Rathenau Instituut

Cyber resilience with new technology

An opportunity and a necessity

Report

Authors

Pieter van Boheemen1, Geert Munnichs1, Linda Kool1, Gijs Diercks1, Jurriën Hamer1 & Anouk Vos2

[1] Rathenau Instituut
[2] Radically Open Security B.V.

Photography

Maarten Hartman / Hollandse Hoogte

Preferred citation:

Rathenau Instituut (2020) Cyber resilience with new technology – An opportunity and a necessity . The Hague (authors: Van Boheemen, P., G. Munnichs, L. Kool, G. Diercks, J. Hamer & A. Vos)

Preface

Some people keep an entire chunk of their lives in the cloud. So do businesses and public authorities, which even store information that is vital to society there. This growing dependence on cloud providers, which are often foreign companies, creates new risks: loss of functionality due to system failures and loss of control of data and data processing. The changing nature of digital vulnerabilities makes it essential to invest constantly in cyber resilience. New digital developments such as machine learning and the rise of the quantum computer compel it.

This report, which has been written at the request of the Cyber Security Council and falls under the theme of Digital Society in our Work Programme, explores the opportunities that will be created by new technological developments in the near future and how they can be exploited to improve the cyber resilience of the Netherlands. For this report, we carried out a literature study, conducted interviews and organised workshops with experts, stakeholders and policymakers.

We discovered that cyber resilience is like the human immune system. It is impossible for the body to repel all of the attacks on it: the immune system deals with intruders and internal incidents or tries to control them. A healthy person who takes precautions will be more successful and for longer in that regard.

New technologies such as (again) machine learning, post-quantum cryptography, LiFi, 5G networks and distributed systems provide opportunities for enhancing cyber resilience. But so do many existing technologies that are not adequately exploited. The government can take the lead in promoting the use of these instruments, for example by widely employing strong forms of encryption and investing in the further development of machine learning and post-quantum cryptography.

The purpose of this report is to provide building blocks for an advisory report by the Dutch Cyber Security Council for the national government.

Melanie Peters

Director, Rathenau Institute

Summary

Introduction

The Dutch Cyber Security Council (CSR) is a national, independent advisory body for the government composed of high-ranking representatives from public and private sector organisations and the scientific community. The CSR promotes cyber resilience in the Netherlands. It asked the Rathenau Institute to investigate how new technologies can contribute to enhancing cyber resilience in the Netherlands. The aim of the study is to provide building blocks for an advisory report by the CSR for the national government.

The report covers:

- the anticipated technological developments in the Netherlands in the medium term (a period of 2-8 years);
- the implications of those developments for existing cyber vulnerabilities;
- the opportunities that these new technological possibilities create for increasing cyber resilience;
- the conditions that have to be met in order to take full advantage of those opportunities; and
- the lessons that can be drawn from experiences in other countries.

The report devotes special attention to public organisations and suppliers of vital services.

The study focuses on new technological developments.[1] However, the significance of technology depends on the practical use that society makes of its potential. This means that technological developments are shaped in part by various non-technical aspects, such as the cyber skills of users, organisational processes and legislation and regulation. This study into how the opportunities created by new technological developments can be grasped therefore concludes with a review of these wider conditions.

1 See appendix 1 for definitions of the technological terms used in this report. Those terms are marked with an asterisk (*) in this summary.

Relevant technological developments

This study concentrates on technological developments that are expected to have practical relevance for cyber resilience in the Netherlands in the coming years. It is not concerned solely with technological developments that are ‘new’ in an academic sense.

Two examples will illustrate this. The quantum computer* will not be sufficiently advanced for use in practice in the immediate future. However, its prospective arrival is relevant for this study because measures will have to be taken in the coming years to protect existing IT systems against the risk of an attack with a quantum computer. On the other hand, the Internet of Things (IoT)* is not a new technological development, but the explosive growth in its use in the coming years will force us to rethink how the Netherlands should address the vulnerabilities it creates. The further development of IoT is therefore relevant for this study.

Digitisation is making society vulnerable

This study also discusses the vulnerabilities associated with the digitisation of society. Measures designed to enhance cyber resilience cannot be considered in isolation from those vulnerabilities and the associated cyber threats.

With the further digitisation of society, the online and offline worlds are becoming increasingly entangled. Consequently, more and more data are processed digitally, more devices contain digital technology and more services are supplied digitally. The further roll-out of IoT will accelerate that trend. This is a problem due to widespread shortcomings in cyber resilience. Because of those flaws, IT systems and applications are frequently vulnerable to malfunctions, system failures and attacks.

Growing dependence on external parties

Another important trend with implications for cyber resilience is the growing dependence of end users on foreign technology companies for the proper functioning of digital products and services. For example, a growing number of digital services are supplied by providers of cloud technology*. This creates new risks: loss of functionality due to system failure and loss of control of data and data processing.

Large foreign companies are also in the vanguard when it comes to the further development and implementation of new technologies such as machine learning*, quantum computing* and satellite and 5G networks*. The Netherlands and the EU are therefore at risk of becoming even more heavily dependent on international parties.

Enhancing cyber resilience with new technology

New technologies like machine learning, post-quantum cryptography*, LiFi*, quantum communication*, 5G networks and distributed systems* offer possibilities for increasing cyber resilience. For example, machine learning will probably make it possible to automatically identify and repair vulnerabilities in software. And the aim of post-quantum cryptography is to enable data encryption that is resistant to attacks using the power of a quantum computer. These technologies are still being developed and are currently only used to a limited extent.

In fact, the use of automatic vulnerability detection and repair or post-quantum cryptography is not merely an opportunity, but also a necessity. To safeguard data security, for example, there will have to be a mass migration to post-quantum cryptography before quantum computers are capable of cracking existing forms of encryption*.

New technologies create new vulnerabilities

New technological advances also create new vulnerabilities. Machine learning makes it easier to carry out cyber attacks, for example, because existing vulnerabilities can be automatically discovered and exploited on a large scale. New technologies can also be a source of new vulnerabilities. Machine learning could be used to manipulate visual material (*deep fakes**), for example. Furthermore, new technologies themselves contain vulnerabilities. For example, machine learning is susceptible to data pollution; malicious parties could abuse this vulnerability by intentionally feeding a machine learning system with inaccurate data.

Increasing cyber resilience with existing technology

There is only limited point to using new technologies if existing technologies that are capable of enhancing cyber resilience are not used more widely. For example, there is still considerable room for improvement in terms of taking basic security measures (strong passwords, 2-factor authentication*), the use of encryption and of Privacy Enhancing Technologies (PETs)*, and the adoption of open data standards*, open source software* and safer communication protocols.

Conditions for exploiting technological opportunities

There are a number of conditions that have to be met in order to take advantage of the opportunities that new and existing technologies offer in terms of enhancing cyber resilience. First and foremost, measures to increase cyber resilience must be based on an adequate risk analysis, at board level, of an organisation’s critical data and processes: which ‘crown jewels’ demand maximum security and what risks are acceptable?

As a major client of digital products and services, the national government could also be an important role model, by making extensive use of PETs* for example. The government could also encourage suppliers to improve the security of the digital products and services they bring on to the market through legislation, certification and standardisation. The Dutch government – or the EU – should be conspicuously involved in the drafting of international standards, which are very important for multinational measures in the domain of cyber resilience.

Strengthening digital autonomy

There are various options for countering the risks associated with the growing dependence on foreign technology companies.

1. The standard use of tools such as strong encryption, open data standards and distributed systems could avert risks such as unauthorised access to data, vendor lock-in* and Single Points of Failure*.
2. A second option is to incorporate stricter requirements in the purchasing conditions in contracts with suppliers of digital products and services. For example, providers of cloud services could be required to encrypt all stored data in order to prevent unauthorised access. The national government and providers of vital services could – and indeed must – play a leading role in this respect.
3. A third option for escaping over-dependence on foreign parties is for the Netherlands and Europe to create a larger IT industry of their own.

Improving the innovation climate

That third option requires a more effective knowledge and innovation policy, with a sharper focus in the government's Netherlands Cyber Security Research Agenda (NCSRA). A more favourable innovation climate is also needed. The government could, for example, make tender procedures more attractive for innovative start-ups. The government and the suppliers of vital services could also play a stronger role as launching customer. The Netherlands' prominent position in terms of knowledge in the field of post-quantum cryptography also creates opportunities for the launch of national IT companies, which could then develop products and services to support the migration to quantum-resistant cryptography.

Another reason for developing a national IT industry on at least a minimum scale is the need to guarantee maximum security for 'crown jewels' such as state and commercial secrets, for example by using strong forms of post-quantum cryptography. The government and suppliers of vital services must be able to buy the necessary products and services from trusted market actors that endorse important values such as privacy and autonomy.

Exploiting opportunities for post-quantum cryptography and machine learning

The government could promote the use of new technologies such as machine learning and post-quantum cryptography in various ways. That will require continued investment in knowledge creation in those domains. The government should also facilitate collaboration between research institutes and organisations devoted to finding innovative solutions for issues relating to cyber resilience. Organisations that do not have their own research capacity and which rely on the products and services supplied by market parties should be able to request assistance in evaluating whether an offer from a commercial supplier is suitable.

Expertise required for successful use of new technology

Exploiting the opportunities for increasing cyber resilience created by new and existing technologies calls for specific capacity and expertise. Due to the chronic shortage of experts in this field, greater investment is needed in programmes for teaching IT skills.

Contents

Preface 3

Summary 5

Introduction 13

1.1 The goal and the questions to be answered 13

1.2 The research method 14

1.3 Observations about the research process 15

1.4 Scope 15

1.5 Overview of the technologies discussed 18

1.6 Reader's guide 21

2 Digitisation makes society vulnerable 22

2.1 Growing digital connectivity creates vulnerability 22

2.1.1 The internet of everything 23

2.1.2 The growth of digitally available data 24

2.1.3 Low level of basic security 24

2.1.4 Chain dependence 25

2.1.5 Developments in the area of cybercrime 25

2.2 New technologies create new vulnerabilities 26

2.2.1 Artificial intelligence and *machine learning* 26

2.2.2 Quantum computer as game changer 29

2.3 Growing dependence on external parties 30

2.3.1 Cloud services 30

2.3.2 5G and satellite networks 32

2.3.3 The Netherlands and the EU are falling further behind 33

3 Increasing cyber resilience with new technology 34

3.1 Defensive use of machine learning 34

3.1.1 Automatic mapping of IT networks 34
3.1.2 Automatic investigation and repair of vulnerabilities 35
3.1.3 Automatic detection of malfunctions, system failures and attacks 36
3.1.4 Automatic response to attacks 37
3.2 Machine learning against deepfakes 38
3.3 Resilient communication networks 39
3.3.1 Advantages of 5G networks 39
3.3.2 LiFi offers benefits in specific situations 40
3.3.3 Quantum communication detects tapping 41
3.4 Distributed systems to prevent Single Points of Failure 42
3.5 Post-quantum cryptography 42

4 Increasing cyber resilience with existing technology 45
4.1 Basic security measures 45
4.2 Biometrics 46
4.3 Privacy Enhancing Technologies 46
4.4 Encryption 47
4.5 Digital signature to combat deepfakes 48
4.6 Permanent attention for cyber resilience 49
4.6.1 SecDevOps for an integrated design process 49
4.6.2 Safer supply chains 50
4.6.3 Safer communication protocols 51
4.7 Open data standards and open source software 52

5 Conditions for taking advantage of technological opportunities 54
5.1 Cyber resilience starts with a risk analysis 54
5.2 The government as role model 55
5.3 Legislation and regulation 57
5.3.1 Open statutory standards and regulation 57
5.3.2 Certification 58

5.3.3 International standardisation 59
5.4 Strengthening digital autonomy 61
5.4.1 Strengthening digital autonomy with technology 62
5.4.2 Strengthening digital autonomy with stricter purchasing conditions 62
5.4.3 Strengthening digital autonomy with a domestic IT industry 64
5.5 Post-quantum cryptography creates opportunities for IT enterprises 68
5.6 Exploiting the potential of post-quantum cryptography and machine learning 69
5.7 Successful use of new technology depends on the available expertise 71

6 Conclusions 72
6.1 Opportunities for new technology 72
6.2 Potential of existing technology 73
6.3 The Netherlands and Europe are falling behind 73
6.4 Options for strengthening digital autonomy 74
6.5 Promoting a domestic IT industry 74
6.6 Conditions for exploiting opportunities 75

Bibliography 77

Appendix 1: Glossary of terms 91

Appendix 2: Participants interviews 94

Appendix 3: Participants workshops 96

Introduction

The digital society is a vulnerable society. Digital products and applications can be hacked, disrupted or manipulated in numerous ways. Data can be stolen or falsified, computers can be operated surreptitiously, disinformation can be spread and the failure of IT systems can cause social disruption. From telephones to cars and from financial transactions to patients' medical files: they are all increasingly being digitised and that trend is accompanied by digital vulnerabilities.

New digital developments, such as machine learning, the steadily expanding use of cloud services and the emergence of the quantum computer, deepen those vulnerabilities. Through the use of deep fakes, for example, disinformation can have a disruptive effect on the democratic process of public news reporting and opinion shaping. The growing importance of suppliers of cloud services could also lead to users becoming more dependent on those suppliers, with all the ensuing security risks.

However, the new developments also create opportunities. With machine learning, vulnerabilities can be detected sooner and repaired more easily. With cloud services, the security of digital systems is in the hands of professionals. Distributed systems can reduce the risk of large-scale system failures.

This study explores the significance of technological developments in the short term and how they can be exploited to improve the cyber resilience of Dutch society.

1.1 The goal and the questions to be answered

This report arises from a request by the Dutch Cyber Security Council (CSR) for the Rathenau Institute to investigate how new technologies could help to enhance cyber resilience in the Netherlands. The CSR is a national, independent advisory body for the national government composed of high-ranking representatives from public and private sector organisations and the scientific community. The CSR promotes cyber security in the Netherlands. The aim of the study is to provide building blocks for an advisory report by the CSR for the national government.

The central question addressed in the study is this: how can new technologies help to enhance cyber resilience in the Netherlands, with special reference to public and private organisations that constitute part of the country's vital infrastructure?

To answer this question, we address the following specific issues:

- What technological developments await us in the medium term (the next two to eight years)?
- What are the implications of those technological developments for existing cyber vulnerabilities and threats and the current state of cyber resilience?
- What opportunities do the new technological possibilities offer for increasing cyber resilience?
- What conditions have to be met in order to exploit those opportunities?
- To what extent are the public and private organisations that make up the vital infrastructure anticipating and exploiting new technological opportunities?
- What lessons can be learned from experiences in other countries? What relevant developments are occurring in the EU?

1.2 The research method

This report is based on desk research, interviews and three workshops. The main findings from the desk research and the interviews were discussed during the workshops, which were held on 31 January, 21 February and 17 June 2019. Prior to each of the workshops, the participants received a briefing paper with a review of the results of the desk research, the interviews and the preceding workshops. Following the workshops, further desk research was carried out into a number of specific subjects and some additional interviews were conducted.

The participants in the interviews and the workshops were experts, stakeholders and policymakers. Some of the persons we interviewed also participated in the workshops. In this report, we refer to them as 'the experts we consulted '. No distinction is made between the interviewees and the participants in the workshops. They were selected on the basis of their expertise and their engagement with various specific issues addressed in the study. The names of the interviewees and the participants in the workshops can be found in Appendices 2 and 3.

This report describes the findings from the desk research, the interviews and the workshops and presents the conclusions drawn from those findings. Progress with the research was discussed on several occasions with the secretariat of the Cyber Security Council and with members of the Council's New Technologies Sub-Committee.

1.3 Observations about the research process

The question posed in the study compels us to look ahead to the opportunities that new technologies will create in the area of cyber resilience in the coming years. In the course of the research we found that the question did not speak for itself. Particularly during the interviews, the respondents appeared to have some difficulty in properly spotlighting the question addressed in the study. Many of the experts who were interviewed initially gave reactions such as: cyber resilience is more an organisational than a technological issue; without a clear understanding of the cyber threats, there is little point in looking for opportunities; and as long as many organisations fail to take basic security measures, there is little point in looking for new technological solutions.

Nevertheless, the experts we consulted were later willing to mention new possibilities that could benefit cyber resilience in the near future. This initially produced a wide range of suggestions without any clear prioritisation or ranking. One reason for this was a difference of opinion about what falls under the term 'new technology'. Whereas some interpreted 'new' in a more academic sense, with the emphasis on ground-breaking research, others felt the term had a more practical meaning and that the primary focus should be on potential new applications.

The three workshops played an important role in interpreting and structuring the varied findings from the desk research and the interviews. The final result is a report with the following scope.

1.4 Scope

To define the scope of the study, it was necessary to clearly understand what we meant by the term 'new technology'. That definition would also make it possible to distinguish between 'new' technological developments that were or were not relevant for the study. This section describes how we ultimately defined the scope of the study.

New technology

The question posed in this study concerns the implications of new technological developments for current practice in efforts to make Dutch society cyber resilient and how that practice could benefit from those developments. The significance of the technological developments is therefore considered in relation to their relevance for existing practice moving forward. Accordingly, this study is not concerned solely with technological developments that are ground-breaking in an academic sense.

The role of technology

In that context, it has to be remembered that technology can never be considered in isolation. It only acquires significance from the way in which a society exploits a technology's potential. In this case, the latter means all of the efforts made by consumers, businesses and public authorities to make Dutch society cyber resilient. It also means that technological developments are shaped in part by various non-technological aspects, such as the cyber skills of users, the organisational processes of businesses and public authorities, and legislation and regulation.[2] It is not without reason that this study also reviews the conditions that have to be met if the opportunities created by new technological developments are to be exploited.

Relevant technological developments

Relating the significance of new technology to its relevance in practice also makes it possible to define which technological developments should or should not be covered in this study.

This aspect can be illustrated with the example of the quantum computer. The development of the quantum computer is not expected to have advanced far enough for it to be used successfully in practice within the next eight years. However, the anticipated arrival of the quantum computer in the more distant future means that measures will already have to be taken in the coming years to protect IT systems against the risk of a hack which exploits the processing power of a quantum computer. Accordingly, the potential consequences of a still futuristic scenario – the use of the quantum computer – are relevant for cyber resilience in the shorter term.

