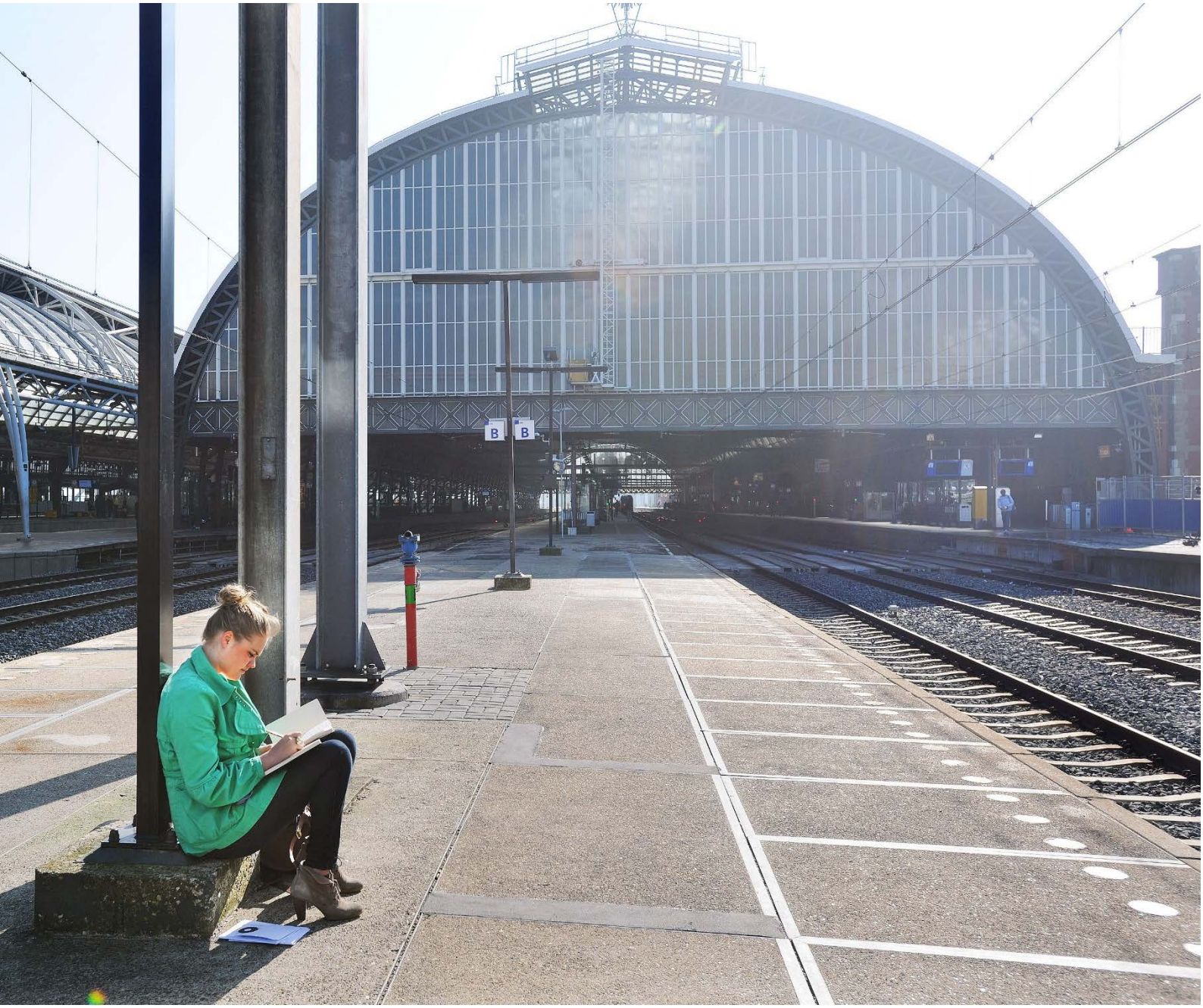
Rathenau Instituut

Cyberspace without conflict

The search for de-escalation of the international information conflict



Report

Authors

Jurriën Hamer, Rinie van Est & Lambèr Royakkers, with the assistance of Nicole Alberts

Infographics
Rikkers Infographics

Cover photo
Amsterdam Central Station after a computer crash had brought train services to a standstill, 2012. Photo: Guus Dubbelman / Hollandse Hoogte

Preferred citation:
Hamer, J., R. van Est, L. Royakkers, with the assistance of N. Alberts (2019). *Cyberspace without conflict – The search for de-escalation of the international information conflict*. The Hague: Rathenau Institute

Foreword

Cyber attacks are a daily occurrence and sometimes have major consequences. Russia has carried out cyber attacks in Ukraine. China hacks and spies on foreign companies. And the United States has used cyberspace to carry out sabotage. As a result, we find ourselves in a complex, unpredictable and threatening international situation. There are also risks for the Netherlands, where international hackers have attacked targets including hospitals and the Port of Rotterdam. This report considers what the Netherlands can do, together with other countries, to prevent the situation from escalating.

The Rathenau Institute's task is to support political decision-making and the public debate about technology's impact on society. That mandate also encompasses the threat of cyber attacks. This report follows on from previous studies, including our report *A never-ending race*. Our hope is that with this report the public can understand what is happening in cyberspace and join in the debate with experts and politicians.

This report provides an overview of the international situation with a focus on the build-up of cyber weapons and the diplomatic policies of countries. From literature and interviews it emerged that states have not made any clear agreements on cyber attacks; we refer to this situation as an information conflict. That is what makes the current international situation so risky and worrying. If the Netherlands wishes to contribute to a de-escalation of this information conflict, five things are needed: international cooperation; clear agreements at international level; coordination of the build-up of cyber weapons; cooperation with companies; and finally, involvement of the general public in the government's decision-making on cyber security.

Particularly in an age of international conflicts, it is useful to keep the strength of citizens in mind. During the Cold War many people were afraid of 'the bomb'. That fear sparked a debate about the use of nuclear weapons, which demonstrated not only that citizens need the government to protect them, but also that the public must demand action from the government. In the information conflict, citizens are more directly involved and the military aspect is more closely intertwined with society. Together we can search for a conflict-free cyberspace. To do that, citizens and their governments have to know what is happening and what options are available to us. We hope that the findings of this study will help to achieve that goal.

Melanie Peters
Director, Rathenau Institute

Summary

A growing number of countries are capable of carrying out cyber attacks that cause enormous damage to businesses, individuals and government institutions.[1] Almost every country also uses cyber weapons. They spy on one another and try to infiltrate each other's digital systems; some states even engage in cyber sabotage or spread disinformation. A new type of conflict is being fought with information technology, which we refer to in this report as an 'information conflict'.

How can the Netherlands contribute to a de-escalation of this information conflict? This report suggests five possible solutions. It calls for the involvement of the public in the political and public debate about international cyber security, since it is the country's citizens who will be affected most by cyber attacks. At the same time, they are also the ones who can call on governments and politicians to work towards de-escalation.

This report expands on previous reports by the Rathenau Institute, including *A never-ending race*, *Digitalisering van het nieuws* [Digitalisation of the news] and *Just ordinary robots: Automation from love to war*.

The nature of cyber attacks
This report first defines what cyber attacks are and compares them with conventional military aggression. The analysis produces the following picture.

Cyber attacks can usually be carried out from a great distance, can spread extremely quickly and are sometimes difficult to detect – especially if they involve highly sophisticated espionage or high-quality falsification of images and sound. Cyber attacks are sometimes even offered as a service. Cyber attackers range from intelligence services to cyber criminals, and seldom have to fear any repercussions, such as facing trial.

At the same time, cyber attacks are not necessarily more harmful than conventional attacks. In fact, cyber attacks are seldom intended to cause serious physical damage and can frequently be neutralised. Once it has been identified, malware can automatically be detected and attacks can be repulsed, provided suppliers and users keep their software systems up to date.

1 This translated report has been updated to include the most important developments since the original report was released on 25 april 2019.

Consequently, while the emergence of cyber attacks creates serious security risks, there are ways of mitigating the damage.

