WRR

THE NETHERLANDS SCIENTIFIC COUNCIL FOR GOVERNMENT POLICY

Summary of WRR report

101

PREPARING FOR DIGITAL DISRUPTION

SUMMARY

Preparing for Digital Disruption

The Netherlands Scientific Council for Government Policy (or the WRR) was first established in 1972. It received formal legal status (Bulletin of Acts and Decrees 1976, 413) on 30 June 1976.
The Netherlands Scientific Council for Government Policy (the WRR) is an independent advisory body. The council informs and advises the Dutch government and parliament regarding cross-sectoral issues that have a major impact on our society. Its advice is based on scientific research and focuses on the long-term perspective.

The council's current term of office runs until 31 December 2022. It is composed of the following members:

Professor C.C.J.H. (Catrien) Bijleveld (as of 1-12-2019),
Professor A.W.A. (Arnoud) Boot,
Professor M.A.P. (Mark) Bovens,
Professor G.B.M. (Godfried) Engbersen,
Professor S.J.M.H. (Suzanne) Hulscher,
Professor J.E.J. (Corien) Prins (chairperson),
Professor M. (Marianne) de Visser,
Professor C.G. (Casper) de Vries,

Secretary: Professor F.W.A. (Frans) Brom.

The Netherlands Scientific Council for Government Policy
Buitenhof 34
PO Box 20004
2500 EA The Hague – The Netherlands
Telephone +31 (0)70-356 46 00
E-mail info@wrr.nl
Website www.wrr.nl/en

WRR

THE NETHERLANDS SCIENTIFIC COUNCIL FOR GOVERNMENT POLICY

Preparing for Digital Disruption

SUMMARY OF WRR REPORT 101

The Netherlands Scientific Council for Government Policy, The Hague 2019

Disclaimer
This publication is an English translation of the summary of WRR report 101: *Voorbereiden op digitale ontwrichting* (Preparing for Digital Disruption).
For a substantiation of the conclusions and recommendations presented in this publication, reference should be made to the detailed analysis of policy and scientific literature that can be found in the full version of the report.

Voorbereiden op digitale ontwrichting (Preparing for Digital Disruption) (ISBN 978-94-90186-77-7) was presented to the Dutch government by the council on 9 September 2019. The report can be downloaded free of charge as a PDF file from www.wrr.nl.

Translation: Taalcentrum VU
Cover and design: Xerox OBT, The Hague
Cover Image: Idee aan Zee, The Hague

The Netherlands Scientific Council for Government Policy, The Hague 2019

SUMMARY

Many provisions, crisis contingency plans and legal regulations are in place to deal with the possibility of incidents in the 'real world'. They are largely absent, however, in relation to incidents in the digital realm. This absence is becoming a concern now that digital disruption can have an increasing impact on the functioning of our society. Better preparations for the risk of digital disruption would enable the Netherlands to act more effectively in the event of disruption, and to recover more quickly following a serious incident.

INCIDENTS CAN HAVE A PROFOUND IMPACT ON OUR SOCIETY

In recent years, all manner of disruptions have occurred in the digital realm, both in the Netherlands and abroad. Most have been remedied swiftly and their impact was limited mainly to inconvenience. However, the consequences of some of those incidents have been much more serious. When computers in the UK's National Health Service were affected by the suspected ransomeware virus *WannaCry* (2017), 19,000 patient appointments had to be cancelled. In 2017, the *NotPetya* attack hit the Port of Rotterdam in the Netherlands, causing container transport through the port and its road and rail connections to grind to a halt. In the Dutch town of Oss, the pharmaceutical company MSD was also affected by this attack, with the production of medicines coming to a stop and the loss of a great deal of documentation. In 2018, the city of Atlanta in the US was hacked, and countless municipal basic services were unavailable for months. And in the early summer of 2019, an hour-long outage affected both the Dutch emergency number 112 and 0900-8844, the national police telephone line. In addition, hospitals, municipalities and companies could not be contacted for some time.

Although cyber attacks are an important cause of incidents, human error, broken servers, software issues or external factors such as cable breaks or power failures can also have a major impact on the functioning of digital infrastructure. The outage of the emergency number 112 mentioned above, but also the failure of Google Cloud – which also occurred in June 2019, provide striking illustrations of this.

The most concerning aspect of these incidents is that they affect critical processes in society. This means that they jeopardize essential services such as healthcare, payment traffic, government services and the electricity supply. Clearly, the potential economic and social cost of such incidents is rising. Although there have been too few incidents to be able to make an accurate prediction of these costs, we have seen already that they can run into the hundreds of millions of euros for individual organizations and companies. It is also clear that the potential for

material damage and victims is growing, as society becomes ever more reliant on digital technologies.