On the other hand, the Internet of Things is not a new technological development (Gabbai, 2015), but the enormous expansion it is expected to make in the coming years forces us to reconsider how we should deal with its vulnerabilities. The further development of the Internet of Things is therefore relevant for this study.

2 See also the Cybersecurity Capacity Maturity Model (CMM) of the University of Oxford's Global Cyber Security Capacity Centre (2016). *Cybersecurity Capacity Maturity Model for Nations (CMM) - Revised Edition. Oxford.*

Quantum computer as the sole *new* technology

As the example of the Internet of Things shows, a number of the technological advances discussed in this study are expansions of earlier developments. That applies for the use of cloud technology, for example, which is no longer devoted primarily to data storage, but is increasingly also used to provide services. The quantum computer is the main exception in this study: in many respects it is the only technological development that deserves the label ‘new’. It is not only ground-breaking in an academic sense, but will probably radically transform existing practice.

Further selection of technological developments

This study does not provide a complete overview of new technological developments, but is confined to a selection of those that are most relevant for answering the question of how cyber resilience can be improved. The two following examples will explain the considerations underlying the selection of technologies.

First, we do not discuss developments in the area of blockchain. We regard blockchain as a derivative application that exploits the possibilities created by encryption and distributed systems. Those two, more basic technologies are discussed.

Second, for similar reasons we do not discuss developments in the domain of user environments and other interaction technology, such as wearables, digital voice assistants and Virtual Reality. The report does discuss the technologies that are relevant for the resilience of the systems underlying this interaction technology. In the case of digital voice assistants like Siri, Alexa and Google Assistant, these are technologies such as machine learning and Privacy Enhancing Technologies.

Section 1.5 contains an overview of the technologies discussed in this report.

Cyber resilience

In this report, we use the term cyber resilience rather than cyber security. Cyber resilience is a relatively new concept. It bears a certain similarity to the term cyber security and the terms are often used interchangeably. Cyber security generally refers to preventing damage caused by system failure or the disruption or abuse of IT. The damage may be caused intentionally (by a cyber attack, for example), unintentionally (by errors in a software update, for example) or through human error, or by a combination of these factors. The term cyber security evokes associations with the metaphor of the fort, which must be impenetrable to attacks and disruption from outside.

Cyber resilience refers not only to preventing damage, but also to the capacity to repel an attack and repair any damage (Ministry of Security and Justice, 2013). It is a more dynamic concept and reflects the fact that the objective is not absolute security (ENISA, 2017), since there is no such thing as absolute security (Rathenau Instituut, 2017). The main priority is that continuity of service can be guaranteed if an attack does take place or damage occurs (Björck et al., 2015; IT Governance UK, 2019). Cyber resilience can be compared with the human immune system (Wlodarczak, 2017). Like a human body, digital systems are not hermetically sealed. The immune system is also not capable of fending off every external attack. The immune system deals with intruders or endeavours to keep them under control.

The use of the term cyber resilience reflects a growing awareness that the internet is an unsafe environment and that it is impossible to build a hermetically sealed fort. It is therefore more important to be able to prevent attacks and disruptions as far as possible, and to be able to identify them, contain them and recover from them when they do occur. Nevertheless, the basic defences – 'the fort' – still have to be as strong as possible.

Resilience and vulnerability

To enhance cyber resilience, it is important to have a clear understanding of the vulnerabilities of IT-related products, services and systems. Measures designed to improve cyber resilience cannot be seen in isolation from those vulnerabilities and the associated cyber threats. In this study we therefore also review the vulnerabilities connected with new and existing technological developments in the digital domain.

Cyber threats come from both attacks by malevolent parties such as cyber criminals and from system failures and malfunctions. In this study, the nature and scale of existing cyber threats that have already been identified in various reports are assumed to be known (Rathenau Instituut, 2017; ITU, 2017; Europol, 2018; McAfee, 2018; NCTV, 2019a).

1.5 Overview of the technologies discussed

On the basis of the findings from the desk research, the interviews and the workshops and the above description of the scope of the study, we selected the following technologies to discuss. We make a distinction between (relatively) new technologies – which are not widely applied or are still being developed – and

technologies that have existed and been used for some time. See Table 1 for the list.[3]

3 See appendix 1 for a more detailed description of these technologies.

Table 1 List of the technologies discussed

New technology	**Potential to increase cyber resilience**
Machine learning	• Automatic monitoring of complex IT systems • Automatic detection of vulnerabilities, malfunctions, system failures and attacks • Automatic response to incidents • Automatic detection of deep fake videos
Post-quantum cryptography	• Quantum computer-resistant data encryption
Quantum communication	• Safer communication through detection of eavesdropping
5G networks	• Safer and more reliable data traffic • Future-proof authentication
LiFi	• Safer communication over short distances by means of light signals
Distributed systems	• Decentralised architecture for IT systems reduces the risk of large-scale system failure
Existing technology	**Potential to increase cyber resilience**
Basic security measures	• Increased resilience against (automated) attacks
Cloud technology	• Increased resilience by virtue of professional cloud services
Privacy Enhancing Technologies	• Containment of spread of (personal) data • Containment of damage from data leaks and theft
Encryption	• Encryption of data

Secure multi-party computation	• Data sharing without complete transparency
Digital signature	• Combating disinformation • Safer supply chains
SecDevOps	• Cyber resilience is built into the design process for digital products and services
Safer communication protocols	• Increase in basic resilience of the internet
Open standards and open source software	• Reduced risk of dependence through *vendor lock-in*

1.6 Reader's guide

The following chapters describe the findings from the research. The chapters are organised in roughly the same order as the sub-questions addressed in the study as listed earlier in the report. Chapter 2 describes the vulnerabilities associated with the further digitisation of society and the new vulnerabilities arising from recent technological developments. Chapter 3 outlines the opportunities that new technologies create for enhancing cyber resilience. Chapter 4 summarises the opportunities created by existing but underutilised technologies. Chapter 5 describes the conditions that need to be met if public organisations and suppliers of vital services are to be able to take advantage of these opportunities for increasing cyber resilience. There is also a discussion of relevant experiences in other countries. Chapter 6 presents the main conclusions of the study.

2 Digitisation makes society vulnerable

As already mentioned in the opening chapter, the measures needed to enhance cyber resilience cannot be seen in isolation from the vulnerabilities of IT-related products, services and systems. Accordingly, to increase cyber resilience it is necessary to know what those vulnerabilities are.

This chapter describes the vulnerabilities associated with the progressive digitisation of society. It also shows how new technological developments such as machine learning and the growing use of cloud services could increase those vulnerabilities or create new vulnerabilities. New technologies could themselves also be a source of new vulnerabilities. For example, the use of machine learning is susceptible to the risk of data manipulation.

2.1 Growing digital connectivity creates vulnerability

The last several decades have seen the progressive digitisation of society, with the online and offline worlds becoming increasingly entwined. More and more data are stored digitally, more and more devices contain digital technology and more and more services are provided digitally. Developments such as the roll-out of the Internet of Things are accelerating this trend. Because of its ever-expanding scale, this phenomenon is now even referred to as ‘the internet of everything’.

With the advancing digitisation of society, there are also more and more digital targets that malicious parties can attack, as well as more and more digital products and services that are susceptible to system failure, breakdown and disruption. This creates various security risks, which can increasingly also have physical consequences. Think of the digital operation of locks or the emergence of smart homes or self-driving cars. The digital manipulation of locks or the braking systems in self-driving cars could cause serious physical damage.

Despite the growing awareness of the risks associated with the digitisation of society, the state of cyber resilience is often dreadful. For example, organisations often fail to take even basic security measures.

The growing integration of digital and other processes is also creating a deeper interdependence between organisations within a chain. Vulnerabilities in one organisation can therefore have consequences for the cyber resilience of others.

In this section we discuss these aspects in more detail, as well as developments in the area of cybercrime.

2.1.1 The internet of everything

The internet has grown enormously since the 1990s. More devices are being connected to the internet all the time, together forming an Internet of Things. In 2018, there were seventeen billion devices connected to the internet worldwide: ten billion smartphones, tablets, laptops and PCs and seven billion other devices such as smart thermostats, digital implants such as pacemakers or insulin pumps, and cars. The number of devices connected to the Internet of Things will probably at least double in the next five years (Lueth, 2018).

5G networks will facilitate the further roll-out of the Internet of Things. 5G stands for the fifth generation of wireless or mobile systems. These networks can transmit data in larger quantities and with less delay. They could improve the functionality of many digital applications, for example by transmitting information to self-driving cars more quickly.

It is important to note that digital applications and devices can also communicate with each other. A self-driving car can only plot its route if it constantly receives the correct information, for instance. Accidents will happen if a satellite or a sensor along the road provides inaccurate information. The interconnection of digital devices could also increase the risk of manipulation, disruption and system failure.

The energy sector faces a similar risk. The increase in decentralised energy generation and the growing demand for energy-intensive charging points for electric vehicles make digital management of the energy network indispensable. That creates new risks, such as disruptions to supply and power cuts (Council for the Environment and Infrastructure, 2018).

In a nutshell, an ‘internet of everything’ has been created in which countless products and services are connected digitally and are vulnerable to attack, malfunction and system failure.

2.1.2 The growth of digitally available data

The growth of the digital society is accompanied by massive data collections. Rijkswaterstaat uses an extensive network of sensors to monitor water levels; search engines on internet monitor the surfing behaviour of users; and the volume of data saved by new cars or by their manufacturers is far greater than in the case of cars that are ten years old (Automotive Insiders, 2018). Businesses, public authorities and other organisations amass steadily larger quantities of data about clients on the principle that more data leads to a better understanding of the individual and hence to products and services that are better matched to their personal needs. The commercial value of all that information, for advertisers for example, makes it is possible to offer digital products and services free of charge to users (Zuboff, 2019).

Collecting all these data is not without risk. Massive datasets have regularly been leaked in recent years. Examples include the leaking of the personal data of 500 million guests of Marriott hotels (Ortiz, 2018), of 150 million users of the MyFitnessPal app (Flinkle & Balu, 2018) and of 87 million Facebook users (Lapowsky, 2018). These leaks underline the vulnerability of central databases and the risk of ever larger data collections. They can be exploited by cyber criminals and other malicious parties, for example by using leaked data to blackmail a target or to manipulate reporting. The more data people place online, the greater the chance of that data being accessed or abused for improper purposes.

2.1.3 Low level of basic security

The growing level of internet connectivity is problematic from the perspective of cyber resilience because even relatively straightforward basic security measures are often not taken. Suppliers often provide digital devices and services with poor or inadequate security and fail to provide updates (Bulletproof, 2019). They usually have no economic incentive to invest in cyber resilience. The price competition on products is intense and the user does not ask for safer products (Rathenau Instituut, 2017).

Users also often fail to take adequate measures to secure their products and services, for example using weak passwords, not making back-ups of important files and putting off the implementation of software updates (Van der Grient & Konings, 2018).

This creates serious security risks, since the manipulation or disruption of digital devices can have serious repercussions. Devices connected to the internet can

also be used to carry out a cyber attack. For example, they could be hacked and incorporated into a botnet that is used for a massive DDoS attack (Hilton, 2016).

2.1.4 Chain dependence

A growing number of IT systems and applications are connected to one another. Organisations often buy network-based products or services from external suppliers. These can be software, hardware, data storage or cloud services. No organisation is capable any longer of performing all of its tasks entirely alone. The vulnerability created by this dependence on other parties is often underestimated. After all, the weakest link in the chain can cause disruptions in functions further up the chain (Rathenau Instituut, 2017). One example that is often used to illustrate the vulnerability of supply chains is the anecdote of the hackers who were able to penetrate the systems of a casino via its aquarium's operating system (Schiffer, 2017).

This chain dependence means that the various social and economic sectors are also more closely interconnected. The cyber resilience of the energy or transport sector, for example, increasingly depends on the resilience of other parties in the chain. The distinction that is often made between 'vital sectors' and other sectors is therefore becoming more difficult to sustain. The National Coordinator for Security and Counterterrorism (NCTV) now uses the terms 'vital infrastructure', 'vital processes' and 'vital suppliers' instead (NCTV, 2018).

2.1.5 Developments in the area of cybercrime

The progressive digitisation of society creates various opportunities for criminals and efforts to counter them are failing to keep pace. Cybercrime not only often pays, cyber criminals often have little cause to fear repercussions. Investigation and prosecution are a problem because attacks are often difficult to trace to a specific individual or organisation. Even if a criminal activity is interrupted, the offenders can generally try again somewhere else or using another method. The threat from cybercrime will not diminish as long as there is little chance of the offenders being caught and prosecuted.

Moreover, cybercrime is becoming increasingly easy to commit. There is a growing market in cybercrime-as-a-service: it is becoming so easy to buy cyber attacks and computers that have been taken over by criminals on underground marketplaces that the buyer no longer needs personal expertise to carry out an attack (McAfee, 2018).

On top of that, there is specialisation among cyber criminals, with some focusing on spam mail and others concentrating on exploiting vulnerabilities, for example. Finally, virtual currencies like Bitcoin can play into the hands of cyber criminals because with these currencies they can trade and launder financial assets anonymously (CipherTrace, 2018).

2.2 New technologies create new vulnerabilities

This section describes how the use of new technologies could create new digital vulnerabilities or exacerbate existing vulnerabilities. For example, machine learning facilitates cyber attacks because it allows existing vulnerabilities to be exploited automatically and on a massive scale. The use of machine learning therefore deepens the risks connected with existing vulnerabilities.

New technologies can also be a source of new vulnerabilities in themselves. With the quantum computer, it will in future be possible to crack existing forms of encryption, so that existing defensive measures that use them will become redundant from one day to the next. The use of machine learning also creates a new vulnerability because the data on the basis of which it works can be manipulated.

2.2.1 Artificial intelligence and *machine learning*

The emergence of artificial intelligence (AI) creates new vulnerabilities. In this section we briefly explain what we mean by AI and machine learning.

AI is not new. The technological concept was already being explored by scientists, mathematicians and philosophers in the 1950s. AI refers to the building of systems that display a certain degree of intelligent behaviour (European Commission, 2019b). It encompasses a number of techniques.

A basic AI technique is *rule-based AI*. This method essentially involves programming a series of ‘if this, then that’ instructions. An example is a computer that issues a warning if the operating program is shutting down and some documents are still open. This is usually no longer regarded as artificial intelligence because we have become accustomed to this ‘intelligent’ and independent behaviour by computer systems.

Machine learning is more advanced than rule-based AI. It works on the basis of data rather than prior instructions. Machine learning centres on detecting patterns in existing data so that similar patterns can be recognised in new data. The technology relies heavily on statistics.

Deep learning is a specific form of machine learning. It is based on neural networks – inspired by the biology of the brain – and combines different layers of information. A deep learning algorithm for facial recognition can contain three layers, for example. The first layer examines an image for contrast and colours. A second layer combines that information and searches for features such as edges or shadows. The third layer checks whether it can recognise specific features such as a nose, lips or eyes (Rathenau Instituut, 2019c).

The increase in computing power and the large volumes of available data have greatly accelerated the development of machine learning and deep learning in the last two decades. It is these forms of AI that attract a lot of attention in the current public and political debate. There is also growing interest in the possibilities they offer in terms of cyber resilience, in both an offensive and a defensive sense. In the remainder of this report we make no distinction between machine learning and deep learning and use the former term.

There are various ways in which machine learning can be used to exploit vulnerabilities in digital systems. Machine learning itself is also vulnerable, because the data that feed the algorithms can be intentionally contaminated (Brundage et al., 2018). The possibilities are briefly discussed below.

Increasing the attack surface

Machine learning makes it easier to carry out cyber attacks. The technology allows vulnerabilities in systems that are inadequately protected and devices connected to the Internet of Things to be identified automatically and on a large scale, and to be exploited. Malevolent parties can take advantage of that.

Manipulation of reporting

Machine learning can also be used to manipulate text and audio and visual material. These creations have become increasingly convincing and more difficult to distinguish from authentic information in recent years (Brundage et al. 2018). The technology has bona fide applications. For example, the dubbing of the sound in foreign films can be matched to changes in the image to give a more natural overall effect for the viewer.

But machine learning can also be used to make deepfake videos, in which words are put into a person's mouth. It is also possible to generate a moving image from a portrait photo (Mehta, 2019). In such a manipulated clip, the voice and the movements of the individual concerned are barely distinguishable from the real thing. Deepfake videos can be used to spread disinformation and mislead citizens, for example by showing prominent politicians making statements that they never actually made (Verhagen, 2019). In 2018, for example, a Flemish political party distributed a video purporting to show US President Donald Trump calling on Belgium to renounce the Paris climate agreement (sp.a, 2018).

The technology is also becoming easier to use. In June 2019, researchers presented a method of automatically adding a transcript to video fragments, whereupon the user only has to revise the text to generate a new video in which the new text is spoken in a natural manner by the person in the video (Fried et al., 2019). In publishing their results, the researchers appealed for the technology to be used responsibly, but it could of course be abused. It was for this reason that the OpenAI consortium had earlier decided not to publish details of a technology that automatically generates written news reports because of their concerns for the impact on news reporting (OpenAI, 2019).

Fake accounts on social media (bots) can promote the spread of manipulated information by repeatedly sharing or 'liking' them (Rathenau Instituut, 2018b). One of the ways that disinformation can have a major impact on public news coverage and public opinion and, by extension, disrupt society, is through its mass dissemination on social media.

The greater possibilities of using machine learning to manipulate text, audio and visual materials underlines the growing importance of data integrity for society.

Data manipulation

There is another way in which machine learning has implications for data integrity. Because machine learning works on the basis of data-fed algorithms, the quality of the outcomes of machine learning depends on the quality of those data. However, data can contain bias and therefore unintentionally or unconsciously influence the results of applications of machine learning.

Malicious parties can abuse this vulnerability by intentionally feeding machine learning systems with incorrect data (*data poisoning*). Attackers who know how a machine learning system has been trained can subtly manipulate the results, for example by presenting a facial recognition algorithm with photos that have been

manipulated with ‘noise’. The human eye still sees the same image, but the facial recognition algorithm can be misled. This could cause applications for making medical diagnoses to arrive at incorrect conclusions on the basis of scans that have been contaminated with noise (Finlayson et al., 2018). Stickers on a road can also lead the Lane Detection System of one particular Tesla model to believe that there is a diversion and cause the car to change lanes, while a human driver would simply ignore the stickers (Ackerman, 2019).