Three rungs on an escalation ladder

Cyber attacks are an everyday occurrence. This report provides an overview of who carries them out, with the emphasis on the role of the major cyber powers – the United States, Russia and China – but also considering the role of the Netherlands and a number of other European countries. It does so by positioning the activities on a so-called cyber escalation ladder. The ladder has three rungs:

1. A rung characterised by **cyber peace**, a situation in which countries do not use digital tools for espionage or engage in sabotage or disseminating disinformation.
2. A rung characterised by **information conflict**, a situation in which states resort to cyber espionage and, sometimes, spreading disinformation and sabotaging digital systems.
3. A rung characterised by **cyber-physical war**, a situation in which the damage caused by states is so serious that one could speak of armed attacks. It should be noted in this context that during a cyber-physical war, every type of cyber attack is in fact covered by international law, not just the few cyber attacks that actually constitute an armed attack.

Most actions currently undertaken by influential states fall within the scope of what we describe above as the information conflict. In peacetime, countries build up their cyber security and try to infiltrate the digital systems of other countries as secretely as possible. Russia is also actively spreading disinformation. That is a strategy that other autocratic countries do not yet appear to employ on a large scale, at least not in relation to other countries, but it fits in seamlessly with their desire to control, censor and manipulate the information that reaches their populations. There are also a number of examples of serious cyber sabotage, such as Operation Olympic Games, which has been attributed to Israel and the United States, and the WannaCry attack, which has been attributed to North Korea. Up to now, cyber attacks have never instigated a cyber-physical war; in that respect, there is no ‘cyber war’. However, cyber weapons are increasingly an element of warfare, as can be clearly seen from the conflict in Ukraine.

International cooperation

The continuing information conflict creates a need for international diplomacy and agreements. In this report, we therefore review the cooperation that exists in this field. In various international and regional bodies states are trying to take steps to create a safe and free digital world.

Although there has been some success at the regional level, especially within the EU, states have not yet succeeded in making binding global agreements on cyber attacks. That does not mean there are no rules governing cyber attacks, but because these attacks seldom exceed the threshold of an ‘armed attack’ which activates international humanitarian law, there are only general principles, such as the prohibition of the use of force. And at present those principles are open to various interpretations.

Five possible solutions for de-escalation

The information conflict could escalate. As our report shows, the current international situation is risky and worrying. On the basis of our findings, we formulate five possible solutions that could contribute to a de-escalation of this conflict.

1. **Continue cooperating to increase international cyber security**
   Important international initiatives have been taken to improve the security of cyberspace, such as the IMPACT coalition, the European network of Cyber Emergency Incident Response Teams and the NATO cyber exercises. The Netherlands has joined them. These collaborative efforts are and will remain very important.

2. **Conclude clear international agreements on de-escalation in relation to cyber sabotage, disinformation and cyber espionage**
   Although the Netherlands and other countries have taken important steps to formulate international rules governing cyber attacks, such as the Tallinn Manual and the Paris Call for Trust and Security in Cyberspace, there are very few binding rules that relate specifically to the information conflict. One option might be a cyber convention.

3. **Ensure that the cyber arsenal is responsibly managed**
   It is important to prevent further proliferation of cyber weapons. That calls for international coordination of the build-up of cyber weapons and for effective collaboration with technology companies in removing vulnerabilities in their products. This collaboration also calls for as much transparency as possible, especially among allies.

4. **Protect the independence of technology companies**
   Technology companies perform a crucial role in creating a secure digital environment. They close the holes in their software and can bring robust digital applications onto the market. It is important to help companies to make their operations as secure as possible. Governments are taking a risk if they insist that companies secretly weaken the security of their products.

Governments must therefore regulate both the technology and technology companies in a sensible manner.

5. Invest in a debate on international cyber security

The information conflict must be subjected to a democratic debate: it is citizens who are particularly affected by cyber attacks. Citizens thus must be resilient. It is also up to citizens to give direction to the digital future. De-escalation of the information conflict therefore calls for a public and political debate.

Content

Foreword 3

Summary 4

Content 8

Introduction 10
1.1 The emergence of cyber attacks 10
1.2 A complex and threatening international situation 11
1.3 The cyber escalation ladder 13
1.4 Definitions 14
1.5 The questions to be answered 16
1.6 The research method 16

2 Offensive cyber capabilities 18
2.1 Cyber espionage 19
2.1.1 Technology 19
2.1.2 Comparison with conventional espionage 21
2.1.3 Resilience 22
2.2 Cyber sabotage 24
2.2.1 Technology 24
2.2.2 Comparison with conventional weapons 25
2.2.3 Resilience 27
2.3 The dissemination of disinformation 29
2.3.1 Technology 29
2.3.2 Comparison with conventional propaganda 31
2.3.3 Resilience 31
2.4 Conclusion 33

3 The information conflict 35
3.1 The United States 35
3.1.1 In brief 35
3.1.2 Strategic development 38
3.2 Russia 42
3.2.1 In brief 42
3.2.2 Strategic development 44
3.3 China 46
3.3.1 In brief 46

3.3.2 Strategic development ... 46
3.4 The Netherlands and other European countries ... 50
3.4.1 In brief ... 50
3.4.2 Strategic development ... 50
3.5 The international attitude of the states: an overview ... 53
3.6 The cyber escalation ladder ... 54
3.6.1 The information conflict ... 54
3.6.2 Cyber peace and cyber-physical warfare ... 55
3.7 Conclusion ... 57

4 International cooperation for a safe and free digital world ... 60
4.1 Worldwide organisations ... 60
4.1.1 United Nations (UN) ... 60
4.1.2 International Telecommunication Union (ITU) ... 62
4.1.3 Public-private global alliances ... 63
4.2 Regional organisations ... 67
4.2.1 European Union (EU) ... 67
4.2.2 North Atlantic Treaty Organisation (NATO) ... 71
4.2.3 The Group of Seven (G7) ... 75
4.2.4 Shanghai Cooperation Organisation (SCO) ... 76
4.2.5 Organisation for Security and Cooperation in Europe (OSCE) 76
4.2.6 Five Eyes alliance and SIGINT Seniors ... 77
4.3 The state of international regulation ... 78
4.3.1 The nature of international law ... 78
4.3.2 Cyber attacks as violations of state sovereignty ... 79
4.3.3 International law that requires considerable interpretation ... 83
4.4 Conclusion ... 83

5 Conclusion ... 86
5.1 The international situation ... 86
5.2 Five possible solutions for de-escalation ... 90
5.2.1 Continue the cooperation to enhance international cyber security ... 90
5.2.2 Make clear international agreements for de-escalation in the areas of cyber sabotage, disinformation and cyber espionage 91
5.2.3 Ensure that the cyber arsenal is managed responsibly ... 94
5.2.4 Protect the independence of technology companies ... 95
5.2.5 Engage in a public debate on international cyber security ... 95

Bibliography ... 97

Introduction

1.1 The emergence of cyber attacks

Imagine that the employees of the Dutch Tax and Customs Administration arrive in the office on Monday morning and find the following message written in bold on their screens:

'YOUR COMPUTER HAS BEEN HACKED BY THE MOTHERLAND WARRIORS'

Their computers have been hacked and the hackers appear to have gained access to sensitive tax data. And it is not only the Tax Administration that has been hit: the 'Motherland Warriors' have also attacked numerous other sectors in society. Banks' online services have crashed under the strain of heavy cyber attacks. Telecom companies have also been infiltrated. The Dutch oil and gas exploration and production company NAM is unable access its supply data. To cap it all, the online environment of hospitals has been hijacked. The threat is always the same: unless economic sanctions against Russia are lifted immediately, essential information will be deleted from the computer systems and private information will be disclosed. Although nothing can be proved with certainty, there are strong indications that the attacks were launched from Russia.