Finally, we also have to realize that attacks on and through digital infrastructures have become a commonly used tool in geopolitical conflicts. The traditional struggle for control over land, sea and airspace has been extended to include the digital realm. In this case, however, the struggle is not about defining boundaries, but about influencing processes and strategic positions in other countries. The question has long since moved on from whether such attacks can be prevented. The main issue now is what to do about them, whether counter-measures are appropriate and under what circumstances, and what an appropriate response to them should look like.

WE ARE INSUFFICIENTLY PREPARED

In recent years, there has been a growing awareness that the increasing use of digital technology implies the emergence of new and significant vulnerabilities for our society. However, it is striking that almost all cyber-security measures taken by the government and other major players are aimed at *preventing* incidents. This seems to be their primary objective. Though in reality, there is no such thing as total digital security, but this uncomfortable message has systematically faded into the background. Whether inside or outside the digital domain, incidents can and will occur and may lead to disruption. Today, a raft of provisions, crisis contingency plans and legal regulations are in place to deal with the possibility of incidents in the 'real world'. But when it comes to the area of cyber security, preparations for disruption have received much more limited attention. The analysis in this report shows that the government has insufficient resources to respond adequately, certainly in view of the fact that such disruption may have adverse consequences in the physical and social realms as well, even including public confidence in constitutional democracy itself.

DIGITAL DISRUPTION

As mentioned above, due to the growing interdependence of the digital realm, the physical realm and society as a whole, major outages or failures in digital processes are increasingly associated with disruption in wider society. The WRR refers to this type of disruption as 'digital societal disruption', or simply 'digital disruption'.

Digital disruption occurs when normal life is seriously and adversely affected. The growing interdependence of the digital and physical realms means that digital incidents can lead directly to disruption in society, with key societal systems and institutions being visibly impacted. This could potentially affect the efficiency of public transport, the internet, payment traffic or the electricity supply, even rendering them unable to function at all. At this point, disruption will often lead to major economic damage.

But quite apart from the material effects, there is also the risk that citizens may lose confidence in the institutions of government, the market economy and the society in which they live. The way in which people perceive disruption will depend on their own value system, how self-reliant they are or can be, and their expectations with regard to organizations, companies and – in particular – the government. Have these actors taken adequate preventive measures and would they be able to get society back on its feet quickly enough?

In relation to digital disruption, two aspects merit particular attention. To begin with, digital processes are largely invisible, which means that people's confidence in them is already precarious. If people suspect that something has gone wrong, this may be enough to undermine that confidence. Secondly, digitalization transcends geographical and political boundaries. It may not always be in the power of national governments to restore the normal functioning of society rapidly.

NEW CHALLENGES

Policymakers face a range of challenges when it comes to the risk of digital disruption:

- The physical and digital domains are now very closely intertwined. Developments such as 'datafication', the use of algorithms to make decisions and the complex web of connections between systems around the world mean that the physical realm now merges seamlessly with the digital realm. This necessitates careful policy preparation for digital disruption on the part of government; however, the current focus is still primarily on events in the physical domain. In this regard, special attention needs to be paid to critical infrastructures, the failure of which would lead to societal disruption.
- Digitalization means that society is vulnerable to new forms of disruption, due to unstable and often poorly secured software and hardware, and complex, cross-border supply and production chains, which create many opportunities for malicious actors to disrupt societal processes or even take them out entirely. The use of generic hardware and software means that such disruption could potentially have an enormous range and impact.
- Due to the policies of recent decades, many public facilities are now in the hands of private actors. Digitalization has further reinforced this trend, as companies, organizations and the government itself have outsourced the digital support of their activities to software suppliers and digital service providers. This means that the stability and continuity of society has become highly dependent on the actions of private actors, who in many cases are based abroad. The cooperation of these parties will be required should things go wrong, and in relation to measures to limit the impact of any incidents.

– Digitalization has made geographical and political boundaries less relevant. Numerous incidents have shown that problems can lead to disruption in several countries almost simultaneously. Digital disruption is therefore an issue that must be placed on the agenda of international bodies, including the European Union.

INVESTING IN PREPARATIONS FOR DIGITAL DISRUPTION

The risk of digital disruption can never be eliminated completely. This means that it is important to be ready for disruption, and this starts with ensuring preparedness and putting in place early-warning mechanisms that can tell us when things are going wrong. If an incident does result in disruption, adequate follow-up action is also vital. After all, recovery and reconstruction are key if society is to resume normal functioning as rapidly as possible.

Preparedness

Currently, a coherent policy is lacking regarding critical infrastructure with respect to back-up options, the isolation of chains and networks, cyber exercises, and information about how to respond to urgent incidents. Not only are different regulations in place for every sector and organization, there are also certain factors that actively undermine the preparedness of society. For example, the number of back-up options is being reduced as analogue alternatives are being abolished and organizations outsource important services to third parties. This is increasing the degree of interdependence between processes and sectors still further.