2.2.2 Quantum computer as game changer

The arrival of the quantum computer will probably have enormous significance for cyber resilience. Quantum computer is the term used for a computer that uses physical phenomena such as superposition, entanglement and interference: these are fundamentally different physical phenomena than those used in existing computer chips. The expectation is that these features will enable the quantum computer to solve some mathematical problems more quickly. This has consequences for the ability to crack existing methods of digital encryption. Today’s commonly used encryption methods will not be able to withstand the computing power of the quantum computer. It is therefore also expected that a quantum computer will be able to gain access to secured data and penetrate secured networks more easily.

The development of quantum technology is still in its infancy, however. As far as is known, no functional quantum computer has yet been produced. It is also impossible to predict when that will be accomplished, because further scientific breakthroughs are needed to translate the insights from physics into practically useful chips and it is unclear how long it will take to achieve them. Experts estimate that a usable quantum computer is very unlikely to be developed within the next ten years (Committee on Technical Assessment of the Feasibility and Implications of Quantum Computing et al., 2019). Some estimates are that it could take at least 20 to 30 years. However, it is likely that once those breakthroughs have been made, the quantum technology will quickly come onto the market and the capacity to crack existing encryption will rapidly spread.

A number of the experts we consulted questioned the wisdom of waiting for the breakthroughs in quantum technology. Because of the time and expense involved in migrating to forms of quantum-resistant encryption, they feel that organisations should start preparing now. They also point out that malevolent parties could employ what is known as a ‘harvest and decrypt’ strategy, where they already collect (encrypted) data now in order to decipher them later. The revelation of certain sensitive data could conceivably still be harmful even after thirty years, medical data or commercial secrets for example.

2.3 Growing dependence on external parties

Another way in which new vulnerabilities are appearing is connected with changes in relationships of dependence and the associated risks. Consumers, businesses and public authorities increasingly rely on external, often foreign, parties to ensure the proper functioning of the digital products and services they use. For example, a growing number of digital services are provided by a small number of cloud providers, which means that the end user depends for many of its functions on the quality, continuity and reliability of the service provided.

The dependence on external parties is a global phenomenon. The scale of business activity in the field of IT and cyber resilience in the Netherlands and the EU is limited. For example, the Netherlands depends on a number of large foreign technology companies for the construction of 5G networks, which raises questions about the associated risks in terms of cyber resilience.

There is also a growing geopolitical dimension to the dependence of the Netherlands and the EU on external parties. The Netherlands and EU play scarcely any role in global discussions relating to IT, including developments in the area of machine learning and the quantum computer. The question is whether the Netherlands and the EU are now falling too far behind and conceding power in this domain.

The risks associated with the shifting relationships of dependence are discussed in more detail below.

2.3.1 Cloud services

It is repeatedly found that many end users lack the necessary expertise and capacity to ensure that the cyber resilience of their IT systems and devices is in order. As mentioned above, even relatively straightforward basic security measures are often not implemented properly. This applies for individuals, businesses and public authorities. Consequently, measures to enhance cyber resilience are increasingly outsourced to external parties by means of cloud services.

This approach has significant benefits because cloud suppliers generally possess greater expertise and capacity to safeguard data and processes than end users. There is also considerable demand for these types of service. In a recent survey of chief technology officers (CTOs), for example, 80% of the respondents said they

could not fully guarantee their own organisation's cyber resilience (Elumalai et al., 2018).

Outsourcing measures relating to cyber resilience is part of the broader trend that the cloud is no longer used solely to store data, but increasingly also to provide a range of services. These include not only the sale of software as-a-service and various forms of data processing that occur in the cloud. It can go so far that the principal function of a computer is to connect the monitor, the keyboard and the mouse to a cloud service that runs all the programs (*desktop-as-a-service*). This trend is expected to continue in the coming years.

The downside of outsourcing responsibilities to cloud suppliers is that it creates new risks: loss of functionality in the event of a disruption and loss of control of data and data processing.

Loss of functionality

When data processing programs are no longer running on an organisation's own computers but are doing their work in the cloud, disruption of the cloud service leads to a loss of functionality. This risk might affect one specific task, but also a number of tasks simultaneously. If more than one task is outsourced to the same cloud supplier and the cloud service is disrupted or does not work properly, the result can be a Single Point of Failure. An example is a computer system in which so many programs are running externally that the system barely functions without cloud computing services. Furthermore, there is often a great temptation to delegate a variety of tasks to the same supplier. This is connected with the fact that the market in cloud computing services is dominated by a small number of players, including Amazon, Microsoft and IBM (Dignan, 2018).

It is important to stress the gravity of this risk: if, for example, a government department or a network manager uses the cloud for many of its processes, the service it provides depends entirely on the stability of the cloud service. The research firm Gartner referred to the serious risks associated with the use of cloud services in its Emerging Risk Report in 2018 (Morris, 2018).

Loss of control

A second risk arising from the use of cloud services is the loss of control of data and data processing. The more data that is stored and processed in the cloud, the more important the question becomes of the extent to which the cloud supplier can access and reuse the data, share them with other parties or alter the method of processing them without the consent of the end user. These actions affect the autonomy of the end user, who is no longer able to determine who can do what with the data.

Vendor lock-in

The increasing use of cloud services is not always a free choice of the end user. Suppliers increasingly compel users to opt for a cloud service by halting the supply of the product that can run on the user's own computers. The migration costs connected with switching to an alternative supplier are an important factor in that context. The users are, as it were, 'locked in' by the supplier (*vendor lock-in*).

2.3.2 5G and satellite networks

The growing dependence on external parties also extends to the construction of 5G and satellite networks.

5G networks

Only a small number of companies possess the expertise to construct and maintain 5G networks. Huawei, Nokia, Ericsson, Cisco and ZTE control 90% of the market for network equipment (Dell'Oro Group, 2019). The use of equipment from market leader Huawei is the subject of heated debate because of concerns that the company might secretly intercept data transmitted over the network and share it with the Chinese government (Kaska et al., 2019).

There are also worries about the quality of Huawei's network. The Huawei Cyber Security Evaluation Centre (HCSEC) in the UK recently reported serious flaws that represent a threat to British national security. According to the Centre, Huawei fails to take basic measures, such as updating software elements with known vulnerabilities. Since the HCSEC had already referred to these shortcomings on a previous occasion (HCSEC, 2019), the report also shows that the bodies responsible for exercising oversight of the construction of the 5G networks are not yet capable of guaranteeing the desired level of security and enforcing improvement.

It is important, however, not to target criticism exclusively at Huawei. Given the scale and complexity of 5G technology, it is very difficult, not to say practically impossible, for every supplier to show that their equipment does not contain covertly installed vulnerabilities (Lysne, 2018). Regardless of the supplier and the measures that users take to mitigate risks, security therefore remains partly a question of trust. The home country of the supplier is a factor in that respect, for example by virtue of the country's regulatory regime (Kleinhans, 2019).

Satellite networks

Satellite networks are also expected to start playing a larger role in internet traffic in the near future. Various companies, including Starlink and OneWeb, are planning to launch large numbers of satellites with which broadband internet can be provided worldwide (*mega satellite constellations*). Networks dedicated to connecting devices to the Internet of Things are already available from companies such as Iridium (McLean, 2019) and the Dutch firm Hiber (Blotenburg, 2018). The fact that the American Federal Communications Commission has granted a radio licence to Starlink for 2,200 satellites (Boyle, 2018) and to OneWeb for 720 satellites (Henry, 2018) gives an impression of the likely size of the future networks. The Chinese firm LaserFleet also started constructing a broadband internet network in 2018 (Jones, 2018). If these satellite networks are able to compete with national networks in future, it will probably lead to the Netherlands becoming more dependent on foreign parties with respect to the control of these communication networks.

2.3.3 The Netherlands and the EU are falling further behind

Countries like the United States and China and those countries' large technology companies lead the way in terms of investment in the development of artificial intelligence/machine learning and the quantum computer. That statement is backed up by figures from the OECD. Private investment in artificial intelligence in Europe is five times lower than in the US. The fact that China registers patents on more than 500 inventions relating to quantum computing every year, while the figure for Europe is just several dozen, points in the same direction (EPSC, 2019).

The Netherlands and EU are therefore at risk of falling further behind and becoming even more dependent on external, foreign parties (European Commission, 2018). Despite investments in research into quantum technology recently announced by the EU, it is highly questionable whether any European party will ultimately succeed in bringing a quantum computer onto the market.

A similar story applies for the development of business activity in the area of cyber resilience in the EU. Normalised for Gross Domestic Product (GDP), the EU occupies ninth position in the global ranking of cyber security companies, after Israel, the United States, New Zealand, Canada, Switzerland, Singapore, Hong Kong and India. Three-quarters of the most innovative cyber security companies are from the United States, while only one in ten is from the EU. This is attributed in part to the fragmented regulation within the EU and to the absence of standards (STOA, 2017).

3 Increasing cyber resilience with new technology

This chapter describes how the use of new technologies could eliminate new and existing vulnerabilities and so create opportunities for increasing cyber resilience. In this chapter we discuss the potential of machine learning, resilient communication networks such as 5G networks, LiFi, quantum communication, distributed systems and post-quantum cryptography.

3.1 Defensive use of machine learning

Machine learning is expected to become very important for enhancing cyber resilience in the near future by virtue of its capacity to automatically detect and repair vulnerabilities. Machine learning could also help in maintaining oversight of complex IT networks. The high expectations for the use of these defensive forms of machine learning are underscored in the National Cyber Security Research Agenda. In this section, we briefly discuss four defensive uses of machine learning.

3.1.1 Automatic mapping of IT networks

It is becoming increasingly difficult for organisations to maintain an overview of their entire network – not just the physical devices and computers, but also the various applications, data and digital services that function on them. The expectation is that organisations will increasingly use automated systems to map and monitor their network. Monitoring the composition of the network is particularly important in sectors where it regularly changes, for example the networks of education and care institutions where people often use their own devices and connect them to the system (*bring your own device*). With machine learning, it should possible for system administrators to detect previously unknown network elements.

If an incident occurs, network administrators must be able to quickly identify the elements of the network that have been affected and need to be repaired. Automatic monitoring systems can help in that. A clear overview of the organisation’s network and the mutual dependencies of the various sub-systems is also essential for the use of automatic response systems. Without that overview, it would be irresponsible to allow a response system to switch a network element on or off.

3.1.2 Automatic investigation and repair of vulnerabilities

The capacity to identify and repair vulnerabilities in software manually is rapidly approaching its limits. Errors that can cause vulnerabilities inevitably slip into the code when computer programs are being written. Advanced computer programs can easily contain millions of lines of code, making it practically impossible to find and repair errors manually. Machine learning is expected to make it possible to identify and repair vulnerabilities (*automatic bug fixing*).

It is also likely that human action will no longer be sufficient to defend against large-scale, high-speed attacks and new types of attacks with previously unknown characteristics. Automatic detection and response with the help of machine learning could provide a solution.

But the development of algorithms that automatically repair vulnerabilities is still in the experimental phase. A high-profile example of the efforts that are being made is Project Mayhem, the winner of a competition organised by the American Defence Advanced Research Projects Agency (DARPA) to develop automatic programs that can detect and repair vulnerabilities (Fraze, 2017). During a DEFCON conference, Mayhem was found to perform better than humans in that regard. The team behind Mayhem gave the following reason for its success: “What machines (currently) lack in creativity, they make up for in speed, tenacity and scale. Mayhem analyzes thousands of programs in parallel in a few hours, a task that would take a human many years of tedious work. Mayhem can find thousands of bugs and previously unknown vulnerabilities in a day running on the cloud. In the time it takes an expert to open up a file, an automated system may have looked at hundreds.”[4] Project Mayhem is confined to recognising known vulnerabilities. For the time being, it will still be up to humans to detect new, unknown vulnerabilities. Accordingly, there will still be a need for cyber security experts who can identify these types of vulnerabilities.

Automatic repair of bugs in software touches on the Software Directive

There are also doubts about the legality of automatically repairing vulnerabilities in software. The Directive on the legal protection of computer programs, also known as the Computer Programs Directive, provides that users must have the owner’s consent before they can modify software. Article 5 of the directive contains an exception for actions that are necessary for the use of the program by the user, including the correction of errors. However, the exception does not extend to the dissemination of improved software, which raises the question of whether automatic repair of vulnerabilities is compatible with the terms of the directive.

4 See https://forallsecure.com/blog/

3.1.3 Automatic detection of malfunctions, system failures and attacks

Whatever measures are taken to enhance resilience, incidents will continue to occur in digital systems. Detecting and remedying incidents is therefore very important. New technological measures also offer possibilities in that regard.

Many large organisations cluster their cyber resilience activities in a security operation centre (SOC). For the automatic detection of malfunctions, system failures and attacks, SOCs can be equipped with Security Information and Event Management (SIEM) technology. The use of this technology is expected to grow strongly in the coming years (TechNavio, 2017). SIEM technology could also assist system administrators in detecting and classifying incident reports. Machine learning could help administrators to make better assessments of reports. Research by Verizon showed that 70% of technical reports of data leaks go unnoticed by system administrators (Verizon, 2018).

Because of the high operational costs involved, SOCs are regularly shared by several organisations. Because the quality of an SOC increases in line with the volume of information it has about possible threats, the sharing of information is an important requirement for the successful functioning of an SOC. A number of organisations within the national government, such as the Tax and Customs Administration and Rijkswaterstaat, have their own SOC (Court of Audit, 2019a). The national government's various SOCs have also marshalled their strengths in a Joint-SOC (SSC-ICT, 2019).

Automatic detection of incidents is not flawless, however. An employee will regularly have to check whether irregularities found by the system are actually incidents and assess their nature and seriousness. Particularly in the case of targeted, advanced attacks, human assessment and intervention will still be necessary to prevent attackers from causing serious damage. Knowledgeable cyber security experts will therefore be needed as badly as ever.

Nor is it only large organisations that can use technology for monitoring and detection. There are numerous products on the market that use similar technology for the home and for SMEs. Slatman IT, for example, is a company that has developed an app that provides users with information about the behaviour of the devices in their (home) network, including security risks. The Dutch company Dyne offers a similar service with Dowse, which is being developed in an open source project with a subsidy from the SIDN Fund (SIDN-fonds, 2018). At present, the

additional workload this type of product imposes on the user is an obstacle to its widespread use by SMEs and consumers.

Behavioural analytics

Machine learning has in fact been used for some time for relatively simple forms of detection. For example, it can be used to automatically analyse the behaviour of users in digital systems (*behavioural analytics*). With machine learning, unusual behaviour can be recognised on a large scale. Banks have been using this approach for years to identify and block unusual transactions with bank cards. Behavioural analytics is also increasing the possibilities for identifying individual users on the basis of personal characteristics such as typing speed and mouse movements. This technology could therefore complement other authentication technologies. For example, users who have access to an organisation's financial records but do not normally use the authorisation could be asked for additional identification when they do. Experts believe that these features could make a major contribution to enhancing cyber resilience (Hill, 2017).

3.1.4 Automatic response to attacks

As soon as it becomes clear that an incident in a digital system is causing damage, a rapid response is essential. In light of the growing scale on which incidents occur, automation could also be a solution in that respect. For example, attackers can use networks consisting of large numbers of infected devices, as many as hundreds of thousands as in the case of the Mirai botnet (Fruhlinger, 2018). In practice, it is impossible to respond manually to such a massive attack.

Technologies that could provide an answer to such attacks are usually based on classical defensive strategies. For example, attackers could be distracted to keep them busy and give the defenders an opportunity to find the attacker's weak spot (*honey pot*). Attacks could also be fended off or averted by digitally changing the route to the target. Another option is to switch off or decouple the part of the system targeted by the attack temporarily (*containment*). Given the speed with which attacks can take place, the automation of these types of defensive strategy is expected to increase further in the coming years.

Sometimes, the most effective way of fending off an attack is to disable the offensive weapons or the attacker. Automatic offensive technologies are therefore emerging. However, organisations that use these methods are bordering on what is legally permissible (Higgins, 2017). The Dutch Computer Crime Act deems infiltration of computer systems without the owner's consent to be hacking. Hacking instruments of attack is permitted once they have entered the target's network. In practice, however, the limits of what is permitted are difficult to define because

internal and external systems are becoming ever more closely entwined. There is also a fear that offensive technologies could lead to a dangerous escalation of attacks and counterattacks (Higgins, 2017). In light of these problems, these processes are still likely to require human action.

These restrictions apply to a lesser extent for the intelligence and security services, which are authorised to use offensive technologies. However, the Intelligence and Security Services Act does impose restrictions on the use of an automatic response system. For example, the use of tapping powers must be ‘as targeted as possible’.

3.2 Machine learning against deepfakes

In addition to automatic identification and repair of vulnerabilities and automatic response to attacks, machine learning could be used to counter manipulated visual material (*deepfakes*) and prevent its dissemination.

There are already a number of tools to counter deepfakes. For example, DARPA’s MediFor system calculates a score for the integrity of news reports on the basis of a range of features. The system searches for evidence of manipulation of images and videos, for example by analysing lighting (the illumination of faces, the reflection from lamps) and by comparing the weather conditions in a photo with the records for the weather at that location at the relevant time. Machine learning is also used to detect fake accounts and automatic bots that send bulk mailings on social media, for example with Botometer (Karatas, 2017).

The detection of deepfakes is also likely to end in a contest. As soon as machine learning systems are used to detect manipulated images, attackers will endeavour to adapt the systems for manipulating visual and video material accordingly.

The effectiveness of the use of technology to detect manipulated reports depends on the timing of its use. Once disinformation has been spread, it is difficult to negate its effects. Since the aim of social media platforms like Twitter, Snapchat and Facebook is to spread information as quickly as possible, it is questionable how much scope there is for preventive filtering. Other media platforms, such as online news sites, are more likely to start using deepfake detection systems.