This is not a fanciful scenario. It is more realistic than ever since the technology exists to carry out all of the attacks in the example. In point of fact, these types of attack have all been carried out at one time or another:

- In 2012, Saudi Aramco, one of the world's largest oil companies, took all of its services offline for five months after it had been attacked by a group calling itself Cutting Sword of Justice. The attack was attributed to Iran (Iasiello 2015, Sanger 2018).
- From 2011 until 2013, the Belgian telecom company Belgacom (now called Proximus) was hacked (Boffey 2018). Hackers reportedly gained access to communication within NATO, the European Council, the European Commission and the European Parliament. The Belgian public prosecutor pointed to the British intelligence service GCHQ as the culprit.
- In 2015, the data of more than 700,000 citizens were stolen when the federal tax administration in the United States, the Internal Revenue Service, was hacked (Crawford 2016). The identity of the perpetrators is not known.

- In the summer of 2017, hospitals throughout Europe, and particularly in the United Kingdom, were infected by the Wannacry malware, which hijacked valuable data (Ehrenfeld 2017). The attack was attributed to North Korea (Sanger 2018).
- And at the beginning of 2018, the networks of the ING and ABN Amro banks were disrupted by a nasty Distributed Denial of Service (DDoS) attack, which was probably carried out by Jelle S., an 18-year-old youth (Modderkolk 2018).

1.2 A complex and threatening international situation

Countries (or 'state actors') have a steadily expanding range of possibilities for carrying out sabotage, espionage and manipulation via cyberspace. For example, the United States has carried out major cyber attacks in the past and appears to be increasingly willing to use its extensive collection of digital weapons (Sanger 2018, United States Cybercommand 2018b). China hacks and spies on foreign companies in order to steal lucrative economic and military secrets (Klimburg 2017). And Russia has carried out major cyber attacks in Ukraine and has tried to infiltrate American power stations (Sanger 2018, Klimburg 2017).

This has created a complex, unpredictable and threatening international situation. Meanwhile, the global powers have all established military cyber commands and reformed their intelligence services. In some states there are close ties between government agencies and patriotic or – as in Russia – criminal hackers (Klimburg 2017). In the process, countries often operate beneath the radar and can disguise cyber attacks in such a way that it is sometimes difficult to establish which 'cyber actor' is responsible for a specific attack.

States no longer intervene solely by land, by sea, from the air or in space. Cyberspace is called the fifth dimension in which states, armed with viruses, ransom software and secret backdoors, defend their interests (NATO 2016b, The Economist 2010). In this new world, the Netherlands must be able to safeguard its interests, including security, prosperity and protecting the democratic rule of law.[2]

A number of steps have already been taken in this regard. For example, the Netherlands has also established a military cyber command, whose task is to gather intelligence, defend the country's networks and carry out cyber attacks. The military intelligence service MIVD and the general intelligence service AIVD can also conduct cyber operations. Dutch government agencies, companies, civil-society organisations and citizens have also been striving for years to ensure that

2 The literature and policy documents also refer in this context to 'vital interests'. 'See Ducheine 2018.

their cyber security provides effective protection against attacks. Institutions in the Netherland must ensure that it is difficult to attack them and that it is easy to repair any damage that may be caused. The Rathenau Institute discussed this issue at length in its report *A never-ending race* (Munnichs et al. 2017). The institute has also published research on the digitisation of the news, indicating how the Dutch government can increase society's resilience to the spread of disinformation (Van Keulen et al. 2018).

But what is the Netherlands' position in the international arena when it is likely that another state is behind a cyber attack? Should it retaliate in kind, together with allies, for example by attacking the Russian tax authorities? Would this be regarded as an 'act of war' (AIV CAVV 2011)? Or is it advisable to employ alternative, more diplomatic measures? While there is growing expertise and policy-making in the field of cyber security, this trend is less pronounced with respect to the international use of cyber capabilities (Van der Meer 2018b).

How can the Netherlands help to ensure that countries develop, regulate and use cyber capabilities in a correct manner? That is the question this report tries to answer. To that end, we review the background to offensive cyber capabilities and the international environment in which these capabilities are acquired and used. We also consider, in light of the characteristics of cyber attacks, the legal rules that currently apply to offensive cyber capabilities. In the process, we also look at international humanitarian law or humanitarian law of war (sometimes also referred to as the law of war). That law prescribes what conduct of parties to a conflict is permissible or otherwise in war situations. In that respect, the report reflects the ambition of the Netherlands and other European countries, such as the United Kingdom and Germany, to embed cyber capabilities in clear international regulatory frameworks (UK Government 2016, German Federal Ministry of the Interior 2011, Ministry of Foreign Affairs 2017).

How to deal with cyber capabilities is a matter of great public importance. The Dutch reaction to cyber attacks from abroad that cause damage and disruption can therefore not be left entirely to experts: it is important that citizens also engage in the debate. Especially since, as we will see, it is they who are often the victims of cyber attacks: they are misled or blackmailed, their computers are hacked and vital public services are harmed. The task of the Rathenau Institute is to support the political decision-making process and the public debate on the impact of technology on society. That mandate also encompasses offensive cyber capabilities. Our hope with this report is to ensure that, as well as experts and politicians, the general public is well-informed about the uncertain and threatening situation in which they find themselves.

1.3 The cyber escalation ladder

In this report we make a distinction between **cyber peace**, **information conflict** and **cyber-physical warfare.** This is the central conceptual framework for our analysis of offensive cyber capabilities and our contribution to the vocabulary in the discourse on cyber attacks.

- **Cyber peace** refers to a situation in which states do not attack other states with offensive cyber capabilities.
- **Information conflict** refers to a phase in which a state launches cyber attacks in and against another country. This phase can include attacks that involve sabotage, but also espionage and disinformation.
- The final phase is that of **cyber-physical warfare**, which arises if a cyber attack by a state is so serious that it exceeds the legal threshold for an armed attack and the country enters into a state of war with the country that was attacked.

These three phases together form a **cyber escalation ladder** (see figure 1), starting with cyber peace and ending with cyber-physical warfare. In this report, we will conclude that practically every state is engaged in an information conflict with one or more other countries – and that it is precisely in relation to this information conflict that adequate clear and widely respected regulatory frameworks are lacking.

It is therefore necessary to formulate sensible international principles that will contribute to a de-escalation of the information conflict. In formulating new principles, it is important to protect citizens and their public services and as far as possible safeguard them against attacks that undermine their rights, such as the right to privacy and to security and their role as democratic citizens.

1.4 Definitions

This report describes the capabilities of a state or state-sponsored actors to carry out cyber attacks involving **cyber sabotage**, **cyber espionage** and the dissemination of **disinformation**.[3] These categories were chosen on the basis of the literature and policy documents (see, *inter alia*, AIVD 2019). Cyber crime therefore falls outside the scope of this study, unless states consciously use cyber crime in furtherance of their interests.

- **Cyber espionage** is the clandestine gathering of intelligence using digital technology.
- **Cyber sabotage** is consciously causing damage to persons, objects or data sets using digital technology.
- **Disinformation** refers to the spreading of untrue, inaccurate or misleading information that is consciously created and disseminated for economic gain or to harm a person, social group, organisation or country (Van Keulen et al. 2018, 14).

These three instruments can harm a society to varying extents and are therefore described in this report as **cyber weapons**. They can also be combined to achieve particular strategic effects. At election time, for example, a malicious party can cause the website of a political organisation to crash (cyber sabotage), steal sensitive secrets (cyber espionage) and spread false reports (disinformation). The entire assortment of cyber weapons at an actor's disposal is referred to as a **cyber arsenal**.

In this study, we describe the capacity to launch cyber attacks as **offensive cyber capability**.[4] By this we mean not only access to the technology, but also aspects such as having at one's disposal expert hackers who can carry out attacks, and having a strategic policy on the use of these capabilities. A **cyber operation** is a series of actions using digital technology, by an intelligence service for example, such as a cyber espionage operation.