Signalling

The exchange of information is complicated because of an overemphasis on individual organizations rather than on production and supply chains and networks, sectoral dividing lines and a partly outdated distinction between so-called 'critical providers' and 'non-critical providers'. All this means that signals may not be received (or received too late) by the relevant actors. Partly as a result of this, the opportunities for pooling and sharing knowledge and information remain limited. The focus is currently on sharing knowledge and information regarding security measures, vulnerabilities and incidents. When it comes to chains and networks, the dependencies within them and the effect of takeovers and investments in new technologies, there is less clarity. This kind of knowledge is vital, however, if we want to be able to grade the severity of incidents and to manage the spread of digital disruption.

Responding to incidents

In combating digital disruption, the government is heavily reliant on information and cooperation from private actors (some of which are based abroad), but lacks any clearly defined authority to intervene. There are also questions about who

should take the lead, because it is often not immediately clear what the cause of an incident is. Greater powers for the government should be accompanied by adequate levels of protection for private parties, because where intervention is achieved through coercion there could be financial consequences for those actors. Moreover, greater clarity is needed about how upscaling would take place, in cases where the seriousness of incidents provides grounds for this. This presupposes a categorization of digital incidents, which is currently lacking in the Netherlands.

Recovery and the resumption of normal functioning

In the aftermath of a disruptive incident, a period of recovery and reconstruction will often be needed. In order to draw lessons from what has happened, a wide-ranging analysis is necessary. Partly as a consequence of new legislation, more attention is now being paid to the reporting of incidents. However, incident data is not always fully utilized, partly due to the fragmented way in which it is utilized by the various supervisory authorities. Financial compensation is also important but again this is problematic, partly due to the high level of uncertainty regarding both the risks and the type of costs that may be involved. In addition, large insurers are currently refusing to compensate for damages brought about by global cyber attacks, which they classify as 'armed conflict' or 'war'.

Responsibilities

Ensuring preparedness for digital disruption must consist of a combination of national measures and international cooperation and 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 extremely urgent, due to the geopolitical dynamic that surrounds digital disruption.

Greater involvement by the government is required at the national level. Some disruptions may be limited to the Netherlands. But global digital disruption would also ultimately affect key processes on Dutch territory. For a large number of measures, such as the deployment of back-up options, scenarios for switching off digital facilities and also financial compensation for material damages and insurance, the Netherlands can act independently to a large extent. Finally, it is vital that better preparation for digital disruption on the part of government is not perceived as a license for other parties to take irresponsible risks. If just one of them decides that preparatory measures are unnecessary, everyone will be affected if things go wrong.

RECOMMENDATIONS

The central message of this report is that preparations for digital disruption should become a stated goal of security policy and policies that aim to safeguard the continuity of our societal functions. The report expands on this central recommendation further in the form of the following more specific recommendations:

- Initiate a public debate about the preparedness of Dutch society in relation to the possibility of digital disruption.

- In addition to the existing Cyber-Security Assessment Report, prepare a Cyber-Dependency Assessment Report in order to provide a clearer picture of which parties, digital processes and services are key to the functioning of critical processes in Dutch society.

- When it comes to policy on critical infrastructure, focus more attention on the chains and networks that support key processes. Also investigate whether digitalization necessitates changes to the prioritization of assets that are essential for the functioning of a society and economy.

- Create a clearly defined legal mandate for a public institution that would take responsibility for combating digital disruption that could have an adverse effect on society. As part of this, examine the need for separate regulations with respect to governmental action that are designed to prevent incidents from escalating further. A categorization of incidents could play a useful role here.

- Encourage research into the feasibility of a Dutch or European 'cyberpool' in order to provide cover for financial damage caused by digital disruption.

- Ensure that information relating to incidents is better available at the national and European levels, make better use of that information and provide effective feedback to the parties involved in order to strengthen the capacity for collective learning.

PREPARING FOR DIGITAL DISRUPTION

Often without our even noticing it, digital infrastructure is closely intertwined with processes that are essential to our society, economy, democracy and the rule of law. The government and other key actors are not adequately prepared for failures or a complete break-down of this infrastructure.

For physical incidents, we have well-equipped emergency services. But who should we call if a 'digital fire' breaks out? What resources would a 'digital fire brigade' need to have at its disposal in order to extinguish that fire effectively? These questions are particularly important if the 'fire' in question is not limited to the digital domain, but also disrupts the physical world and/or undermines confidence in public institutions.

The Netherlands Scientific Council for Government Policy therefore recommends better preparation for what it refers to as 'digital disruption'. For instance, we need a clearer picture of dependencies, a new approach to critical infrastructure, adequate powers for government to prevent escalation and measures in the field of cyber insurance.

WRR

THE NETHERLANDS SCIENTIFIC COUNCIL FOR GOVERNMENT POLICY