3.3 Resilient communication networks

An important aspect of cyber resilience is the availability, reliability and security of data transmission via communication networks. Various new technological developments are occurring in this domain, including the emergence of 5G networks, LiFi, satellite networks and quantum communication. Each of these developments creates opportunities to improve cyber resilience. Because we assume that the Netherlands will not build any major satellite networks of its own within the next eight years, we will not discuss that technological development here.

3.3.1 Advantages of 5G networks

In addition to faster connection to the network and greater data capacity, 5G also increases the possibilities for improving the availability, reliability and security of data traffic (Shafi, 2017; Norrman et al., 2018). This section focuses mainly on some differences between 5G and 4G networks. 5G communication technology is in fact the collective term used for a variety of methods of connectivity, some of which are still under development.[5]

5G provides Ultra-Reliable Low Latency Communication (URLLC), which is intended to ensure that data in critical systems can be transmitted without error and with a minimum of delay. For example, 5G devices can switch from one antenna to another more quickly, thus increasing the reliability of the transmission of information to mobile devices. This is important for self-driving cars or remote control of surgical robots, for example.

An important distinguishing feature compared with 4G is that with 5G data streams can be separated (*network slicing*). This makes it possible to determine more precisely who has access to what data, for example. Network slicing also opens the door to new business models. Suppliers could provide services with differentiation in terms of the volume of data, the speed of transmission, the speed of connection and the reliability. End users would be able to make different choices according to the level of cyber resilience they require. With 5G, communication within a network can also be encrypted more effectively.

Another difference between 5G and 4G is the transition to virtual SIM cards. A physical SIM card is no longer required with 5G. Network operators can instead

5 In particular, the standards are currently being developed. A large number of organisations are involved in this process, including the 3rd Generation Partnership Project (3GPP), the Internet Engineering Task Force (IETF), the GSM Association (GSMA), the European Telecommunications Standards Institute (ETSI) working group and the Open Network Automation Platform (ONAP).

choose their own authentication method based on software certificates, token cards or other codes. New methods could be added later to the 5G Authentication and Key Agreement (5G AKA). The 5G network is therefore more future-proof. On the other hand, the absence of a physical element in the authentication process might diminish its reliability.

The intention is that 5G will also incorporate new measures against interception, including the prevention of IMSI-*catching,* a method whereby an attacker intercepts traffic by adding an additional transmission tower to the network. In 5G networks, fake transmission towers can be excluded because the transmission towers have to authenticate themselves to each other. However, recent research has shown that even 5G is vulnerable to IMSI-catching (Whittaker, 2019). But as already mentioned, 5G technology is still evolving and it is therefore entirely possible that this vulnerability will have been remedied by the time the technology is being widely used.

Finally, there is a lot of discussion about the possible existence of ‘back doors’ in the equipment or software of suppliers for 5G networks. In that context, it is important to realise that, in the interests of combating crime and terrorism, the Dutch Telecommunications Act obliges telecom providers to implement measures that allow their services to be tapped (*lawful interception)*. However, built-in functions that allow communication to be tapped can also be exploited by attackers.

All in all, it is almost impossible to say in advance whether the potential of 5G will actually lead to communication networks that are more resilient than 4G networks. That remains to be seen in practice.

3.3.2 LiFi offers benefits in specific situations

LiFi is a technology that uses light to transfer data between devices. The data is transmitted by switching LED lights on and off very rapidly, with a frequency that is invisible to the human eye. The technology is already marketed by the firm PureLifi.

There are certain circumstances in which LiFi communication is particularly promising. The technology could be a solution in situations where the interception of radio signals has to be prevented. With LiFi, data can be transmitted over very short distances: because light cannot pass through walls, the signal is contained within a space. In contrast to radio signals, light can also travel long distances under water. Lifi might also be an option in planes and other environments where

electromagnetic interference is a risk. There was a lot of interest in the applications of the technology in aviation at the annual LiFi conference.[6]

In a report in 2018, the Radiocommunications Agency Netherlands referred to other advantages of LiFi. LiFi is seen as a possible alternative to the commonly used WiFi, which is susceptible to disruption at locations where many WiFi networks converge, for example in cities and at busy locations. However, the agency warned that there is no universal standard for LiFi communication yet and therefore no agreement on the appropriate form of authentication and encryption. From the perspective of cyber resilience, it is important for these aspects to be regulated in a standard before the technology becomes widely used (Van der Gaast et al., 2018).

3.3.3 Quantum communication detects tapping

With quantum technology, information can be transmitted between two locations without being covertly intercepted. This is because the laws of physics state that the mere observation of a quantum object inevitably causes a change in the signal. The sender can therefore immediately halt the transmission if it is being intercepted.

There have been systems that use quantum communication on the market for more than ten years. One firm that sells such systems is ID Quantique, whose systems use fibre optic connections stretching up to several hundred kilometres. In 2017, Chinese scientists reported that they had succeeded in transmitting information over a distance of more than 1,200 kilometres with a quantum communication satellite (Liao et al., 2017). In the Netherlands, a quantum communication network is being built between the cities of Amsterdam, Delft, Leiden and The Hague. A European consortium has also been formed to build a quantum communication network covering seven European countries, including the Netherlands. This latter initiative is still in the planning phase (DG CONNECT, 2019b).

Major drawbacks of quantum communication systems are their costs and dimensions. A quantum communication system is not yet small enough to fit in smart phones or Internet of Things devices. For the time being, the use of quantum communication is limited to industrial and government organisations which have to minimise the risk of their communication being intercepted.

6 See https://lificongress.com/

3.4 Distributed systems to prevent Single Points of Failure

Distributed systems are a means of preventing large-scale IT system failures. This is mainly a risk with Single Points of Failure, where various systems, for example linked systems, depend on a single component to function. If that component fails, the systems that depend on it also fail. With a distributed system, instead of using a single service provider or a single computer system, data and software are divided among various suppliers and systems. Distributed systems can therefore continue to function even if one or more of the suppliers or systems are unavailable.

For example, the Interplanetary File System (IPFS) enables distributed data storage without having to use centrally managed data centres. Bits and pieces of the data, and their management, are divided over a large network without a central point. This decentralisation can go so far that systems are designed in such a way that they continue to function even without human operation. One then speaks of *distributed autonomous organisations*.

Distributed systems are already widely used in large organisations. Netflix, for example, provides its streaming service by means of a distributed system of tens of thousands of computers (Chella, 2018). However, the use of distributed systems by consortia of organisations is still in the experimental phase. For example, the absence of a central point of contact deters public organisations from forming partnerships.

3.5 Post-quantum cryptography

As described in the previous chapter, the quantum computer will make the existing encryption technology obsolete and ineffective from one day to the next. The quantum computer can therefore be regarded as a game changer. With the arrival of the quantum computer, new, stronger cryptographic standards will therefore have to be developed. This ‘post-quantum cryptography’, which uses larger and more complex keys, must be able to withstand the computing power of quantum computers. Although it will probably be some time before a working quantum computer is available, some organisations should already be preparing for migration to post-quantum cryptography.

NIST’s international competition

It is not yet clear what form of post-quantum cryptography will be adopted worldwide. Various parties are currently engaged in drafting a standard. The National Institute of Standards and Technology (NIST) in the United States has

organised an international competition to develop, evaluate and formulate standards for one or more quantum-resistant cryptographic algorithms. It could be 2024 before NIST makes a final choice, which will probably be adopted by the principal players in the digital domain (NIST CSRC, 2019).

The question that needs to be asked here is why the EU is being so hesitant and leaving the initiative to the NIST in this domain. After all, the European Telecommunications Standards Institute (ETSI) or the International Standardisation Organisation (ISO) would also seem to be suitable parties to initiate the process of formulating standards.

Quantum migration as a challenge

Because of the uncertainty surrounding the standard(s) for post-quantum cryptography, it is not yet clear what the migration to this strong form of encryption will involve. According to experts, it will in any case be an enormous challenge (Committee on Technical Assessment of the Feasibility and Implications of Quantum Computing et al., 2019).

It is also important to remember that the successful production of a powerful quantum computer will mark the end of the protection afforded by the regular encryption technology worldwide. An earlier worldwide replacement of an encryption standard shows how long it can take to complete such a migration. When a vulnerability was found in the popular MD5 encryption technology in 2005, it was not until 2014 that Microsoft decided to disable the technology in Windows (Microsoft, 2014). Although it might be relatively easy for an individual organisation to introduce a new, quantum-resistant encryption standard to safeguard its digital systems, the general environment with which the organisation is digitally connected must also take the same step. Only then can the former standard be disabled.

The migration to quantum-resistant encryption could easily take twenty years. Once agreement has been reached on the standards, they will have to be implemented in all the programming languages, protocols and chips. Suppliers will then have to incorporate them in their products. History shows that it could then still be many more years before the majority of internet systems have been provided with updates (Saffman, 2016).

It also has to be remembered that the migration will not only involve protecting the sensitive data of businesses and public authorities with quantum-resistant encryption, but also the encryption or destruction of every copy that was made using the old encryption technology. Many organisations will then suddenly realise just how widely dispersed their data are.

It is also important to bear in mind that as soon as a powerful quantum computer is available, all of the information that is sent across the internet today using regular encryption could be stolen and decrypted.

It is therefore necessary to prepare for the arrival of the quantum computer now by taking measures to protect sensitive personal data and business secrets. Access by unauthorised persons to information ranging from patients' medical files to commercially sensitive information could conceivably still have major repercussions even after thirty years. For that reason alone, it is advisable to commence the migration to post-quantum cryptography as soon as possible.

The technologies for quantum-resistant encryption are already available and are already being used for some purposes – such as safeguarding state secrets.

Monitoring

Because of the considerable uncertainty surrounding the length of time it will take to develop a working quantum computer and the major impact it could have, it is important to monitor developments in this area closely (Committee on Technical Assessment of the Feasibility and Implications of Quantum Computing et al., 2019).

4 Increasing cyber resilience with existing technology

As already mentioned in the introduction, there is little point in mobilising various new technologies to enhance cyber resilience without simultaneously making greater use of the technologies that already exist. This was an important conclusion of the experts we consulted. Existing but underutilised technological measures do indeed provide opportunities to increase cyber resilience.

In this chapter, we discuss the most important examples of existing technological measures: basic security measures such as strong passwords and software updates; biometric identification; Privacy Enhancing Technologies; encryption; digital signature; Secure Development and Operations; safer supply chains; safer communication protocols; and open standards and open source software.

4.1 Basic security measures

As already mentioned in Chapter 2, there is considerable room for improvement in the implementation of basic security measures to enhance cyber resilience. This applies for consumers, businesses and public authorities. Failing to adopt these measures makes IT systems and devices vulnerable to cyber attacks. That vulnerability will only become greater when attackers are able to use new technological tools such as automatic detection and exploitation of vulnerabilities with the help of machine learning.

The basic security measures have often been described. They include using strong passwords and two-factor authentication, promptly installing software updates and making back-ups of important files (NCTV, 2019b; Rathenau Instituut, 2017).

Experience shows that it is often difficult to persuade end users to adopt these measures (Van der Grient & Konings, 2018). Year in and year out, the Netherlands' Cyber Security Monitor reports that not enough is being done to improve basic security.

4.2 Biometrics

The use of biometrics is growing rapidly. Biometric technologies, such as fingerprint or facial scans, enable users to log on to a device, their smartphone for example, without having to use a password. This could yield benefits in the short term, because the method provides greater security than the often weak passwords that users install. However, these technologies also introduce new vulnerabilities. For example, fingerprint scanners can be deceived by the DeepMasterPrints algorithm (Hern, 2018). And researchers have been able to hoodwink the facial recognition feature on popular smartphones with a 3D print of their head (Major, 2018).

Another point that has to be borne in mind is that a biometric hack could have more serious consequences than if a password with characters or a PIN code is used. If a password or PIN code is leaked or discovered it can be changed, but that is not possible with a fingerprint or iris scan that has been hacked. Furthermore, sensitive information about a person can also be derived from a biometric scan, for example a diagnosis of diabetes on the basis of an iris scan (Pultarova, 2017) or other information about their health. There are therefore serious reservations about the large-scale use of biometrics for identification purposes.

4.3 Privacy Enhancing Technologies

The more data (including personal data) that are shared on internet, the greater the risk of the data being leaked or hacked. Curtailing the quantities of data that are shared could therefore substantially increase cyber resilience. There are various Privacy Enhancing Technologies (PETs) available that make that possible. They include search engines like DuckDuckGo and Startpage, which do not save the users' search commands, and the chat service SnapChat, which can delete the tracks left by users after the app has been used.

A PET that was developed in the Netherlands is I Reveal My Attributes (IRMA), an identity management system. IRMA allows users to manage their own digital identity and to confine the data they disclose to the attributes that are required for a particular purpose. For example, a person selling alcohol must be able to establish that the customer is over the statutory minimum age. Compliance with the minimum age is an example of a personal attribute. With IRMA the user can disclose only the evidence that he or she meets the age requirement, in contrast to a traditional ID, such as a driver's licence, which also contains other personal information. Accordingly, the system keeps the data exchanged to a minimum.

Another PET is Social Linked Data (Solid), an open source project led by the internet pioneer Tim Berners-Lee. Solid encourages software developers to separate data storage from data processing. Data added to Solid can be managed in Personal Online Data Stores (PODS). Users can then decide for themselves when and for what purpose the data in their PODS will be used, for example to provide identification (Solid, 2019).

4.4 Encryption

Encryption can be used to encode (personal) data in such a way that they can only be read by those with the correct key. Encryption is often used to protect data that are being transmitted via networks and sensitive data on computers, servers and mobile devices. The information security of Privacy Enhancing Technologies is also based on encryption.

The expectation is that in the coming years encryption will be used not only in the private domain, for example in chat apps such as Whatsapp, Signal and Telegram, but also for business communication. Furthermore, data that is stored, in cloud services for example, is also increasingly being encrypted.

Secure multi-party computation

One reservation regarding the use of encryption concerns the ability to exchange data with other parties. Many encryption technologies require the information to be decrypted before it can be shared or processed. Once it has been decrypted, the information is vulnerable to cyber attacks. Advances in what is known as homomorphic encryption might solve that problem. This technology enables users to process encrypted data without first having to decrypt them, thereby reducing the risk of the information being seen by unauthorised persons.

This technology could be used, for example, in situations where parties have an interest in gaining access to each other's data but do not want to give away all their information. This might be the case if various parties wish to share information about cyber vulnerability and attacks, but none of them wants to reveal that they themselves were targeted by an attack. *Secure multi-party computation* allows the parties to share information without providing details from which a particular party can be identified.

Vulnerabilities in encryption technology

A second reservation regarding the use of encryption is the risk that the encryption key will be broken. The best-known method of cracking encryption is with a *brute-force* attack. In this case, an attacker keeps trying different keys until the correct

one is found. The greater the attacker's computing power, the greater chance of success.

Another method of cracking encryption is with *side-channel* attacks, which target the program's immediate operating environment. For example, energy consumption, electromagnetic fields or sound can provide information from which the correct key can be identified. An attacker can also employ *social engineering*: the use of psychological manipulation to induce individuals to reveal the encryption key or disclose the encrypted information.

As already mentioned, the arrival of the quantum computer will in time make it possible to crack many existing forms of encryption.

Obstacle to criminal investigations

A third remark to be made about the use of encryption (however strong) is that it can also be used by criminals or terrorist groups to protect their communication and so evade investigation by the law-enforcement authorities. Some governments therefore advocate 'responsible encryption'. In that case, technology companies would be able to decrypt information on the basis of a court order. Australia has passed a law requiring technology companies to do this (Scott, 2018). But there is controversy over whether, and if so how, responsible encryption could be implemented in practice. The Dutch government is not a proponent of responsible encryption (Minister of Security and Justice & Minister of Economic Affairs, 2016).

4.5 Digital signature to combat deepfakes

As mentioned in the previous chapter, machine learning could be used to combat manipulated images and videos known as deepfakes. However, this type of disinformation can also be countered with existing, relatively simple technological tools. For example, news sources could add a digital signature to reports, photos and videos. A digital signature allows the reader or viewer to verify the origin of reports – and hence the reliability of the reporting. The technology is widely applicable. Consumers can also use it when sending e-mails, posting messages on social media or transmitting other digital documents, but at present the technology is only used on a small scale.

As with most other technologies, the effectiveness of a digital signature depends entirely on its correct implementation. Vulnerabilities were recently discovered in the signatures on e-mails in Mozilla Thunderbird (Mozilla, 2019), for example, and guarantees of the reliability of PDFs with digital signatures have been found to be inadequate (Stewart, 2019). Moreover, the method does not prevent people from

attaching their signature to unreliable digital documents, consciously or otherwise, and thus helping to spread disinformation.

Digital signatures are also only effective against the spread of disinformation if they are widely used. Government bodies could take the lead in this by encouraging or requiring the use of digital signatures. For media companies, the EU's current policy is based on self-regulation. If that proves insufficient, it might need to switch to more binding rules (EC Media Convergence and Social Media Unit 1.4, 2019).

4.6 Permanent attention for cyber resilience

Cyber resilience would benefit in particular from more structural efforts to prevent digital vulnerabilities. In this section we discuss three examples of a varying nature: SecDevOps, where the importance of cyber resilience is already taken into account during the design process; safer supply chains, where an organisation's focus extends beyond its own processes; and safer communication protocols, which are intended to improve cyber resilience at a more basic level.

4.6.1 SecDevOps for an integrated design process

Well-secured products and services start with a good design process. Secure Development and Operations (*SecDevOps*) is a set of practices designed to promote an integrated approach to IT-related organisational processes.[7] To that end, an organisation's security department, development department and operations department work together to reduce vulnerabilities in the development and roll-out of software (Pal, 2018). In this context, roll-out might refer to how a supplier provides software updates for end users. Updates can also contain vulnerabilities. For instance, researchers at Kaspersky Lab recently revealed that until a short time ago the users of popular Asus devices faced the risk of being attacked through Asus's update tool (GreAT & AMR, 2019).

The aim of SecDevOps is to automate and integrate security measures throughout the development process, from design to implementation by the user. One option might be to use technical tools that proactively scan code for vulnerabilities and identify where systems could be infiltrated (*vulnerability testing and penetration testing*). SecDevOps technologies could also be employed to perform an automatic audit of a new version of software. Jenkins is one such system that is popular amongst software developers for writing new software. In this way, software could

7 See https://www.devsecops.org/

be checked automatically for the ten most common vulnerabilities identified by the Open Web Application Security Project (OWASP) foundation.