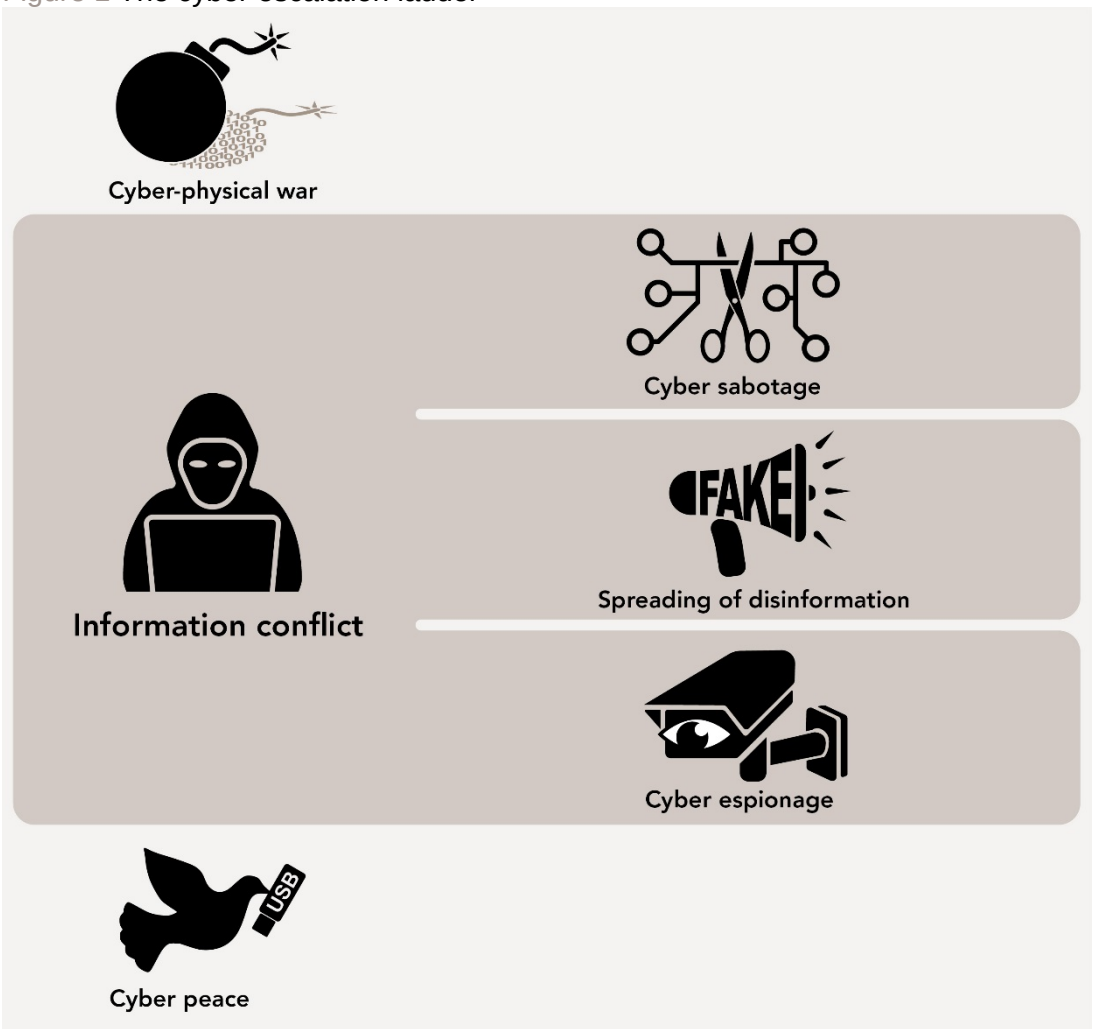
There are also weapons that combine conventional military technology with digital technology, such as an armed drone or a digitally-operated missile installation. The Rathenau Institute published a report earlier on military robots (Royakkers & Van Est 2016). That type of technology is not the focus of this report, in which the emphasis is on the damage that one state can cause to another through the use of computer code or of digital devices, such as infected USB sticks or WiFi routers.

3 The term 'attack' as used here refers to more than simply attacks in a miltary conflict.
4 Views also differ on this terminology. See, inter alia, Ducheine and Van Haaster 2014.

The report also explicitly focuses on the international context. We discuss national developments insofar as they are relevant for the Netherlands' orientation. The report also expands on the analysis of the national cyber security policy in our earlier report *A never-ending race* (Munnichs et al. 2017).

Figure 1 illustrates the cyber escalation ladder, including the various types of cyber attack.

Figure 1 The cyber escalation ladder



1.5 The questions to be answered

The emergence of offensive cyber capabilities has altered the international environment in which the Netherlands finds itself. The central research question in this report is therefore:

How can the Netherlands, in light of the emergence of offensive cyber capabilities, contribute to de-escalation of the information conflict?

To answer that question, in this report we outline the international situation with regard to offensive cyber capacities in three steps.

First, we explain the nature of offensive cyber capabilities: **What are offensive cyber capabilities?** We answer that question by reviewing various aspects of cyber operations and what they imply for the relationship between attackers and defenders and compare them with conventional espionage, propaganda and military capabilities.

We then examine the build-up of capacity by a number of global players: **What offensive cyber capabilities are being developed in the United States, Russia, China, the Netherlands and European countries?**

Finally, we examine the ways in which countries collaborate with one another and with partners in civil society at international level in designing measures to regulate offensive cyber capabilities and so could contribute to lasting cyber peace: **What joint steps are being taken by the international community to guarantee a safe and free digital world?**

We answer the main question on the basis of a description of the international situation.

1.6 The research method

This study is based mainly on desk research, supported by background interviews and discussions with experts.

Desk research and discussions with experts
A combination of government documents, journalism and academic literature provides the best insight for a study into the emergence and use of offensive cyber capabilities from an international perspective. The government documentation shows what states and intergovernmental organisations themselves say about their

offensive cyber capabilities. For example, the US Department of Defense regularly publishes strategic documents, and agencies of the United Nations report to the General Assembly on the results of their deliberations.

But these documents do not provide a complete picture. Many cyber operations occur in secret and defence organisations and intelligence services generally withhold details of their cyber arsenals from the press. This means that for a clearer impression of international developments it is essential to consult investigative journalism, tech blogs and publications of cyber security companies, as these sources often disclose the details of cyber operations.

Finally, it is important to read academic publications and to remain up-to-date with relevant developments in international law. Prior to this study, we therefore conducted a number of interviews. The results were submitted to a number of experts in the field: Paul Ducheine of the Netherlands Defence Academy's Faculty of Military Science; Sico van der Meer of the Clingendael Institute; Frank Slijper of PAX; and Dimitri Tokmetzis of De Correspondent. We also spoke to Pim Takkenberg of Northwave. We would like to express our warm gratitude for their assistance.

2 Offensive cyber capabilities

Box 1 Three examples of cyber espionage

Around 2003, the US Defense Department found that a growing number of attacks were being carried out on its networks. These attacks went on for years and were jointly referred to as Titan Rain (Adkins 2013, Bowcott 2008). Some attacks reportedly penetrated the networks, but it is unclear what espionage or sabotage activities actually occurred. The United States and the United Kingdom accused Chinese hacker groups (Bowcott 2008).

In 2013, Edward Snowden revealed the extensive espionage operations carried out by the American security agency NSA (Sanger 2018, Ball et al. 2013). He reported that in association with the British GCHQ it had intercepted secure traffic on platforms such as Facebook and Gmail, tapped the communication of European allies and collaborated with IT producers to insert vulnerabilities in their products.

In April 2016, the network of the Democratic National Committee was hacked. The committee manages the Democratic Party in the US. Conversations in chat rooms and e-mails were monitored and hacked. The NSA and the government agencies FBI and CIA (see box 4) were among those that later said the Russian government was responsible (DHS, ODNI, FBI 2016). On 13 July 2018, special prosecutor Mueller indicted twelve Russian intelligence officers for hacks, including this one (Ward 2018).

In this chapter we discuss the three separate offensive cyber capabilities that were introduced in chapter 1: cyber espionage, cyber sabotage and the dissemination of disinformation. We give a brief technical description of these capabilities, compare them with conventional military capabilities and study the ways in which society can defend itself against these offensive cyber capabilities. We also include text boxes with some examples of cyber attacks.

