-van-bestuurlijke-gevolgen-van-informatie--en-communicatietechnologie

WRR [Netherlands Scientific Council for Government Policy]. (2008). *Onzekere veiligheid. Verantwoordelijkheden rond fysieke veiligheid* [Uncertain security. Responsibilities for physical safety]. Amsterdam University Press. https://www.wrr.nl/publicaties/rapporten/2008/10/01/onzekere-veiligheid

WRR [Netherlands Scientific Council for Government Policy]. (2017a). *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

WRR [Netherlands Scientific Council for Government Policy]. (2017b). *Weten is nog geen doen. Een realistisch perspectief op zelfredzaamheid* [Knowledge is not the same as action. A realistic perspective on self-reliance]. WRR. https://www.wrr.nl/publicaties/rapporten/2017/04/24/weten-is-nog-geen-doen