An important condition for the widespread application of SecDevOps is that the technology comes ready-to-use. Organisations in the public sector could stipulate its use in their purchasing terms and conditions.

The Dutch Ministry of Defence is already preparing for the adoption of SecDevOps methods. For example, the ministry's Joint IT Command, which is responsible for IT services, has incorporated the method in the New IT Readiness Programme (*Gereedstelling Nieuwe IT*), as can be seen from recent job advertisements (Werken bij de Overheid, 2019).

4.6.2 Safer supply chains

When an organisation's security is in order, attackers will turn their attention to its suppliers. Organisations are therefore well advised to look beyond their own cyber resilience.

The implementation of new software could be safeguarded by attaching a digital watermark (hash) to the installation file, for example. The watermark is a form of digital signature by which users can easily check whether the installation file has been manipulated. Software distribution systems like Google Play and the Apple App Store automatically carry out such checks.

Checks can also be carried out on hardware. For example, the T2 chip in Apple's iMac Pro verifies that the computer is only using trusted software during the start-up process (Apple Support, 2019).

Other – non-technological – measures to enhance the cyber resilience of suppliers are certification, purchasing conditions and oversight. The Ministry of Defence, for example, imposes strict conditions on suppliers in its General Security Requirements for Defence Orders (ABDO).

4.6.3 Safer communication protocols

The internet's technical infrastructure consists of a number of technological 'layers'. Vulnerabilities can be found not only in the higher application layers, but also at more basic levels. The more basic IT infrastructure includes communication protocols, such as connection protocols (for data exchange between network elements), network protocols (for data exchange between source and destination), and application protocols (for data exchange between applications). Other basic elements are hardware, firmware and operating systems. Generally speaking, the same basic infrastructure is used by multiple applications. Technological innovations that remove vulnerabilities at these 'deeper' levels could therefore have a very significant effect in terms of enhancing cyber resilience.

Dutch research institutes such as Delft University of Technology, the University of Twente, SURF and TNO are working on improvements to communication protocols. If they are to genuinely improve cyber resilience, the protocols must be widely implemented. The problem is that they not always are, or only partially. For example, there is a safer alternative to the commonly used Internet Protocol (IP) Version 4, namely IP Version 6 (IPv6). However, the new protocol's penetration of the worldwide web has only reached 25% in the last ten years (Google, 2019).

In fact, even the new version of the IP protocol contains vulnerabilities. The reason for this is that the protocol works in such a way that the digital addresses of users are often visible and accessible to every participant on the internet. An alternative protocol such as RINA hides the digital addresses and thus increases their security. Furthermore, with the IP protocol administrators are required to take additional measures to safeguard important data. There is another way: a protocol like Named Data Networking (NDN) takes data security as its point of departure. The project Scalability, Control and Isolation on Next-Generation Networks (SCION) is also worth mentioning. In this alternative network protocol, communication is based on important principles such as control, transparency and resilience. However, these alternative protocols are still in the experimental phase.

In practice, the widespread replacement of a communication protocol with a newer version is problematic. That applies to an even greater extent for the transition to an entirely new communication protocol. It is a bit like introducing driving on the right in the United Kingdom. A communication protocol can only be successfully replaced if a large majority of the participants in a network agree to it, or if both the old and the new system continue to run simultaneously. However, for many existing devices and programs it is not possible to replace the communication protocol. A complete worldwide transition can therefore only be made by entirely replacing the equipment and software.

The great difficulty of implementing safer communication protocols is the reason why only small steps are being taken in this direction worldwide. Another obstacle to progress is the deadlock in the intergovernmental talks on a worldwide system of internet governance. The deliberations of the UN Group of Governmental Experts (UN-GGE) ended without a final declaration in 2017. There have been a number of public-private initiatives since then, such as the Cyber Security Tech Accord in 2018, but more than anything worldwide progress in this domain calls for a broad consensus on specific standards and enforcement (Rathenau Instituut, 2019b).

The transition to an alternative communication protocol might be easier if a major player in the digital domain expresses its support for it. For instance, a number of years ago Google decided to promote the use of the HTTPS protocol. Today, the Chrome browser displays a warning if surfers are visiting a website without HTTPS. Providers of websites responded by quickly implementing the HTTPS protocol (Sheridan, 2018) and in just a few years HTTPS was being used in more than 90% of all websites (Google, 2019).

In the public sector in the Netherlands, the principle of ‘comply or explain’ applies with respect to the use of safer standards like HTTPS and IPv6 when purchasing products or services worth €50,000 or more (Standardisation Forum, 2019). In practice, this rule is still not always followed. For example, the websites of a large number of Dutch hospitals fail to comply (Van der Laan, 2019). Experts call on the government to adopt more binding measures to promote compliance (Schneier, 2018).

4.7 Open data standards and open source software

As with the growing use of cloud services discussed earlier, when buying digital products or services end users often enter into relationships whose consequences they are unable to appreciate. For example, users are regularly confronted with changes in the terms and conditions under which a digital service or product is provided by the supplier. They then have to decide between accepting the revised terms and conditions or incurring the expense of switching to an alternative supplier. This can also be at the expense of cyber resilience, because users are not always offered the product with the best security.

Using open data standards and open source software could make it easier for a user to switch to a different supplier because the costs would be lower. Suppliers would also come under greater pressure to improve their products and services. There would be gradations in the degree of openness, ranging from the right to

inspect the software code to the freedom to make changes to the software and disseminate it. The greater the user's freedom of choice, the weaker its dependence on a supplier.

The Reuse of Public Sector Information Act (*Wet hergebruik overheidsinformatie*, *Who*) is intended to promote the use of open data standards. For example, public and semi-public organisations are obliged to use the Open Document Format (ODF) for text files rather than software-specific formats such as Microsoft Word's Docx. The experts we consulted observed that the law on open data standards is not universally complied with. The use of open source software is encouraged in the public sector but has not been adopted as a standard (Ministry of the Interior and Kingdom Relations, 2014).

Not necessarily safe

Incidentally, the use of open standards and open source software does not automatically enhance cyber resilience. This was demonstrated by the *HeartBleed* vulnerability in 2014, which affected 66% of all global web services but went unnoticed for a long time even though everyone had access to the software's source code and could have discovered the vulnerability.

Accordingly, malicious parties could also learn more about potential vulnerabilities in software and exploit them. Many of the initiatives in this domain are undertaken by volunteers, who also perform the maintenance. Since arrears of maintenance can be at the expense of security, software and standards must be constantly updated to remedy recently discovered vulnerabilities.

5 Conditions for taking advantage of technological opportunities

This chapter describes the conditions that need to be met in order to benefit from the opportunities created by new and existing technologies for enhancing cyber resilience, with the focus mainly on the public sector and providers of vital services.

5.1 Cyber resilience starts with a risk analysis

The use of technological measures to enhance cyber resilience presupposes an adequate risk analysis at board level of those of the organisation's critical data and processes that require maximum security. On the basis of this risk analysis, a decision then has to be made on which of the organisation's units and processes need to be connected to the internet and which do not. This review should devote special attention to large databases with sensitive data.

Decision should be made at board level

Decisions on the digitisation of organisational processes and the need for connection to the internet are often regarded as technological issues falling under the auspices of the IT department. However, the decision to digitise processes and how it should be done must be preceded by a risk analysis at board level: what are the organisation's critical data and processes ('crown jewels') that require maximum security? What risks are acceptable? And how should the benefits of being linked to the internet be weighed against the drawbacks?

Assessment frameworks for analysing risks and information about the effectiveness of measures to reduce risks can help organisations to make these decisions. The Netherlands does not yet have a generally accepted systematic approach to making an adequate risk assessment (NCTV, 2019a). Rijkswaterstaat has formulated its own list of criteria for risk assessments. These Cyber Security Implementation Guidelines for Structure Managed by Rijkswaterstaat (*Cybersecurity Implementatierichtlijn Objecten Rijkswaterstaat, CSIR*) are based on the standards laid down in the State Baseline Information Security (*Baseline Informatiebeveiliging Rijksdienst, BIR*) (Netherlands Court of Audit, 2019a).

Critical databases

A number of the experts we consulted said that greater attention was needed for critical databases containing sensitive data, such as information about people's

health, or large registers of personal data. When large volumes of data about individuals are collected in a database, a data leak or a hack can have serious social consequences.

Sensitive data should be better secured, for example with strong forms of encryption or Privacy Enhancing Technologies (PETs). In the case of medical data, various parties advocate the introduction of ‘patient confidentiality’ to give patients greater powers to prevent data from being automatically shared, for example with parties outside the medical domain (Hooghiemstra, 2018; Rathenau Instituut, 2019d; Patiëntenfederatie, 2019).

5.2 The government as role model

The government is in a position to play a prominent and exemplary role in relation to cyber resilience. As a major customer of digital products and services and a major service provider, the government could have a huge influence on the overall level of cyber resilience, for example through the standard use of multi-factor authentication, strong encryption of sensitive data and Privacy Enhancing Technologies. The government could also insist that public news media add digital signatures to their reports to counter the risk of the spread of fake news and disinformation.

Box 1 Elevating Privacy Enhancing Technologies to a standard

The national government occupies a key position with respect to promoting the wider use of PETs through its role in managing files and issuing identity papers and by virtue of the digital logging on to government services with DigiD. For example, providing a PET like the KopieID app, which enables users to hide unnecessary information on a copy of an ID and to attach a watermark to the copy, would immediately make a difference.

To be adopted on a wide scale, PETs must be reliable, transparent and user-friendly and familiar to users.

National government's cyber resilience not fit for purpose

There is still work to be done before the government can perform this exemplary role. In a recent report, for example, the Netherlands Court of Audit found 'serious problems' in the information security of various public sector organisations. These organisations fail to comply with all the measures prescribed by the government in relation to cyber resilience. The number of shortcomings had actually increased compared with the previous year, the Netherlands Court of Audit observed, adding that they were due in a part to a lack of expertise within the ministries (Netherlands Court of Audit, 2019b).

To strengthen efforts to create a cyber-resilient government and enhance the government function as a role model, there is a lot to be said for concentrating responsibility in this domain in a single entity. A number of the experts we consulted said that responsibility for cyber resilience is too fragmented across the various ministries. They favour tighter coordination and direction. Whether the recent Coordination of Central Government Organisation and Operational Management Decree (*Coördinatiebesluit*), which delegates more powers in this domain to the Ministry of the Interior and Kingdom Relations, is adequate to accomplish this is open to question. The United Kingdom chose to respond to the need for tighter coordination by delegating responsibility for the central government's cyber resilience to a single ministry.

Anticipation of new technologies

To fulfil its function as a role model the government must also adequately anticipate the possibilities that new technologies will create for increasing its own cyber resilience.

It proved difficult to form a clear impression of the level of awareness in the public sector – and more widely among suppliers of vital services – of the potential of new technologies. The experts we consulted generally expressed themselves in general terms. They are concerned about the government and about sectors such as care and education. Their anxieties for the government are rooted in part in the critical findings of the Elias Committee (which conducted a parliamentary investigation into large government IT projects) and the advisory report of the Information Society and Government Study Group entitled ‘Make it Happen!’. Their feeling is that those findings are still relevant and that not enough is being done to make use of new technologies to increase cyber resilience in the public sector.

But that view does not apply for all vital suppliers. According to the experts, cyber resilience is high on the agenda in the financial, telecom and energy sectors and these sectors are taking advantage of the possibilities offered by the new technologies. Experts who work in these sectors are also very aware of the opportunities that technologies such as machine learning create to enhance cyber resilience.

5.3 Legislation and regulation

A second way in which the government can increase the general level of cyber resilience is by encouraging suppliers to market digital products and services with stronger in-built security. Here we discuss three frequently mentioned instruments that are available to the government: legislation, preferably based on open standards; certification; and standardisation.

5.3.1 Open statutory standards and regulation

In light of the rapid pace of technological developments in the field of IT, legislation and regulation should preferably be based on ‘open’ standards. For example, the Networks and Information Systems (Security) Act (Wbni) from 2018 imposes a duty of care on all suppliers of vital services and digital service providers (such as online market places and cloud service providers). The law provides that suppliers must take ‘appropriate and proportionate technical and organisational measures’ to safeguard stored and processed data. Using open standards prevents the

requirements laid down in a law from becoming outdated even before the law takes effect.

Oversight of open standards

The use of open standards requires clear frameworks and adequate oversight. Regulators must have guidelines for monitoring the further implementation of the open standards and supervising compliance with them. This implies an important role for regulatory bodies such as the Radiocommunications Agency Netherlands, the Authority for Consumers and Markets and the Dutch Data Protection Authority. These agencies must also have the necessary resources to perform that role, in terms of both manpower and expertise.

Coordination of oversight

Digitisation affects a growing number of domains. Consequently, digital products and services increasingly transcend the boundaries of specific legal domains and can therefore fall under the scrutiny of more than one regulatory body. A single product, such as a car or a ‘lifestyle app’, can be covered by the guidelines for consumer products, digital service providers, goods with a digital element and sector-specific legislation. Adequate regulation of such products calls for cooperation and coordination among the regulatory bodies at both national and international level. One of the questions this raises is which agency has authority in a particular area. That calls for research into the possibilities for national and international coordination and cooperation. Research into governance issues is one of the priorities in the National Cyber Security Research Agenda. The European research project CyberSec4Europe is also concerned with issues of this nature (DG CONNECT, 2019a).

The international consumer organisations Consumers International and BEUC are critical of the manner in which the regulators in the EU member states protect consumers in the digital domain. According to these organisations, the regulators devote too little attention to protecting privacy and information security and their approach is often too fragmented (Coll & Simpson, 2016). In their view, regulators should adopt a more integrated approach to the protection of consumers’ digital rights and devote more attention to issues such as fairness in the relationship between consumers and companies (Consumers International et al., 2017).

5.3.2 Certification

A second instrument the government could use to encourage suppliers to market digital products and services with better security is certification. Certificates would enable consumers to determine whether digital services and products meet minimum requirements.

The European Cybersecurity Act was adopted in 2018. The law establishes a Cybersecurity Certification Framework for digital products and services. The expectation is that the framework will require developers of Internet of Things devices to employ the security-by-design principle. Certification will be voluntary and there will be three levels: basic, substantial and high. The framework still has to be implemented in national legislation, so it is not yet clear precisely what impact the European Cybersecurity Act will have. The EU opted for voluntary certification in order to avoid increasing the costs of market entry (Stupp, 2018a). Consumer organisations have expressed disappointment in that decision (Stupp, 2018b). A number of the experts we consulted also mentioned the importance of mandatory certification.

Certification in the digital domain could also be based on the EU's Radio Equipment Directive, which was amended in 2017. The directive regulates CE marking as it applies to radio equipment. The rules govern aspects such as safe use, prevention of interference and reliability. The Netherlands intends to lobby in the EU for the inclusion of minimum safety requirements for Internet of Things devices in the directive (Ministry of Economic Affairs and Climate Policy, 2018).

Proof of safety?

An important remark that needs to be made in connection with the use of certification for suppliers of digital products and services is that it is not yet possible to prove incontrovertibly that products and services are safe (*provable secure*). Instead, suppliers and users can use contractual agreements, tests can be carried out and suppliers can allow users to inspect the software they used. For the time being, research into the possibilities of demonstrating the safety of products and services is still an academic affair. It is also an item on the National Cyber Security Research Agenda (Dcypher, 2018).

With respect to cryptography, developers are able to provide mathematical evidence of the security of their encryption. For example, the mathematical principle behind the RSA encryption technique – which forms the basis for the 'green lock' in the browser – is known. The level of information security claimed for the RSA algorithm can therefore be verified independently.

5.3.3 International standardisation

Standardisation is a third instrument the government can use to persuade suppliers to market more secure digital products and services. Standards are crucial for international measures in the area of cyber resilience.

Market actors in charge

Up to now, standards in the digital domain have been formulated mainly by the market without being preceded by a formal standardisation process. For example, in the past communication protocols such as HTTP and IP became the standard mainly because of their popularity among users. Where there are standardisation processes, large technology companies generally have a large say in what happens. They often possess the expertise to provide technical know-how and are willing to deploy the necessary manpower to attend meetings and so exercise influence on the standardisation process. Governments generally lag behind in that regard.

Although there are international policy forums, such as the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Governance Forum (IGF), the International Telecommunication Union (ITU) and the Internet Society (ISOC), they currently have little or no say in the matter of the global internet infrastructure (Van Eeten, 2017).

International role of governments

For a long time, it was also regarded as impossible to formulate international policy in the field of cyber resilience. This was possibly due to the fact that the process would quickly involve thousands of parties in a great many countries. The recent emergence of a small number of dominant players, such as cloud services and platform companies whose operations encompass a large part of the international market, has created a situation where international policy measures could have a major impact.

The competition organised by the American NIST to develop a standard for post-quantum cryptography also shows that governments can indeed play a significant international role. This is also apparent from the worldwide impact of the EU's General Data Protection Regulation (GDPR). Given the importance of the international forums in which decisions on international guidelines and standards are made, the Dutch government – or better yet the EU – should be more intensively involved in them. One of the aims should be to ensure that the final guidelines and standards adequately reflect important European values such as security, privacy and autonomy.

Even a relatively small country like the Netherlands can exert influence on international standards. The Netherlands is the market leader in the field of charging points for electric vehicles, for instance. Accordingly, it influences choices that have a worldwide impact. For example, the car maker Tesla responded to the charging points manufactured by the Dutch company FastNed by supplying adapters with which the Tesla can also be easily charged in the Netherlands (De

Jong, 2019). Although this is not an example of cyber resilience, it does show that even a small country can secure an international following by being in the vanguard of developments and introducing a particular standard.

5.4 Strengthening digital autonomy

In this study we have seen that there is a trend towards more services being offered by cloud suppliers. That trend could lead to greater cyber resilience, because cloud service providers generally possess more knowledge and greater capacity to make systems secure than users have. But, as we have also seen, it can also lead to greater dependence on cloud suppliers and the accompanying risks such as loss of functionality in the event of a system failure and loss of control of data and data processing.