2.1 Cyber espionage

2.1.1 Technology

We define cyber espionage as the gathering of information using digital technology. Roughly speaking, this intelligence gathering has two targets: state secrets and economic secrets. Both forms of espionage occur on a large scale in the digital domain (AIVD, MIVD 2017). It can be interesting for a state, and for companies connected with that state, to steal intellectual property, such as a new design for an electric car. Equally, a state's defence forces may wish to get hold of another state's secret plans for a new fighter jet. See box 1 for a number of examples of cyber espionage.

Broadly speaking, there are two phases to most cyber attacks: penetration and action (AIVD, MIVD 2017, Ducheine & Van Haaster 2014, Andress & Winterfeld 2011, Janczewski & Colarik 2007).[5] Once a system has been penetrated, there are two possible actions: an act of cyber espionage or an act of cyber sabotage. Cyber espionage works in a similar way to a reconnaissance plane: the plane first has to enter hostile territory and then gather information. Cyber sabotage (see section 2.2) is similar to a bomber: again the plane first has to enter the hostile territory and then drop its harmful payload (Herr & Rozenzweig 2013). Cyber sabotage and cyber espionage therefore partly involve similar actions, but they have different purposes.

Cyber espionage is used to penetrate information systems to which an actor does not have regular access. In that context, we can make a distinction between actions that do or do not use software. After all, organisations can also be infiltrated through fraud, or social engineering: for example, a person can pose as a client and creep behind a salesperson's computer at an unguarded moment, or trick a credulous person into revealing their log-in data during a telephone conversation. This is why cyber security also includes physical security and why it is so important to control who has access to computers and what information may be shared with persons outside the organisation.

Cyber espionage via phishing, spear phishing and spoofing
One of the most common methods used to break into an information system digitally and remotely is phishing. This method involves sending e-mails to people and persuading them to click on a particular link or to call someone and provide

5 All of these authors suggest more complex structures, which differ from one another in minor aspects. For example, the AIVD and MIVD focus more on safeguarding access to a digital system. The distinction we propose provides a handy simplication of this discussion.

their log-in details. Sometimes a specific e-mail is sent to a large number of addresses, which is commonly referred to as spam mail. And sometimes an e-mail, or a website for which a link is provided, is designed for the specific purpose of deceiving a particular person – this is known as spear phishing. A related strategy is spoofing; in this case, an e-mail appears to have been sent by an acquaintance or a trusted person or organisation, such as the individual's line manager – although that is not actually the case.

These strategies are frequently used for bank fraud. A person receives a fake e-mail purportedly from the director of the bank saying that there has been a mistake in a transaction and that customers have to log on to the bank's website. Anyone clicking on the link then reaches a fake version of the bank's website and enters the data there (Politie 2018). When the customer does so, the criminal can steal money and transfer it to a third account.

Phishing, spear phishing or spoofing are all attempts to persuade someone to do something. If the person doesn't click on a particular link and does not enter data, the intruder cannot enter his or her information system. Furthermore, these strategies can be observed clearly – the intruder has introduced himself to the victim with the e-mail or the telephone call.

Cyber espionage via zero-day exploits

The technology that enables a system to be penetrated in the least conspicuous manner uses so-called zero-day exploits. These are as yet unidentified vulnerabilities in the source code of software such as Windows or Android or of a WiFi router (Bilge & Dumitras 2012).

The term 'zero day' refers to the fact that the software manufacturer is unaware of the vulnerability and has not had even a single day (zero days) to remedy the vulnerability in its program code. In other words, technically speaking, as soon as the fault is discovered the vulnerability is no longer a zero day. However, even known vulnerabilities can be used for a far longer period because it can take a while before a producer can remedy the vulnerability with a piece of software (*patch*) and because older systems are sometimes not kept properly up to date. Furthermore, once the existence of a vulnerability is revealed, other malicious parties learn of it. Some authors therefore assert that the abuse of zero days increases following their disclosure, because more actors can carry out attacks on systems that have not been properly updated (Bilge & Dumitras 2012).

Zero days are ideal for espionage purposes: if the victim is unaware of the zero day, the spy can slip into a system unseen and perhaps monitor relevant activities for months – or even years.

Cyber espionage via hardware
Finally, a person can also infiltrate a system via hardware, for example by inserting an infected USB stick in a device or simply by introducing spyware during the production of a computer or a router.

It is often a combination of different technologies
To sum up, there are various ways of penetrating a system and they can also be used in combination. In the case of the infiltration of the uranium enrichment facility in Natanz in Iran, for example, a virus was smuggled into a closed network by a person using an infected USB stick containing a number of zero days (Zetter 2011). Another possibility is that a relatively cheap phishing attack is tried first, before more expensive zero days are considered.

Furthermore, espionage operations often occur in stages. For example, someone first penetrates the poorly secured user account of someone who has few authorisations and rights within the information system and therefore does not have access to all of its information and functions. The intruder then tries to acquire more rights via this first account, for example by breaking into the account of a system manager or administrator. In this way, the intruder tries to expose the information system step by step, using various strategies to achieve his ultimate goal.

2.1.2 Comparison with conventional espionage

Digital espionage has several advantages over conventional espionage. Enormous files can be instantly transferred from one side of the world to the other at the press of a button rather than having to secretly carry files around. Moreover, a cyber spy can in a short time attempt to break into systems in different countries from behind his computer.

Digital espionage is therefore far more efficient. If the digital spy does his work well, it can be years before a government agency is aware that it is being monitored or that its documents are being read. That is also the goal of intelligence services: to gain lengthy, clandestine access to the adversary's secrets (see, *inter alia*, U.S. Department of Defense 2018, U.S. Cybercommand 2018b). Cyber spies can also make gaining access easier for themselves by, once they are inside the system, building backdoors in the system's firewall (AIVD, MIVD 2017). At this point, cyber espionage clearly becomes harmful since backdoors weaken the security of the entire system.

But the greatest difference between digital and conventional espionage lies in the relative safety of cyber espionage for spies. We are all familiar with the exciting stories of spies in constant fear of being discovered and the enormous risks they face. Cyber spies have no need to be so scared. Although for some forms of cyber espionage an organisation does have to be physically infiltrated, any computer connected to the internet can be hacked remotely. This makes browsing in a system far less risky for the cyber spy – there is little chance of being prosecuted if the spying takes place under the protection and from the territory of another state. It is also sometimes difficult to identify the perpetrator of a cyber attack. This is known as the attribution problem. For example, attackers can hack a computer, or even a series of computers, and launch their attack from those computers. This can create a trail that runs through various states and which can sometimes only be followed with the cooperation of all those states.

There is undoubtedly a link between this absence of risk and the scale of cyber espionage. In many states, regular attempts are made to penetrate important government systems (AIVD, MIVD 2017). The character of cyber espionage can therefore be described as simultaneously covert and brazen: companies and governments do not know precisely who is attacking them but may be aware, certainly in the case of less refined attacks, that numerous attempts are being made to spy on them. Cyber espionage is therefore far more visible than the traditional shadow play between secret services and spies.

2.1.3 Resilience

Governments, companies, civil society organisations and citizens naturally try to prevent attempts at espionage. But it is difficult. An infiltrator usually needs just one mistake or weakness to infiltrate a system, while an organisation under attack has to get a great many things right at the same time (Farwell & Rohozinski 2012).

To give an example, if a user in an organisation with hundreds of employees unthinkingly clicks on a link in a phishing mail the malware immediately enters the network. Furthermore, with the help of a zero day the attacker can evade various security measures, including firewall software. Some experts therefore argue that in principle every digital network can be infiltrated.

Nevertheless, security measures are useful. An encrypted connection for which only a password is required is easier to hack than a system that uses encryption with two-factor authentication, which also uses a fingerprint scan for example. Building firewalls between different parts of a digital system (segmentation) also

does not prevent attempts at infiltration altogether, but does make them far more difficult.[6]

It is also important to note the difference in terms of refinement and expertise between some cyber attacks and others. Phishing mails can look convincing, but they can also be clumsy and easy to recognise. It is also easier for a cyber attacker to send a phishing mail than to gain possession of zero days, which are rare and very valuable. For example, Zerodium, an information security company that sells information about vulnerabilities to businesses and public authorities, pays up to $ 1.5 million for some vulnerabilities in the iPhone's operating system (Zerodium 2018). Effective defensive measures, such as making backups and using strong passwords, may not protect against the most advanced attacks, but will fend off a great many relatively simple attacks.

Ultimately, the relationship between cyber attackers and defenders can best be described as a race in which, at least at the moment, the attackers seem to be in the lead (Munnichs et al. 2017). They can often carry out attacks without fear of repercussions and only have to exploit a few weak links. At the same time, there are security systems, such as the iPhone's operating system, that are extremely difficult to hack. But it is a race with no finishing line: even reliable security systems are eventually penetrated, which again calls for new security measures.

6 These and other recommendations to promote cyber security are listed and explained in the report *A never-ending race* (Munnichs et al. 2017).

2.2 Cyber sabotage

Box 2 Three examples of cyber sabotage

In 2007, patriotic Russian hackers launched a cyber attack on neighbouring Estonia. The two countries were in dispute over the relocation of a Russian war monument in the Estonian capital, Tallinn. When the Estonians moved the monument, the hackers responded with a cyber attack that crippled the Estonian government's website, the media and banks. For almost a week these institutions were unable to do any business online and citizens could not contact them (Karatzogianni 2008). Russia denied any involvement.

In 2010, a malware attack was carried out on a uranium enrichment facility near Natanz in Iran. The malware, called Stuxnet, was developed by the US in association with Israel during Operation Olympic Games and was used by both states to sabotage Iran's nuclear programme. The attack delayed the nuclear programme for months (and perhaps for more than a year) (Gross 2011).

In 2015, various places in Ukraine suffered a power failure two days before Christmas (E-ISAC SANS ICS 2016, Zetter 2016). It was night and the temperature was almost below freezing at the time of the attack. Within a few hours, the engineers were able to manually restore the power. This was the first cyber attack that succeeded in shutting down a power station. The attack also involved a DDoS attack that sabotaged the customer service. The Ukrainian secret service says it has no doubt that the Russian government was behind the attack.

2.2.1 Technology

A cyber attack can also be used for the purpose of sabotaging a digital system and causing damage. Various forms of sabotage are possible because many different applications are connected digitally. We describe a number of major incidents in box 2.

In addition to the examples in box 2, we can also imagine other forms of sabotage:

- breaking into a self-driving car that is connected online and cause it to crash;
- penetrating the network of a hospital and using ransomware to encrypt patient files and demand a ransom;
- gaining access to a secret file of a country's intelligence service and posting the content on a public website;
- penetrating a WiFi-operated pacemaker and switching it off.

It is important to remember in this context that cyber attacks generally comprise elements of both sabotage and espionage. For example, during the Stuxnet operation (see box 2) the system was infected via a USB stick which itself contained code to sabotage the system (Zetter 2011).

A specific type of cyber sabotage is a DDoS attack. These attacks do not depend on infiltration of a computer system. A DDoS attack involves sending so many service requests to a website or other digital service that it becomes overburdened and no longer functions. In other words, such an attack can be launched by a large group of computer users acting in concert without using additional malware. In this context, Klimburg has written of the countless computers of Chinese citizens that the Chinese state could use to carry out a DDoS attack (Klimburg 2017). Often, however, a large number of computers are hacked to create a so-called botnet, whereby service requests can be sent from an even larger number of sources. In this case, a DDoS attack does have an extensive infiltration phase. The automated hacking of digital devices is a major problem in this context. With smart software, a hacker can quickly assemble thousands of bots and launch an enormous attack with relative ease. DDoS attacks are as popular as ever and more advanced and hard-to-detect variants are emerging.

2.2.2 Comparison with conventional weapons

There are interesting differences between cyber sabotage and the use of conventional weaponry. The most striking difference is the potential damage. Bombers, grenades, tanks and missile installations can kill people and often totally destroy physical objects, from bridges to power stations. We live in a world full of nuclear weapons that could totally destroy human civilisation. Although cyber weapons can sometimes cause physical damage, as in the case of the operations in Ukraine and in Natanz, the damage they can cause pales in comparison with conventional weapons. This probably explains why states have up to now responded very differently to cyber attacks than to conventional attacks. If Russia were to attack Rabobank's head office with bombs rather than a computer virus, the

NATO countries would very probably declare war on Russia. We will return to this subject in detail in chapter 4.

As already mentioned, the potential damage from cyber weapons is still growing rapidly. A surprise and extremely damaging cyber attack, referred to by some as a *Cyber Pearl Harbour*, is perhaps a real possibility, and future cyber weapons could greatly disrupt a society (Trautman 2016). But even in that case the perception of a cyber attack might still be very different to the perception of an act of war that directly costs lives or destroys buildings. Destroying a power station is not the same as manipulating the technology in such a way that the power station is unable to supply electricity for weeks.

In some cases the damage caused by cyber attacks can also be easily repaired (Libicki 2016). A lost life is gone forever and an historic church cannot easily be rebuilt. But if a bank's website is offline for a few hours and then works again, no one feels that something has been lost forever. There is of course still serious damage: repairs have to be carried out, new security measures have to be purchased and installed and important services are delayed. But most people will quickly forget the cyber incident. Naturally, that is not always the case. For example, a cyber attack could also delete crucial documents that cannot easily be rewritten.

This reparability has prompted some authors to describe cyber weapons as an elegant alternative to conventional weapons (Rid 2013). Would it not perhaps be fantastic if a country had such digital dominance that it could resolve international conflicts simply by threatening to use cyber weapons? But that narrative could also be naive. Cyber weapons might not replace conventional weapons, but they are perhaps creating a new, rapidly escalating phase in international diplomacy that could suddenly spill over into violence. We explore this tension in more detail in chapter 4.

Another major difference compared with conventional military weapons lies in the possibility of neutralising the cyber weapons themselves. It is far easier to deactivate cyber weapons than to deactivate a conventional rifle or missile. In that respect, cyber weapons can be compared with viral diseases and inoculation. If there is an effective vaccination, a viral disease can be eradicated entirely. Equally, the effectiveness of a cyber weapon diminishes greatly if the vulnerability targeted by the harmful code no longer exists. That requires that computer systems are regularly updated, which is often not done. But the dynamic is similar. An effective update can remove the sting from a cyber weapon. In that respect, cyber weapons differ greatly from conventional weapons such as rifles and nuclear bombs. A single

physical weapon can be destroyed and one can design all sorts of defences, but the type of weapon has significant potential to cause harm.

At the same time, in contrast to a regular soldier, a cyber attacker is almost impossible to disarm (Libicki 2016). In the vast majority of developed countries it is easier to buy a computer than a firearm – and advanced military weapons in particular are only available to very specific actors. So even if the United States is capable of disabling hostile computers, a cyber attacker can plan another attack on a new computer. This raises questions about plans to counter cyber attackers by attacking them with cyber technology – it is almost impossible to permanently disable an opponent in this way (Libicki 2016).

Finally, cyber weapons can spread far more easily than conventional weapons. A virus can be sent from one side of the world to the other in a matter of seconds with just the press of a button – that is not the case with firearms or nuclear missiles. Cyber attackers can carry out an attack from anywhere in the world, just as long as they have a connection to the internet. An attack can therefore also spread at an alarming rate. This happened with Stuxnet, for example, which spread from Iran to computers in Europe (Zetter 2011). Furthermore, a party can steal cyber weapons, sometimes from a great distance. For example, the hackers collective known as the Shadowbrokers was able to steal various cyber weapons from the NSA, which were later posted online (Sanger 2018).

There is a serious risk of cyber weapons being reused by other parties and, as in the case of Stuxnet, of a harmful code unintentionally affecting various other targets. The problem of collateral damage is naturally also a factor with the use of conventional military weapons, and those weapons are also stolen or replicated by the enemy. But the scale is different. A bombing mission might also hit the hospital close to the military base, but a misguided virus targeted at a computer in the Netherlands can easily cause damage in the UK a short time later.