The experts we consulted share the view that these risks of dependence are undesirable. Opinions differ, however, on the possibilities for reducing that dependence – and thus also increasing the digital autonomy of users. A number of the experts argue that the Netherlands – and in a broader perspective, the EU – is not doing enough to build a domestic IT industry. They say that too many promising Dutch or European start-ups are acquired and monetised by foreign technology companies, which merely increases the dependence of these companies. Heavier investment in national businesses and innovation could reduce the dependence on external parties, they feel. This business activity and innovation could in fact also be generated by ‘social enterprises’, non-profit organisations or public IT service providers.

Others feel that Dutch or European suppliers of digital products and services would not be able to match the large technology companies, which lead the world in R&D in the field of cyber resilience. See also the remark by Jeff Moss, founder of the hackers conference Black Hat, that there are perhaps twenty companies in a position to make a substantial contribution to increasing cyber resilience worldwide (Sheridan, 2018). It might therefore be more effective to combat undesirable dependence by stipulating stricter conditions for the reliability and continuity of service provision, at national or EU level, and incorporating them in the purchasing conditions.

A third option for preventing undesirable dependence and increasing digital autonomy is the use of technical measures such as PETs, encryption and open standards and open source software. The first two measures could prevent the undesirable dissemination or reuse of data; the last two could prevent excessive dependence on a single cloud supplier.

The various options are not mutually exclusive. The goal of expanding the IT industry in the Netherlands or Europe and providing better protection for businesses against takeovers could be accompanied by the adoption of more stringent security requirements – such as the obligation to use PETs and encryption – in purchasing conditions.

5.4.1 Strengthening digital autonomy with technology

Technologies such as PETs and encryption could prevent other parties from disseminating and using one's data and so help the data's owner to retain control of the data and its processing. The use of open standards and open source software could also help end users to avoid undesirable dependence on a cloud supplier and the risk of vendor lock-in by making it easier for them to switch to another supplier.

The use of PETs, encryption and open source software are obvious possibilities to strengthen the user's digital autonomy, since these options already exist but are underutilised.

Opinions differ among the experts we consulted on the necessity, from the perspective of cyber resilience, of storing the national government's data in data centres within the national borders. While some take the view that this would improve the government's control of the security and reliability of the data storage, others argue that it makes little difference where data are stored as long as they are encrypted strongly enough.

On that latter point, it is important that the encryption can be fully trusted, which means it has to be developed and implemented by trusted parties, at least as far as the security of the critical data of government and business, such as state secrets or the 'crown jewels' of companies, is concerned.

5.4.2 Strengthening digital autonomy with stricter purchasing conditions

A second way of avoiding the negative effects of dependence on foreign parties and increasing digital autonomy would be to impose stricter requirements for cyber resilience and control over data and data processing in purchasing conditions. For example, Dutch and European parties could insist that providers of cloud services prevent stored data from being inspected by the providers themselves or by third parties, for example by always encrypting data. For some time, the Dutch Ministry

of Defence has imposed specific conditions on suppliers in relation to cyber resilience, among other things (see box).

According to various experts we consulted, the ABDO purchasing conditions are a good example of how stricter requirements can be imposed on suppliers of digital products and services. However, others wonder whether all of the ABDO conditions actually lead to the greatest possible resilience (Olsthoorn, 2017). For example, the ABDO requires that every one of a contractor's employees in a position requiring confidentiality must have Dutch nationality. This condition is pointless if there are not enough Dutch nationals with the necessary qualifications available to fill the position.

Box 2 ABDO purchasing conditions for IT suppliers

Suppliers of the Ministry of Defence must comply with the General Security Requirements for Defence Contracts (ABDO). The category of the Interest to be Protected (*Te Beschermen Belang, TBB*) is an important factor in this context. Interests are divided into four categories according to the potential damage that could result from information being seen by unauthorised persons. The requirements imposed on the supplier vary according to the category of the interest to be protected.

Since 2017, a separate chapter of the ABDO has been devoted to IT security. The requirements relate to organisational measures, such as the obligation to appoint a cyber security officer, and technical measures, relating to encryption and cloud computing, for example. The requirements are specific and together constitute a checklist.

According to various experts, the national government and the suppliers of vital services should play a leading role in drafting stricter requirements for cyber resilience. To this end, they should join forces and together draft purchasing conditions. Others point out that, with a view to the necessary market strength, it would be better to coordinate purchasing conditions at European level. The European Union Agency for Cyber Security (ENISA) has also drawn up guidelines for purchasing policy (ENISA, 2014).

Purchasing conditions for 5G

There is growing attention in the Netherlands to the implications of the construction of the 5G network for cyber resilience. The NCTV's Economic Security Task Force recently published an advisory report on the subject, which was adopted by the government in July 2019. As a result, telecom providers will be obliged to take additional security measures to protect their network, including setting extra high requirements for suppliers of services and products in critical areas (Ministry of Justice and Security, 2019). It is not known which elements will be affected (Hijink, 2019).

This situation accords with the EU's policy on 5G networks, which is geared to the adoption of additional conditions in relation to cyber resilience. That strategy diverges from the United States' policy of excluding countries with an 'offensive' cyber programme from involvement in the construction of 5G networks. In addition to the United States, Australia, New Zealand and Japan have also decided to exclude the Chinese supplier Huawei on the same grounds (Tao, 2018). It is not yet clear what the extra conditions envisaged by the EU will amount to.

A similar debate is taking place in Germany. At the beginning of 2019, this led to the adoption of stricter requirements for companies that wish to bid in the auction of 5G frequencies (Bundesnetzagentur, 2019). The requirements were drawn up by the German regulatory authorities for telecommunication and data protection. They include mandatory certification of critical components by Germany's Federal Office for Information Security (BSI), periodic security tests and the prevention of 'monocultures'.[8]

The EU has drafted a proposal for the coordination of national purchasing conditions. In March 2019, the European Commission proposed a common European approach to the security of 5G networks (European Commission, 2019a).

5.4.3 Strengthening digital autonomy with a domestic IT industry

A third way in which the Netherlands and the EU can avoid excessive dependence on major foreign parties is by developing their own IT industries. This implies that the Netherlands and the EU must give greater priority to establishing a stronger IT industry, and in particular to developing and implementing new technologies that enhance cyber resilience. As mentioned above, these activities could be carried out

8 For the complete list of requirements, see https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2019/20190307_SL.html

by private enterprises, but also by other organisations such as NGOs or public IT service providers.

The Netherlands is not necessarily too small – as is often asserted – to perform this role, and certainly not when seen in the context of larger alliances such as NATO or the EU. The fact that an even smaller country like Estonia can play an independent role within NATO in the area of cyber resilience shows that a country's size is not decisive. However, the experts we consulted did point out that Estonia is in a special position. The continuous threat from and experiences with (Russian) cyber attacks in Estonia were often mentioned as a crucial factor, leading as they did to a widely shared sense of urgency regarding the need to strengthen cyber resilience.

Focus in the knowledge and innovation agenda

Developing a larger domestic IT industry – with the primary aim of improving cyber resilience – calls for a more effective knowledge and innovation policy. The Dutch government took a first step in that direction last year by drafting a 'mission-driven' innovation policy, in which cyber security is one of the 25 missions (Ministry of Economic Affairs and Climate Policy, 2019). The Dutch Cyber Security Research Agenda (NCSRA) has formed an important substantive guideline for this.

However, the experts we consulted take the view that the NCSRA lacks the necessary focus to make a real difference. In their opinion, the government should make more specific choices with respect to the areas in which Dutch research institutes should be in the international vanguard, and then market the knowledge that is created.

Innovation policy would also benefit from a sharper focus. The funding of innovation is mainly general in nature in the Netherlands. For years, approximately 90% of investment in innovation has taken the form of general tax-related support (Rathenau, 2018). One of the few non-tax instruments, the Small Business Innovation Research (SBIR) programme, could be used to create a sharper focus. For the time being, however, this instrument is being used across the full breadth of the NCSRA (see box 3: SBIR Cyber Security stimulates IT activity across the full breadth of the NCSRA).

The government as launching customer

The government could also foster a domestic IT industry by assuming the role of *launch customer*. In that capacity, the government would invest risk-bearing capital in promising start-ups, social enterprises and non-profit organisations and be a major customer of successful digital products and services, thus contributing to the scaling up of the enterprise or organisation concerned. Suppliers of vital services could also act as launch customers more frequently.

It is important to bear in mind that the number of start-ups and SMEs in the IT sector is relatively large. To promote and reap the benefits of innovation, it is important to create favourable conditions for innovative organisations. One aspect that demands attention is tender procedures. According to a number of the experts we consulted, tender procedures often take too little account of start-ups. They feel that tenders are usually too large and too complex for them, which means that it is mainly larger parties that qualify for the contracts.

Box 3 SBIR Cyber Security programme encourages IT-related business activity across the entire spectrum of NCSRA

The Small Business Innovation Research Cyber Security programme subsidises research into the feasibility and the development of innovations (RVO, 2017). Ninety percent of the budget comes from the European Union's Fund for Internal Security (ISF); 10% is a subsidy from the National Coordinator for Security and Counterterrorism (NCTV).

The NCSRA provides the guidelines for the SBIR programme. Enterprises are invited to bid for funding for projects that contribute to achieving the government's main policy objectives for cyber resilience in a tender procedure. Those main objectives are broadly formulated.

An analysis of 43 selected project proposals showed that a wide range of initiatives receive financing. Roughly half of the proposals involved a technology for information or network security, for example a method of authentication or an app or cloud technology. Another third of the project proposals focused on the development of management instruments, for example for gathering and publishing information about data, networks and vulnerabilities. Most of the remaining proposals were for training and awareness-raising projects.

The criteria adopted by the SBIR assessment committee to evaluate proposals are impact, technological feasibility, economic perspective and the bid price. This list does not reflect a preference for a particular technology or a particular ratio of technological to more organisational proposals.

To promote innovation, the government should therefore also create more scope for involvement by small enterprises and non-profit organisations. That is one of the objectives of the planned Cyber Innovation Hub, in which ministries, research institutes and businesses will collaborate in addressing issues relating to cyber resilience (Rathenau Instituut, 2019a).

In addition to the regular public sector parties, there could also be a role for the intelligence services. There is very little collaboration between small start-up enterprises and the intelligence and security services in the Netherlands. The reason for this is that enterprises and their products and employees must undergo a strict screening procedure before they are allowed to operate in the intelligence domain. In practice, small companies are seldom able to successfully complete these procedures.

DARPA as an example

The American agency for military innovation DARPA employs a form of collaboration with technology developers that is interesting in light of the aforementioned conditions for innovation. By acting as launch customer, DARPA is involved in the process of translating knowledge into innovations from an early stage. Nor does DARPA require a screening of the parties with which it works during this phase. Advanced simulation environments have been created to allow the collaboration to take place outside the secret domain (DARPA, 2008).

In 2018, Germany established an organisation whose mission is similar to DARPA's (Delcker, 2018). According to the German government, the organisation's goal is to reduce Germany's dependence on foreign suppliers. However, its budget of 200 million euros for a period of five years pales in comparison to DARPA's annual budget of almost three billion euros.

Value-driven innovation

An incidental, but not insignificant, argument in favour of the Netherlands or the European Union establishing its own position in the global IT market, is the prominent role the EU plays in the normatively charged regulation of IT developments, as illustrated by the worldwide impact of the General Data Protection Regulation (GDPR). The EU could strengthen the normative force of its interventions by campaigning more strongly for the development of IT-related products and services that reflect values such as security, privacy and autonomy (Dobbe & Stikker, 2019). European enterprises could in this way set themselves apart from their American, Chinese and Russian competitors.

5.5 Post-quantum cryptography creates opportunities for IT enterprises

A number of parties in the Netherlands are taking part in the NIST competition to establish an international standard for post-quantum cryptography. With institutions such as Radboud University, CWI Amsterdam, Eindhoven University of Technology and Philips, the Netherlands has a solid knowledge base in this field.

The Netherlands' prominent international knowledge position creates opportunities for the country to develop its own industry in the field of post-quantum cryptography. With the help of the expertise in Dutch research institutes, that industry could develop products and services to support the forthcoming, large-scale migration to quantum-proof encryption.

That other countries are already moving in that direction is demonstrated by the activities of the British company PQShield and the support it receives from the British government. In anticipation of the migration to post-quantum cryptography, this company is already laying the groundwork for product development, by recruiting experts for example. No such steps are being taken yet in the Netherlands.

5.6 Exploiting the potential of post-quantum cryptography and machine learning

The preceding review raises the question of what is needed to take advantage of the opportunities created by the new technologies. What demands will be made on the relevant public authorities, businesses and research institutes? In answering that question, we will focus mainly on post-quantum cryptography and machine learning and on central government and suppliers of vital services.

Dealing with technological innovation

It has to be remembered that although there are already applications of machine learning and post-quantum cryptography, both technologies are still evolving. With respect to post-quantum cryptography, an important example is the NIST competition to develop standards for cryptography. Because new applications of the technology are still being developed, it is not yet possible to say precisely what shape this technology will ultimately take and what will be required to implement it properly in specific situations.

It is, however, possible to say something about how organisations can anticipate and exploit the emerging technological possibilities. This study shows that there are major differences in how vital suppliers deal with technological innovations. Large organisations with their own research departments are able to look ahead to technological developments in the more distant future and to develop innovative solutions for issues connected with cyber resilience in collaboration with research institutes. An example would be measures to prevent pollution or bias in the datasets used to train smart algorithms. However, the organisations would still have to implement the ensuing applications.

For the collaboration with research institutes, the organisation concerned will also have to be aware of where new knowledge and products are being produced. That means they will need the necessary in-house expertise to identify those developments and the internal capacity to experiment with them. The experts from the external partners will have to be familiar with the organisation and the issues it faces. This applies, for example, to an organisation like the AIVD, which is investigating the potential of using machine learning for the purposes of investigation in association with research institutes in the Netherlands and elsewhere. The collaboration could benefit from the geographic and cultural 'proximity' of the organisation to the research institutes (Boschma, 2005; Rathenau Instituut,2018a), but that does not appear to be essential.

However, suppliers of vital services do not all have their own research capacity. They rely on commercial suppliers for innovative products or services. What they need most of all is the help of experts in accurately assessing the true value of what is available on the market, including the question of whether the products and services genuinely provide a solution for the issues they currently face or are likely to face in the near future in relation to cyber resilience. Because these organisations are required to put contracts for the purchase of the necessary products and services out to tender, they are dealing with a global supply market. However, large, international suppliers of digital products and services could also provide local support.

Support from the government

The government could support the use of new technologies such as machine learning and post-quantum cryptography in various ways. In the first place, it should continue investing in the development of knowledge in the field of machine learning and post-quantum cryptography by research institutes. Collaboration between research institutes and other organisations should be facilitated wherever possible. Organisations that do not have their own research capacity should be able to request assistance in assessing which of the products and services available on the market are appropriate. This support could be provided by the existing Information Sharing and Analysis Centres (for vital suppliers) and Digital Trust Centre (for non-vital suppliers).

Transparency of statutory frameworks

As mentioned in Chapter 3, it is questionable whether the use of machine learning to automatically repair vulnerabilities and to provide an automatic response to attacks is compatible with the Software Directive or the statutory rules on hacking. The government would be well-advised to clarify this situation.

5.7 Successful use of new technology depends on the available expertise

Perhaps the most important requirement for taking advantage of the opportunities offered by new and existing technologies to increase cyber resilience is the availability of sufficient expertise. Government, suppliers of vital services, other businesses and regulatory bodies must all have sufficient manpower and expertise to develop and implement these technologies.

There are serious concerns that this expertise is lacking, however. A number of the experts we consulted referred to a large and persistent shortage of experts in the field of cyber resilience in the Netherlands. According to the international association of IT professionals ISACA, half of the cyber security organisations faced staff shortages in 2018 (ISACA, 2018). The trade association ISC2 says the worldwide deficit is three million professionals (ISC2, 2018). Dutch enterprises regard the lack of expertise as a major obstacle to the use of machine learning (AINED, 2018).

Because of this shortage of experts, it is necessary to invest more in IT training at the level of secondary and higher professional education (MBO and HBO) and at university level. The Cyber Security Council called earlier for the training of more IT professionals (Broekhuizen, 2018).

6 Conclusions

The findings presented in the previous chapters lead to the following conclusions.

6.1 Opportunities for new technology

New technologies create opportunities to enhance cyber resilience

Machine learning, post-quantum cryptography, 5G networks, LiFi, quantum communication and distributed systems are new technologies that create opportunities to enhance cyber resilience in the Netherlands. With machine learning, it will be possible to detect and repair vulnerabilities in software on a large scale and automatically. Machine learning can also be used to counter deepfakes, visual materials that have been manipulated. Post-quantum cryptography can be used to produce data encryption that is strong enough to withstand attacks using the computing power of a quantum computer. 5G networks could improve the security of communication networks. LiFi and quantum communication also facilitate safer forms of digital communication that are more difficult to intercept. Finally, the use of distributed systems could help to increase resilience against loss of functionality in the event of malfunction. These technologies are still evolving and are only used to a limited extent.

Machine learning and post-quantum cryptography: opportunity and necessity

The use of new technologies such as automatic detection and repair of vulnerabilities or post-quantum cryptography not only represent an opportunity to increase cyber resilience. It is also essential to use them if cyber resilience in the Netherlands is to keep pace with the possibilities that the new technologies also offer for malicious parties.

The urgency is most clearly illustrated in the field of quantum computing: a mass migration to post-quantum cryptography will have to be made before the quantum computer makes it possible to break existing forms of cryptography. A similar argument applies for the use of machine learning for automatic detection and response: the expectation is that manual defences alone will soon be insufficient to counter the massive and advanced attacks that machine learning makes possible.

6.2 Potential of existing technology

Basic security measures remain underutilised

There is little point in exploiting the possibilities of new technologies for increasing cyber resilience unless wider use is made of existing technologies at the same time. Existing, but underutilised technologies also provide opportunities to increase cyber resilience in the Netherlands.

The same applies for resilience against advanced attacks, for example attacks which use machine learning for offensive purposes. Basic security measures (such as strong passwords and software updates) and other available measures (encryption, adding digital signatures to reports) could make a substantial contribution to the resilience against the automatic detection and exploitation of digital vulnerabilities or the dissemination of deepfake images and videos. It is therefore problematic that such measures, which are already available, are not fully utilised. The government should therefore intensify efforts to increase the use of these options to enhance cyber resilience.