The global nature of the internet therefore complicates the use of cyber weapons. There is a serious risk that other parties will ultimately also use the dangerous code and that this will cause various unforeseen boomerang effects.

2.2.3 Resilience

Some of the measures to protect against cyber sabotage have been discussed. If you ensure that a hacker cannot infiltrate a system and cannot expand his authorities within a system, in most cases the system cannot be sabotaged. But

once a hacker is inside the system and has gathered the necessary authorisations, various forms of sabotage are possible.

However, some forms of sabotage require more expertise than others. For example, to write malware for a petrochemical plant a hacker has to understand the industrial software. But no such expertise is required for a lot of harmful sabotage. There is in fact a lucrative market in the provision of services such as sending spam mail, carrying out DDoS attacks, writing malware and recruiting bots (Libicki 2016). For example, there are criminals who will launch a DDoS attack against an unprotected site for $ 100 a day, while the price of an attack on a site protected against DDoS is $ 400 (Markushin 2017). In contrast, the costs for the party that is the target of a cyber attack can quickly mount. Kaspersky estimates the average costs for a small company at almost $ 90,000 and the costs for a large company at almost $ 900,000 (Kaspersky 2016). In other words, the difference between the attacker's costs and the costs for the defender can be enormous – and that is without even considering the revenues earned by the attackers.

All of these aspects create a worrying picture: many types of cyber attacks can be carried out cheaply, can be ordered by laypersons and can be difficult to defend against. It is not without reason that there have been repeated warnings of the enormous challenges in building cyber resilience (NCTV 2018). At the same time, the comparison with conventional weapons shows that although cyber sabotage has caused severe damage in the past, it has not claimed human lives, has not shocked a society in the same way as a terrorist attack and has not disrupted society to the same extent as an economic crisis, a serious drought or a flood. Although vital infrastructure has been damaged by cyber attacks, the infrastructure has normally been restored to its former level within a few hours. Nevertheless, the relative mildness of past cyber attacks naturally provides no guarantee for the future.

The defence against cyber attackers can also consist of causing damage to the attacker, for example by eliminating or deterring the attacker. As already mentioned, it is sometimes difficult to identify cyber attackers – but it is certainly not impossible. Various cyber criminals have in fact been successfully prosecuted and convicted in the past and intelligence services sometimes claim to be certain of the identity of the perpetrators of a particular attack (Westcott 2018, Ward 2018). But when the attack is carried out by or with the consent of another state, it is not immediately clear what action should be taken and what strategy would ultimately promote cyber security. We will discuss that issue in more depth from chapter 3 onwards.

2.3 The dissemination of disinformation

Box 3 Three examples of disinformation

The quantity of false information circulating on online fora increased steadily ahead of the US presidential elections in November 2016 (Faris et al. 2017, Ritchie 2016). The Pope was reported to have endorsed Donald Trump. Hillary Clinton was alleged to have sold weapons to Islamic State (IS). And John Podesta, Clinton's campaign manager, and other senior staff members were said to have abused children.

Since 2008, Russian media, right-wing groups and Donald Trump have spread the demonstrable lie that Barack Obama was not born in the United States and should therefore not have been president (Haberman 2017). This conspiracy theory is known as *birtherism*, and is still being repeated, even since Obama's birth certificate was published. Trump ultimately gave a press conference at which he admitted that Obama had been born in the United States.

Ahead of the French presidential election in May 2017, a document entitled EMLEAKS appeared on Pastebin, a site where documents can be shared, containing a lot of false information about Emmanuel Macron, who was then a presidential candidate, for example that he had a secret bank account in the Cayman Islands (Valance 2017).

2.3.1 Technology

Spreading disinformation is not necessarily connected with digital technology, but is certainly made easier by digital channels. Cyber attacks, like the attack on the Ukrainian energy network, generally also involve a disinformation campaign. What do we actually mean by disinformation?

The Council of Europe has distinguished three forms of dissemination of perverse information: the spreading of disinformation, misinformation and malinformation (Wardle & Derakhshan 2017).

- **Disinformation** means consciously creating and disseminating untrue, inaccurate and misleading information for economic gain or to harm a person, social group, organisation or country (see also Van Keulen et al. 2017). For example, a person might spread the inaccurate report on Twitter that a well-known politician has committed a sex offence.
- **Misinformation** means disseminating inaccurate information which on believes to be correct. So if another person were to re-tweet the above report about the politician believing it to be true, he would be misinforming others.
- **Malinformation** means the dissemination of embarrassing, but accurate information to defame a person or organisation and to incite others against that organisation.

As already mentioned, this report focuses on the spreading of disinformation; see box 3 for a number of examples.[7] Misinformation does play a role in that: the instigator hopes that others will believe the inaccurate reports and spread them further. An example of disinformation is the report on the website of WTOE 5 News that Pope Francis endorsed Donald Trump's candidacy for the presidency. That was not true. Even today, academics, journalists and the American Federal Bureau of Investigation (FBI) are still trying to form a clear picture of how much disinformation was disseminated during the US presidential election in 2016, and by whom precisely (Ferrara 2017).

Anyone with a Twitter or Facebook account can spread lies. But disinformation is generally disseminated through anonymous accounts and by online profiles, so-called bots, that are controlled by software and circulate messages on the basis of algorithms (Varol et al. 2017). Particularly on Twitter there are a lot of bots. In March 2017, researchers estimated that bots accounted for between 9% and 15% of all Twitter accounts. That would be almost 48 million accounts (Varol et al. 2017). This enormous throng of bots plays a crucial role in the spreading of disinformation. You only have to imagine the effect of an untruthful report being re-tweeted by 500,000 bots.

Finally, it is important to note that disinformation can be spread with falsified images or audio fragments (Rathenau Institute 2019). Digital applications can create increasingly convincing films in which politicians seem to be making a particular statement, for example. It is often impossible for the average layperson to see the difference between an authentic and a fabricated recording. There have recently been many warnings against this new technology, which can significantly increase the impact of disinformation campaigns (Polyakova & Boyer 2018).

7 Disinformation intended for economic gain is not discussed here because the phenomenon does not play a role of any significance in relations between states.

The spreading of disinformation manipulates the public debate. Precisely how depends on the objective. Nevertheless, it is noticeable that disinformation often has a polarising effect and can, in addition to supporting a particular message or agenda, compromise a balanced and substantive public debate (Wardle & Derakhshan 2017). As the Rathenau Institute wrote in its report *Digitialisering van het nieuws*: 'Disinformation often consciously refers to differences and encourages divisions between supporters of different political parties or between groups of different nationalities, race, ethnicity, religion or class. Once uttered, such ideas can be used to create scapegoats, popularise prejudices, strengthen divisions and even catalyse and justify violence.' (Van Keulen et al. 2018, 49).

2.3.2 Comparison with conventional propaganda

Disinformation campaigns have considerable promise: anyone who can influence the public can win them over to his own ideas and influence policy. Naturally, this depends on how effective the campaigns are and how well citizens and their institutions are able to unmask and neutralise disinformation. Faced with a campaign of disinformation, Macron was still able to win the election by a large margin, while Hillary Clinton, also confronted by disinformation, narrowly lost the election to Donald Trump.

This uncertainty about the effect of disinformation in no way deters some states from experimenting with it. Compared to tradional propaganda campaigns, spreading disinformation is cheap and can be automated to a large extent. This makes it possible to structurally influence the public debate. Furthermore, the spreader of disinformation seldom has to fear personal repercussions. Here too there is the problem of precisely identifying the perpetrator and the fact that the perpetrators can hide in the territory and under the protection of a hostile state. It is therefore likely that disinformation campaigns, state-sponsored or otherwise, will continue to play a significant role in the future.

2.3.3 Resilience

Can a society protect itself against disinformation? That is partly the responsibility of the media platforms on which the disinformation is published. Here are a few examples.

- Twitter tries to automatically identify and eliminate bots (Crowell 2017). Unfortunately, Twitter bots are becoming increasingly refined and will become

increasingly difficult to distinguish from human users in the future (Van Keulen et al. 2018, Rathenau Institute 2019).