Attention to structural resilience could yield substantial benefits

The resilience of the internet's technical infrastructure could also be improved at a more basic level. There is a lot to be gained by always taking cyber resilience into account in the design of systems and applications. Think, for example, of the use of safer hardware and communication protocols, whose use should be made compulsory by the government.

6.3 The Netherlands and Europe are falling behind

Dutch and European parties depend heavily on large foreign – mainly American and Chinese – technology companies for their digital products and services. The same applies for various applications that could improve cyber resilience. An important trend in this context is that end users (consumers, businesses and governments) increasingly outsource measures connected with cyber resilience to – foreign – cloud suppliers. This creates a growing dependence on these parties, as well as new risks including loss of functionality, Single Points of Failure and loss of control of data and data processing.

Large foreign companies also lead the way in the development and implementation of new technologies such as machine learning, quantum computing and 5G networks. The Netherlands and the EU are therefore in danger of falling further behind.

6.4 Options for strengthening digital autonomy

There are various options for averting the risks connected with the growing dependence of Dutch and European parties on foreign technology companies and strengthening the digital autonomy of the Netherlands and the EU: adopting technological measures such as Privacy Enhancing Technologies, encryption and open standards; formulating stricter purchasing conditions for digital products and services; and by developing the domestic IT industry.

Strengthening autonomy through technological measures

Risks such as undesirable access to data, vendor lock-in and Single Points of Failure can be averted by making it standard practice to use instruments such as Privacy Enhancing Technologies, strong encryption, open data standards, open source software and distributed systems.

Strengthening autonomy through stronger purchasing conditions

A second option for averting the risks of dependence is to stipulate stricter requirements for suppliers of digital products and services in the purchasing conditions. For example, insisting that cloud service providers encrypt all stored data so that they cannot be inspected by the supplier or by third parties.

Strengthening autonomy through a domestic IT industry

A third option for avoiding excessive dependence on foreign parties is to create a larger IT industry in the Netherlands and Europe.

6.5 Promoting a domestic IT industry

Post-quantum cryptography creates opportunities for domestic enterprises

Dutch research institutes possess cutting-edge knowledge in the field of post-quantum cryptography. Marketing this knowledge will create possibilities for developing a domestic IT industry. Instead of waiting until the American National Institute for Standards and Technology (NIST) has formulated standards for post-quantum cryptography, the Netherlands – or better yet, the EU – could take their own initiatives in that domain in the short term.

The time it will take to complete a large-scale migration to post-quantum cryptography and the risk of harvest-and-decrypt attacks underline the importance of introducing strong encryption of sensitive data in the short term, as well as using quantum-resistant cryptography wherever possible. The urgency of the situation is

a further reason not to wait for the results of the NIST competition, which might not be announced before 2024.

Start with the national crown jewels

A further reason to establish at least a minimum level of domestic IT enterprise is the need to ensure maximum security of ‘crown jewels’ such as state secrets, commercial secrets and other critical databases – for example through the use of strong forms of (post-quantum) cryptography. The government and suppliers of vital services must be able to buy products and services from trusted market actors who endorse important values such as privacy and autonomy. Although that does not necessarily mean that products and services would have to be bought from Dutch or European suppliers, that could help.

6.6 Conditions for exploiting opportunities

The following conditions have to be met to exploit the opportunities that new and existing technologies create for increasing cyber resilience in the Netherlands.

Improve the climate for innovation

A more favourable climate for innovation is needed to generate more domestic business activity in the field of IT. The government could help to create that climate by making tender procedures more attractive for innovative start-ups; by acting as launch customer; and by continuing to invest in knowledge development and collaboration between research institutes and the business community.

Sharper focus in research and innovation agenda

A more effective knowledge and innovation policy, with a sharper focus in the Dutch Cyber Security Research Agenda (NCSRA), would also help in achieving the goal of generating more business activity in the field of IT. In consultation with the business community and research institutes, the government should make more specific choices with respect to the knowledge areas in which the Dutch research institutes should take the lead – and then market the knowledge that is generated.

Given the knowledge that exists in the Netherlands with regard to post-quantum cryptography and the importance of guaranteeing maximum security for state secrets and the commercial secrets of vital suppliers, research into the further development and implementation of strong forms of encryption should obviously be encouraged.

It is also important for the Netherlands – and Europe – to continue promoting research for the further development and use of machine learning, distributed systems and safer hardware, products and communication protocols.

Influence of guidelines and standards

Given the enormous influence of international guidelines and standards for technologies on the general level of resilience, it is important for the Dutch government – or better yet, the EU – to participate in their drafting in international forums. One of the aims should be to ensure that they adequately reflect important European values such as privacy and autonomy.

The government as role model

As an important customer of digital products and services and a major service provider, the government should set the right example by always employing basic security measures such as 2-factor authentication, by using Privacy Enhancing Technologies in its services wherever possible, and by insisting that public news media attach digital signatures to their reports.

The government and the suppliers of vital services should also take the lead in stipulating stricter purchasing conditions for digital products and services. To increase market strength, the purchasing conditions should preferably be agreed at EU level.

To perform its exemplary role, it would appear that more central direction is required within the government, for example by delegating responsibility for central government’s cyber resilience to a single ministry.

Investment in expertise

Finally, exploiting the opportunities for increasing cyber resilience created by the new and existing technologies ultimately depends on the availability of sufficient expertise. Public authorities, suppliers of vital services, other enterprises and regulators must all possess the necessary capacity and expertise. Because of the chronic shortage of experts, greater investment in courses in cyber security is badly needed.

Bibliography

Ackerman, E. (2019). *Three Small Stickers in Intersection Can Cause Tesla Autopilot to Swerve Into Wrong Lane*. https://spectrum.ieee.org/cars-that-think/transportation/self-driving/three-small-stickers-on-road-can-steer-tesla-autopilot-into-oncoming-lane

AINED. (2018). *AI voor Nederland*. https://www.vno-ncw.nl/sites/default/files/aivnl_20181106_0.pdf

Algemene Rekenkamer. (2019a). *Digitale dijkverzwaring: cybersecurity en vitale waterwerken*. https://www.rekenkamer.nl/publicaties/rapporten/2019/03/28/digitale-dijkverzwaring-cybersecurity-en-vitale-waterwerken

Algemene Rekenkamer. (2019b). *Rijksoverheid heeft informatiebeveiliging en IT beheer nog niet op orde.* https://www.rekenkamer.nl/actueel/nieuws/2019/05/15/rijksoverheid-heeft-informatiebeveiliging-en-it-beheer-nog-niet-op-orde

Apple Support (2019). *About the Apple T2 Security Chip.* https://support.apple.com/en-us/HT208862

Automotive Insiders. (2018). *Branchemonitor Schadesector beschikbaar – Automotive Insiders*. https://automotiveinsiders.nl/onderzoek/

Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). *Cyber Resilience – Fundamentals for a Definition*. Advances in Intelligent Systems and Computing, 353, 311–316. https://doi.org/10.1007/978-3-319-16486-1_31

Blotenburg, S. (2018). *Startup lanceert minisatelliet: "Begin van een wereldwijd IoT-netwerk"*. https://www.rtlz.nl/business/artikel/4493866/hiber-internet-things-nanosatelliet-telecom-netwerk-iot

Boschma, R. (2005). *'Proximity and Innovation: A Critical Assessment'*, Regional Studies, Volume 39, Issue 1. https://www.tandfonline.com/doi/abs/10.1080/0034340052000320887

Boyle, A. (2018). *FCC approves SpaceX's plan to provide broadband services with Starlink satellites.* https://www.geekwire.com/2018/fcc-approves-spacexs-plan-provide-broadband-services-starlink-satellites/

Broekhuizen, K. (2018). *Noodklok over Nederlandse braindrain bij cybersecurity.* Financieel Dagblad. https://fd.nl/economie-politiek/1251379/noodklok-over-nederlandse-braindrain-bij-cybersecurity

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., … & Amodei, D. (2018). *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. arXiv:1802.07228 [cs]. http://arxiv.org/abs/1802.07228

Bulletproof. (2019). *Annual Cyber Security Report 2019*.

Bundesnetzagentur. (2019). *Bundesnetzagentur publishes key elements of additional security requirements for telecommunications networks*. https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2019/20190307_SL.html

Chella, V.K. (2018). *Cassandra serving netflix @ scale*. https://www.slideshare.net/VinayKumarChella/cassandra-serving-netflix-scale

CipherTrace Cryptocurrency Intelligence. (2018). *2018 Q3 Cryptocurrency Anti-Money Laundering Report* (p. 22).

Coll, L., & Simpson, R. (2016). *Connection and protection the Internet of Things and challenges for consumer protection*. https://www.consumersinternational.org/media/1292/connection-and-protection-the-internet-of-things-and-challenges-for-consumer-protection.pdf

Committee on Technical Assessment of the Feasibility and Implications of Quantum Computing, Computer Science and Telecommunications Board, Intelligence Community Studies Board, Division on Engineering and Physical Sciences, & National Academies of Sciences, Engineering, and Medicine. (2019). *Quantum*

Computing: Progress and Prospects (E. Grumbling & M. Horowitz, Red.). https://doi.org/10.17226/25196

Consumers International, ANEC, BEUC & ICRT. (2017). *Securing consumer trust in the Internet of Things*. https://www.consumersinternational.org/media/154809/iot-principles_v2.pdf

DARPA. (2008). *Prizes for Advanced Technology Achievements.* https://www.grandchallenge.org/grandchallenge/docs/DDRE_Prize_Report_FY07.pdf

Dcypher. (2018). *National Cyber Security Research Agenda III (NCSRA III) 2018*. https://www.dcypher.nl/national-cyber-security-research-agenda-iii-ncsra-iii-2018

De Jong, M. (2019). *Charging with a Tesla Model S/X*. *http://support.fastned.nl/hc/en-gb/articles/205418987-Charging-with-a-Tesla-Model-S-X*

Delcker, J. (2018). *Germany to launch US-style agency to develop cyberdefense*. https://www.politico.eu/article/germany-to-launch-darpa-style-agency-to-develop-cyber-defense/

Dell'Oro Group (2019). *Key Takeaways - Worldwide Telecom Equipment Market 2018*. http://www.delloro.com/delloro-group/telecom-equipment-market-2018

DG CONNECT (2019a). *Four EU pilot projects launched to prepare the European Cybersecurity Competence Network*. https://ec.europa.eu/digital-single-market/en/news/four-eu-pilot-projects-launched-prepare-european-cybersecurity-competence-network

DG CONNECT. (2019b). *The future is quantum: EU countries plan ultra-secure communication network*. https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network

Dignan, L. (2018). *Top cloud providers 2018: How AWS, Microsoft, Google, IBM, Oracle, Alibaba stack up*. https://www.zdnet.com/article/top-cloud-providers-2018-how-aws-microsoft-google-ibm-oracle-alibaba-stack-up/

Dobbe, R. & M. Stikker (2019). 'Vergeet China en Silicon Valley', *NRC Handelsblad* 13 & 14 april 2019.

EC Media Convergence and Social Media Unit 1.4. (2019). Tackling online disinformation. https://ec.europa.eu/digital-single-market/en/tackling-online-disinformation

Elias, T. (2014). *Parlementair onderzoek ICT-projecten bij de overheid*. https://www.tweedekamer.nl/kamerstukken/detail?id=2014Z17985&did=2014D36603

Elumalai, A., Sprague, K., Tandon, S., & Yee, L. (2018). *Ten trends redefining enterprise IT infrastructure*. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Modernizing%20IT%20for%20digital%20reinvention/Modernizing-IT-for-digital-reinvention-Collection-July-2018.ashx

ENISA. (2014). *Security Guide for ICT Procurement*. https://www.enisa.europa.eu/publications/security-guide-for-ict-procurement

ENISA. (2017). *Cybersecurity in the EU Common Security and Defence Policy (CSDP): Challenges and risks for the EU*. https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-eu-common-security-and-defence-policy-csdp-challenges-and-risks-for-the-eu

European Political Strategy Centre. (2019). *Rethinking Strategic Autonomy in the Digital Age*. https://ec.europa.eu/epsc/sites/epsc/files/epsc_strategic_note_issue30_strategic_autonomy.pdf

European Commission. (2018). *State of the Union 2018 – Cybersecurity: Commission proposes to invest in stronger and pioneering cybersecurity capacity in the EU*

European Commission. (2019a). *A common EU approach to the security of 5G networks*. https://ec.europa.eu/commission/news/common-eu-approach-security-5g-networks-2019-mar-26_en

European Commission. (2019b). *A definition of Artificial Intelligence: main capabilities and scientific disciplines.* https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines

Europol. (2018). *Internet Organised Crime Threat Assessment 2018*.

Finlayson, S. G., Chung, H. W., Kohane, I. S., & Beam, A. L. (2018). *Adversarial Attacks Against Medical Deep learning Systems*. arXiv:1804.05296 [cs, stat]. http://arxiv.org/abs/1804.05296

Flinkle, J., & Balu, N. (2018). *Under Armour says 150 million MyFitnessPal accounts breached*. Reuters. https://uk.reuters.com/article/us-under-armour-databreach-idUKKBN1H532W

Forum Standaardisatie (2019). *Lijst open standaarden.* https://www.forumstandaardisatie.nl/open-standaarden/lijst/verplicht

Fraze, D. (2017). *Cyber Grand Challenge (CGC).* https://www.darpa.mil/program/cyber-grand-challenge

Fried, O., Agrawala, M., Tewari, A., Zollhöfer, M., Finkelstein, A., Shechtman, E., … Theobalt, C. (2019). Text-based editing of talking-head video. ACM Transactions on Graphics, 38(4), 1–14. https://doi.org/10.1145/3306346.3323028

Fruhlinger, J. (2018). *The Mirai botnet explained: How IoT devices almost brought down the internet*. https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html

Gabbai, A. (2015). *Kevin Ashton Describes "the Internet of Things"*. https://www.smithsonianmag.com/innovation/kevin-ashton-describes-the-internet-of-things-180953749/

Global Cyber Security Capacity Centre - University of Oxford. (2016). *Cybersecurity Capacity Maturity Model for Nations (CMM)* - Revised Edition. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20revised%20edition_09022017_1.pdf

Google (2019). *IPv6*. Geraadpleegd 16 april 2019, van: https://www.google.com/intl/en/ipv6/statistics.html

Google. (2019). *Google Transparency Report*. https://transparencyreport.google.com/https/overview?hl=en

GreAT, & AMR. (2019). *Operation ShadowHammer*. https://securelist.com/operation-shadowhammer/89992/

Henry, C. (2018). *SpaceX won't seek U.S. rural broadband subsidies for Starlink constellation.* https://spacenews.com/spacex-wont-seek-u-s-rural-broadband-subsidies-for-starlink-constellation/

Hern, A. (2018*). Fake fingerprints can imitate real ones in biometric systems – research*. The Guardian. https://www.theguardian.com/technology/2018/nov/15/fake-fingerprints-can-imitate-real-fingerprints-in-biometric-systems-research

Higgins, K. (2017). *New Tool Debuts for Hacking Back at Hackers in Your Network*. https://www.darkreading.com/attacks-breaches/new-tool-debuts-for-hacking-back-at-hackers-in-your-network/d/d-id/1330121

Hill, M. (2017). *Behavioral Analytics in Cybersecurity*. https://www.infosecurity-magazine.com:443/editorial/behavioral-analytics-in/

Hilton, S. (2016). *Dyn Analysis Summary Of Friday October 21 Attack*. https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

Hijink, M. (2019). *Details van 5G-netwerk met Huawei blijven mistig*. https://www.nrc.nl/nieuws/2019/07/01/details-van-5g-netwerk-met-huawei-blijven-mistig-a3965775

Hooghiemstra, T. (2018). *Informationele zelfbeschikking in de zorg*. https://research.tilburguniversity.edu/en/publications/informationele-zelfbeschikking-in-de-zorg

Huawei Cyber Security Evaluation Centre. (2019). *Huawei cyber security evaluation centre oversight board: annual report 2019*. https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2019

ISACA. (2018). *State of Cybersecurity 2018*. https://cybersecurity.isaca.org/state-of-cybersecurity

ISC2. (2018). *Cybersecurity Workforce Study*. https://www.isc2.org:443/Research/Workforce-Study

IT Governance UK. (2019). *Cyber Resilience*. https://www.itgovernance.co.uk/cyber-resilience

ITU. (2017). *Global Cybersecurity Index*.

Jones, A. (2018). *Spacety a Chinese Startup Plans Launch of Four Satellites on October 29*. http://satnews.com/story.php?number=2063954306

Karataş, A., & Şahin, S. (2017). *A Review on Social Bot Detection Techniques and Research Directions*.

Kaska, K., Beckvard, H., & Minárik, T. (2019). *Huawei, 5G and China as a Security Threat* (p. 26). Tallin: NATO Cooperative Cyber Defence Centre of Excellence.

Kleinhans, J.-P. (2019). *5G vs. National Security*. https://www.stiftung-nv.de/sites/default/files/5g_vs._national_security.pdf

Lapowsky, I. (2018). Facebook Exposed 87 Million Users to Cambridge Analytica. *Wired*. https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica/

Liao, S.-K. et al. (2017). *Satellite-to-ground quantum key distribution*. Nature, 549(7670), 43–47. https://doi.org/10.1038/nature23655

Lueth, K.L. (2018). *State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating*. https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

Lysne, O. (2018). *The Huawei and Snowden Questions: Can Electronic Equipment from Untrusted Vendors be Verified? Can an Untrusted Vendor Build Trust into Electronic Equipment?* https://www.springer.com/de/book/9783319749495

Major, M. (2018). *A Look at How Easily 3D-Printed Heads Can Hack Facial Recognition*. https://interestingengineering.com/a-look-at-how-easily-3d-printed-heads-can-hack-facial-recognition

McAfee (2018). *McAfee Labs 2019 Threats Predictions Report.* https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/mcafee-labs-2019-threats-predictions/

McLean, V. (2019). *Iridium Declares Victory; $3 Billion Satellite Constellation Upgrade Complete*. http://www.spacedaily.com/reports/Iridium_Declares_Victory_3_Billion_Satellite_Constellation_Upgrade_Complete_999.html

Mehta, I. (2019). *Samsung's new AI can create talking avatars with a single photo*. https://thenextweb.com/artificial-intelligence/2019/05/23/samsungs-new-ai-can-create-talking-avatars-with-a-single-photo/

Microsoft (2014). *Microsoft Security Advisory 2862973*. https://docs.microsoft.com/en-us/security-updates/securityadvisories/2014/2862973

Ministerie van Binnenlandse Zaken en Koninkrijkrelaties. (2014). *Open overheid*. https://www.rijksoverheid.nl/onderwerpen/digitale-overheid/open-overheid

Ministerie van Economische Zaken en Klimaat. (2019). *Missies voor het* topsectoren- en innovatiebeleid. https://www.rijksoverheid.nl/documenten/publicaties/2019/04/26/missies

Ministerie van Economische Zaken en Klimaat, Ministerie van Justitie en Veiligheid. (2018). Roadmap Digitaal Veilige Hard- en Software. https://www.rijksoverheid.nl/documenten/rapporten/2018/04/02/roadmap-digitaal-veilige-hard-en-software

Ministerie van Justitie en Veiligheid. (2019). *Kamerbrief Maatregelen bescherming telecomnetwerken en 5G.* https://www.rijksoverheid.nl/documenten/kamerstukken/2019/07/01/kamerbrief-maatregelen-bescherming-telecomnetwerken-en-5g

Ministerie van Veiligheid en Justitie. (2013). *Nationale Cyber Security Strategie 2*. https://www.rijksoverheid.nl/documenten/rapporten/2013/10/28/nationale-cyber-security-strategie-2

Minister van Veiligheid en Justitie, & Minister van Economische Zaken. (2016). Kabinetsstandpunt encryptie. Geraadpleegd 7 augustus 2019: https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail

Modderkolk, H. (2019). *Grapperhaus stuurt na Volkskrant-publicatie alsnog kritisch AIVD-advies over 5G naar de Kamer.* https://www.volkskrant.nl/gs-b820d00f

Morris, S. (2018). *Cloud Computing Tops List of Emerging Risks*. Geraadpleegd 15 april 2019: https://www.gartner.com/smarterwithgartner/cloud-computing-tops-list-of-emerging-risks/

Mozilla (2019). *Security vulnerabilities fixed in Thunderbird 60.5.1.* https://www.mozilla.org/en-US/security/advisories/mfsa2019-06/

NCTV. (2018). Factsheet weerbare vitale infrastructuur.

NCTV. (2019a). Cybersecuritybeeld Nederland CSBN 2019.

NCTV. (2019b). *Uw Eigen Veiligheid*. https://www.nctv.nl/binaries/WEB_117467_NCTV_UwEigenVeiligheid_A5_tcm31-371131.pdf

NIST CSRC (2019). *Workshops and Timeline - Post-Quantum Cryptography*. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Workshops-and-Timeline

Norrman, K., Nakarmi, P., & Fogelström, E. (2018). *5G security - enabling a trustworthy 5G system [White paper]*. https://www.ericsson.com/en/white-papers/5g-security---enabling-a-trustworthy-5g-system

Olsthoorn, P. (2017). *Fox-IT moet Nederlands blijven van Defensie*. https://www.netkwesties.nl/957/fox-moet-nederlands-blijven-defensie.htm

OpenAI. (2019). *Better Language Models and Their Implications*. https://openai.com/blog/better-language-models/

Ortiz, E. (2018). *Marriott says data breach compromised info of up to 500 million guests*. NBC News. https://www.nbcnews.com/tech/security/marriott-says-data-breach-compromised-info-500-million-guests-n942041

OWASP IoT Security Team. (2018). *OWASP IoT Top 10 2018*. https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10

Pal, G. (2018, april 2). *Secdevops or devsecops or devops next-generation (NG) – What is your take on devops?* https://www.csoonline.com/article/3267633/secdevops-or-devsecops-or-devops-next-generation-ng-what-is-your-take-on-devops.html

Patiëntenfederatie Nederland. (2019). *Het Patiëntgeheim*. https://www.rijksoverheid.nl/documenten/rapporten/2019/01/17/het-patientgeheim

Pultarova, T. (2017). *Picture of Health: Can AI Eye Scan Reveal What Ails You?* https://www.livescience.com/61171-artificial-intelligence-eye-scan.html

Raad voor de Leefomgeving en Infrastructuur. (2018). *Stroomvoorziening onder digitale spanning*. https://www.rli.nl/publicaties/2018/advies/stroomvoorziening-onder-digitale-spanning

Rathenau Instituut (2017). *Een nooit gelopen race – Over cyberdreiging en versterking van weerbaarheid*. The Hague (authors: Munnichs, G., M. Kouw & L. Kool). https://www.rathenau.nl/nl/digitale-samenleving/een-nooit-gelopen-race

Rathenau Instituut (2018a). *Bedrijf zoekt universiteit – De opkomst van strategische publiek-private partnerships in onderzoek.* The Hague (authors: Tjong Tjin Tai, S.Y., J. van den Broek, T. Maas, T. Rep & J. Deuten). https://www.rathenau.nl/nl/vitale-kennisecosystemen/bedrijf-zoekt-universiteit

Rathenau Instituut (2018b). *Digitalisering van het nieuws – Online nieuwsgedrag, desinformatie en personalisatie in Nederland* The Hague. (authors: Keulen, I. van, I. Korthagen, P. Diederen & P. van Boheemen). https://www.rathenau.nl/nl/digitale-samenleving/digitalisering-van-het-nieuws

Rathenau Instituut (2019a). *Kennis in het vizier – De gevolgen van de digitale wapenwedloop voor de publieke kennisinfrastructuur*. The Hague (authors: Diercks, G., J. Deuten & P. Diederen). https://www.rathenau.nl/nl/vitale-kennisecosystemen/kennis-het-vizier

Rathenau Instituut (2019b). *Cyberspace zonder conflict – De zoektocht naar de-escalatie van het internationale informatieconflict.* The Hague (authors*:* Hamer, J., R. van Est & L. Royakkers). https://www.rathenau.nl/nl/digitale-samenleving/cyberspace-zonder-conflict

Rathenau Instituut (2019c). 'Zo brengen we AI in de praktijk vanuit Europese waarden.' Website Rathenau Instituut, 19 maart 2019 (authors: Jong, R. de, L. Kool & R. van Est) https://www.rathenau.nl/nl/digitale-samenleving/zo-brengen-we-ai-de-praktijk-vanuit-europese-waarden

Rathenau Instituut (2019d). *Gezondheid centraal – Zorgvuldig data delen in de digitale samenleving*. The Hague (authors: Niezen, M., R. Edelenbosch, L. van Bodegom & P. Verhoef). https://www.rathenau.nl/nl/maakbare-levens/gezondheid-centraal

RVO (2017). *3e tender SBIR Cyber Security*. https://www.rvo.nl/subsidies-regelingen/sbir/overzicht-sbir-oproepen/3e-tender-sbir-cyber-security

Saffman, M. (2016). *"Quantum Computing with atomic qubits and Rydberg interactions: progress and challenges,"* Journal of Physical B: Atomic, Molecular and Optical Physics, 49, 202001

Schiffer, A. (2017). *How a fish tank helped hack a casino*. https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/

Schneier, B. (2018). *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World* (1 edition). New York: W. W. Norton & Company.

Scott, J. (2018). *Australia Passes Law Targeting WhatsApp and Signal*. https://www.bloomberg.com/news/articles/2018-12-06/australia-moves-toward-passing-law-targeting-whatsapp-signal

Shafi, M., Molisch, A. F., Smith, P. J., Haustein, T., Zhu, P., Silva, P. D., … Wunder, G. (2017). *5G: A Tutorial Overview of Standards, Trials, Challenges, Deployment, and Practice*. IEEE Journal on Selected Areas in Communications, 35(6), 1201–1221. https://doi.org/10.1109/JSAC.2017.2692307

Sheridan, K. (2018). *Google Engineering Lead on Lessons Learned From Chrome's HTTPS Push*. Dark Reading.

SIDN fonds (2018). *Dowse*. https://www.sidnfonds.nl/projecten/dowse

Solid (2019). *How It Works.* https://solid.inrupt.com/how-it-works

sp.a. (2018). "Trump heeft een boodschap voor alle Belgen... #Klimaatpetitie https://t.co/Kf7nIaDOKj" Twitter. https://twitter.com/sp_a/status/998089909369016325

SSC-ICT (2019). *In het digitale hart van de Rijksoverheid*. https://www.ssc-ict.nl/actueel/nieuws/2019/soc.aspx

Stewart, R. (2019). *Digital signatures in PDF applications exploited by researchers*. https://cyware.com/news/digital-signatures-in-pdf-applications-exploited-by-researchers-2df0bc66

STOA. (2017). *Achieving a sovereign and trustworthy ICT industry in the EU*. http://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2017)614531

Studiegroep Informatiesamenleving en Overheid. (2017). *Maak Waar!* https://www.rijksoverheid.nl/documenten/rapporten/2017/04/18/rapport-van-de-studiegroep-informatiesamenleving-en-overheid-maak-waar

Stupp, C. (2018a). *National governments reach breakthrough deal on voluntary cybersecurity certification*. https://www.euractiv.com/section/cybersecurity/news/national-governments-reach-breakthrough-deal-on-voluntary-cybersecurity-certification/

Stupp, C. (2018b). *Plan for EU cybersecurity certification receives Parliament approval*. https://www.euractiv.com/section/cybersecurity/news/plan-for-eu-cybersecurity-certification-receives-parliament-approval/

Tao, L. (2018). *Japan latest country to exclude Huawei, ZTE from 5G roll-out*. https://www.scmp.com/tech/tech-leaders-and-founders/article/2177194/japan-decides-exclude-huawei-zte-government

TechNavio. (2017). *Global Security Information and Event Management Market 2017-2021.* https://www.technavio.com/report/global-it-security-global-security-information-and-event-management-market-2017-2021

Van der Gaast, S., Xu, H., Koonen, T., & Tangdiongga, E. (2018). Optical Wireless Communication: Options for extended spectrum use [Rapport]. https://www.agentschaptelecom.nl/documenten/rapporten/2018/02/07/onderzoek-lifi

Van der Grient, R., & Konings, F. (2018). *Nationaal Cybersecurity Bewustzijnsonderzoek 2018*. https://www.alertonline.nl/cybersecurityonderzoek

Van der Laan, S. (2019). *Nederlandse ziekenhuizen kwetsbaar voor cyberaanvallen*. https://www.elsevierweekblad.nl/kennis/achtergrond/2019/02/nederlandse-ziekenhuizen-kwetsbaar-voor-cyberaanvallen-163181w/

Van Eeten, M. (2017). *Patching security governance: an empirical view of emergent governance mechanisms for cybersecurity*. Digital Policy, Regulation and Governance, 19(6), 429–448. https://doi.org/10.1108/DPRG-05-2017-0029

Verhagen, L. (2019). *Overal hangen beveiligingscamera's. Hoe betrouwbaar zijn de interpretaties die computers maken van de beelden?* Geraadpleegd 7 augustus 2019, van: De Volkskrant website: https://www.volkskrant.nl/gs-bef1fd8b

Verizon (2018). *Data Breach Investigations Report*. https://enterprise.verizon.com/resources/reports/dbir/

Werken bij de Overheid (2019). *Manager Release • Ministerie van Defensie*. Geraadpleegd 15 april 2019, van: https://www.werkenbijdeoverheid.nl/vacatures/manager-release-DEF-2019-0859

Whittaker, Z. (2019). *New flaws in 4G, 5G allow attackers to intercept calls and track phone locations*. http://social.techcrunch.com/2019/02/24/new-4g-5g-security-flaws/

Wlodarczak, P. (2017). *Cyber Immunity - A Bio-Inspired Cyber Defense System*. 199–208. https://doi.org/10.1007/978-3-319-56154-7_19

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (1 edition). New York: PublicAffairs.

Appendix 1: Glossary of terms

This report discusses the following new technologies.

Technology	Explanation
2-factor authentication	Method whereby users have to take two steps to prove that they are who they say they are.
5G networks	The fifth generation of wireless or mobile systems. They can transmit data in larger quantities and with less delay, for example. This can improve the functionality of many digital applications.
Automatic response systems	Systems that respond independently to incidents.
Behavioural analytics	A method of analysing the behaviour of users in digital systems, for example to identify unusual behaviour.
Biometric identification	A form of identification, which is often used for access control, based on a person's biological features, such as a fingerprint or iris.
Botnet	A network consisting of a large number of digital devices that can be operated simultaneously by a single actor, usually with the aim of causing damage without the owners or the devices being aware of it.
Cloud technology	Services provided by software companies whereby users make use of the supplier's systems.
Deepfakes	Visual material that has been manipulated by machine learning software in such a way that it can barely be distinguished from authentic.
Deep learning	Form of machine learning based on neural networks – inspired by the biology of our brain – and which combines various layers of information.
Desktop-as-a-service	A service that simulates and provides practically the entire user experience of a traditional desktop computer in the form of a cloud service.
Encryption; homomorphic encryption	Digital encryption; with homomorphic encryption users can process encrypted data without having to decrypt them.
Distributed systems	A coherent network of independent computer systems that performs functions for the user as a coherent system, without any central point of control
Harvest and decrypt strategy	A decryption strategy that is based on the assumption that in the (near) future it will be possible to crack encryption methods that are in common use at present. To that end, encrypted data are being collected now.

IMSI-*catching*	A method by which an attacker can intercept communication on a mobile telephone/communication network.
Interference	The interaction or counteraction of different waves at the same time and location.
Internet of Things (IoT)	The sum of the devices connected to the internet.
IP protocol	A network protocol which enables computers in a network to communicate with one another.
Lawful interception	Statutory rule that permits telecommunication to be tapped.
LiFi	Data transmission technology based on rapidly flickering LED light.
Quantum computer	Computer whose computing power is derived from the properties of quantum physics.
Quantum communication	Data transmission technology based on quantum physics.
Quantum computing	The exploitation of the computing power of a quantum computer.
Machine learning	Algorithms with a certain learning capacity. Generally based on the comparison of data with a dataset or learned patterns. The technology relies heavily on statistics.
multifactor-authentication	Method of authentication that combines different methods to establish authenticity.
Named Data Networking (NDN)	Network protocol that takes the security of data as its point of departure.
network slicing	The possibility that 5G offers to separate data streams.
NIST competition	In this report, this term refers to a competition to develop, evaluate and standardise one or more quantum-proof cryptographic algorithms.
post-quantum cryptography	An encryption method that is strong enough to withstand the computing power of a quantum computer.
Open data standards and software	Public standards for databases and software with public source code, which, depending on the degree of openness, can be used, processed and disseminated by everyone.
Privacy Enhancing Technologies (PETs)	Technologies that enhance the user's privacy, for example through the use of a strong form of encryption and by minimising the collection of data.
secure multi-party computation	Computing method that enables multiple parties to share information with each other, without the data being traceable to a specific party.
Single Point of Failure	The risk that arises when one or more crucial functions of a process are delegated to a single party with the result that a malfunction at that party leads to disruption of the entire process.
superposition	The quantum mechanical phenomenon that a system can be in two different positions at once.

vendor lock-in	A situation where a user is so dependent on a single supplier that the costs of switching to another supplier have become prohibitive.
wearables	Mobile digital gadgets that are worn on the body.

Appendix 2: Participants interviews

Jaya Baloo, KPN

Maarten Bodlaender, Philips

Hans Bos, Rijkswaterstaat

Jeremy Butcher, Fox-IT

René van Buuren, Thales

Frank Fransen, TNO

Wil van Gemert, Europol

Koen Gijsbers

Frank Groenewegen, Fox-IT

Allard Kernkamp, TNO

Raymond Kleijmeer, De Nederlandsche Bank

Cees de Laat, University of Amsterdam

Erwin Mededorp, Dutch Safety Board

Jasper Nagtegaal, Radiocommunications Agency Netherlands

Bert Jan te Paske, TNO

Roeland Reijers, University of Amsterdam

Hessel Schut, Team High Tech Crime

Dimitri Tokmetzis, De Correspondent

Jos Weyers, Tennet

Paul Wijninga, Radiocommunications Agency Netherlands

Rejo Zenger, Bits of Freedom

Annemarie Zielstra, TNO

Lodewijk van Zwieten, Dutch Public Prosecution Service

AIVD

Appendix 3: Participants workshops

Maarten Bodlaender, Philips

Pieter van Boheemen, Rathenau Institute

Mark Crooijmans, Municipality of Amsterdam

Gijs Diercks, Rathenau Institute

Sander van Dorst, Ministry of Defence

Jeroen Gaiser, Rijkswaterstaat

Jurriën Hamer, Rathenau Institute

Elly van den Heuvel, Cyber Security Council

Andreas Hülsing, University of Eindhoven

Bart Jacobs, Radboud University Nijmegen

Linda Kool, Rathenau Institute

Michiel Leenaars, Internet Society

Geert Munnichs, Rathenau Institute

Luisella ten Pierik, Stedin

Remco Poortinga, SURF

Inge Quest, NCTV

Melanie Rieback, Radically Open Security

John Sinteur, Radically Open Security

Harold Vermanen, Microsoft

Anouk Vos, RevNext/Radically Open Security

René Vroom, Radiocommunications Agency Netherlands

Sandra van der Weide, Ministry of Economic Affairs and Climate Policy

Jos Weyers, Tennet

Paul Wijninga, Radiocommunications Agency Netherlands

Ministry of Justice and Security

Open Access

The Rathenau Instituut has an Open Access policy. Reports and background studies, scientific articles and software are published publicly and free of charge. Research data are made freely available, while respecting laws and ethical norms, copyrights, privacy and the rights of third parties.

Contact

Rathenau Instituut

Anna van Saksenlaan 51

P.O. Box 95366

2509 CJ The Hague

The Netherlands

+31 70 342 15 42

info@ Rathenau.nl

www.Rathenau.nl

Publisher: Rathenau Instituut

Board of the Rathenau Instituut

The Rathenau Institute supports the formation of public and political opinion on socially relevant aspects of science and technology.It conducts research on this subject and organises debates on science, innovation, and new technology.

Rathenau Instituut