- Platforms could also introduce an alternative communication architecture, for example one that requires every account to be linked to an authenticated human user. However, there is also an objection to this, since online anonymity also has advantages, for example when proclaiming a particular message is dangerous for the sender.
- Finally, social platforms could reveal how their algorithms work. That would create awareness among citizens about the influence of algorithms on the information they receive (Van Keulen et al. 2018). For example, a study by the psychologist Robert Epstein has shown how search results can heavily influence voter preferences simply by changing the order in which the results appear in a search engine like Google (Epstein 2015).

Politicians could also play a more active role, for example by facilitating independent institutions, for example to employ fact checkers to monitor the news and verify the accuracy of information in public (online and offline) debates (Harambam 2017). But there is a risk in this. Western democracies have a free press that is not controlled by the state. In a properly functioning democracy, primary responsibility for exposing lies resides mainly in an open public debate.

Journalists and citizens therefore have their own important roles to play. Journalists can build a close bond with the public, online and offline, by conducting in-depth research and thoroughly checking facts and by explaining how journalists do their work. Journalists could also raise their online profile. An example of this is *The Daily,* The New York Times' daily podcast, in which the editors explain their work and sometimes consciously broadcast interviews in their entirety.[8]

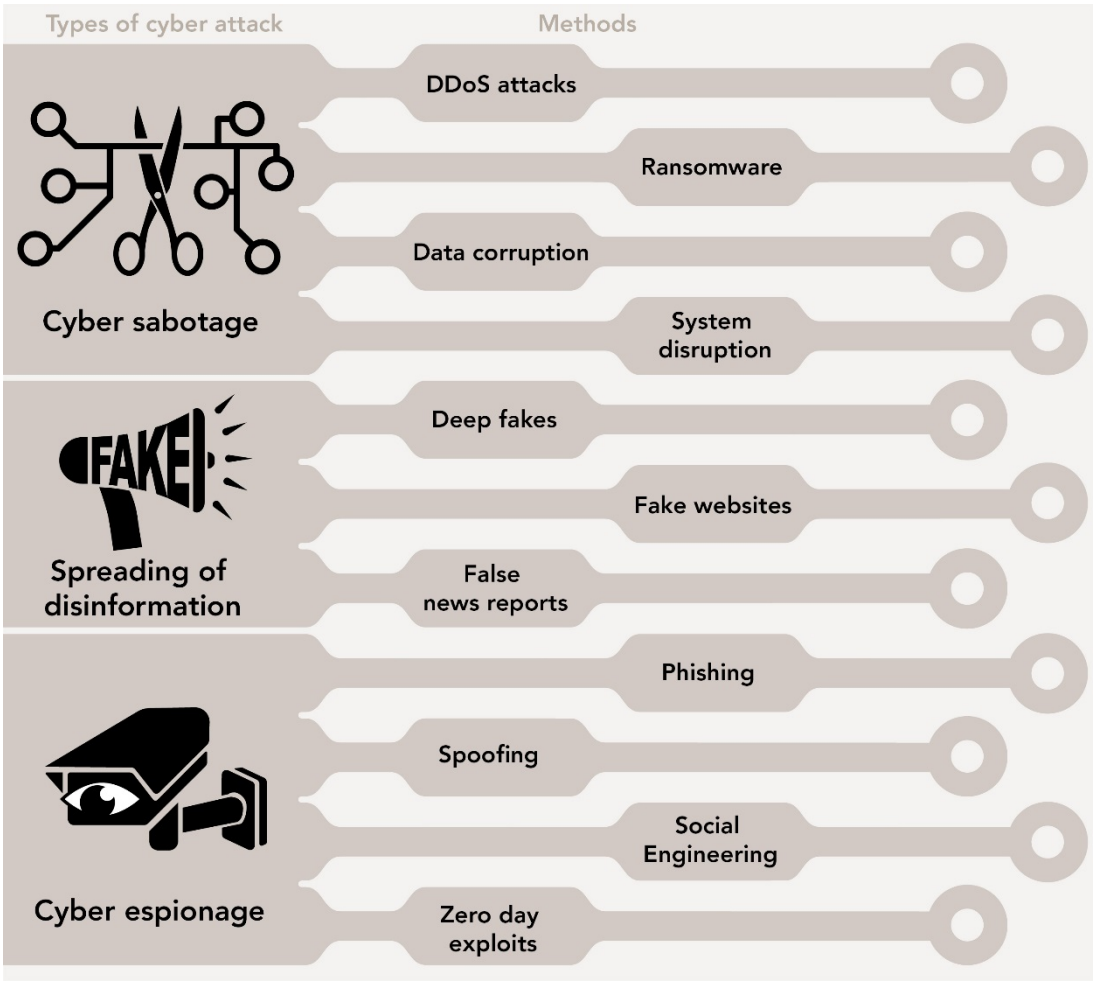
Finally, society needs citizens who are technologically literate: individuals who understand how disinformation is spread, who can reflect critically on the information they receive and who understand the impact that a disinformation campaign can have on their own life (Van Keulen et al. 2018). These are citizens who could identify and challenge disinformation and so reduce the effectiveness of this sort of influence. In Sweden, for example, pupils from the age of ten receive compulsory education in digital competences (Roden 2017). An important element of this is learning to evaluate sources critically.

8 See https://www.nytimes.com/column/the-daily.

2.4 Conclusion

This chapter has provided an overview and analysis of the technological developments relating to offensive cyber capabilities. The various types of cyber attacks are illustrated in figure 2.

Figure 2 Different types of cyber attacks



These are the main findings:

- **We have made a distinction between three types of cyber attacks: cyber espionage**, **cyber sabotage** and the **dissemination of disinformation**. These types of cyber attacks are closely interrelated: cyber espionage, for example, often precedes cyber sabotage, and during the attack on the US elections in 2016 the dissemination of disinformation was combined with the hacking of the Democrats' mail server.

- **Cyber attacks differ fundamentally from conventional attacks in some respects.** Cyber spies face far less risk than conventional spies and can infiltrate and monitor multiple digital systems for lengthy periods and from a great distance. Digitisation has made spying simultaneously more brazen and more elusive. Cyber saboteurs also run far smaller risks and can cause damage that is unpredictable and widespread. However, the potential damage differs fundamentally from that caused by conventional weapons. A lot of damage can be repaired and serious physical damage is rare. Finally, the internet allows disinformation to be disseminated on an unprecedented scale, and lies can reach media from many different profiles and along numerous channels. This makes it difficult to discover who is spreading propaganda and why. In that respect, digitisation is a blessing for actors who wish to use propaganda to pursue their goals and polarise debates.

- **Cyber attacks are sometimes very difficult to defend against and effective cyber security measures require substantial investment in terms of resources and manpower**. Unlike cyber defenders, cyber attackers can strike from the shadows and can often carry out or outsource attacks at little expense. At the same time, the relative expertise of attackers and defenders makes a huge difference: some attacks are easier to defend against than others. Ultimately, the attackers are engaged in a never-ending race with the defenders. However, the attackers seem to be ahead at present.

3 The information conflict

In this chapter and chapter 4, we analyse international developments in the area of offensive cyber capacities. This chapter explores the extent to which the United States, Russia, China, the Netherlands and other EU countries such as France, Germany and the United Kingdom acquire the capabilities to conduct cyber espionage, cyber sabotage and disinformation campaigns, why they do so, how they have used those capabilities, and whether we can observe any similarities and differences in the conduct of these states. We also discuss the private, sometimes criminal, market for cyber weapons in the various countries.

We have selected the United States, Russia and China because these countries are global players in today's international digital landscape. We discuss the EU countries because of the importance of the European environment for the Netherlands. At the end of this chapter, the escalation ladder (see chapter 1) is explained in more detail and we use it to rate the activities of the various states. On the basis of this escalation ladder, we conclude that the current international situation can best be described as an information conflict.

One reservation that needs to be expressed in this context is that overview of the build-up of capabilities in each country in this chapter is not comprehensive and does not cover many countries – North Korea is not discussed at all and Iran only in passing, for example – although these states are referred to as major threats by other countries (U.S. Department of Defense 2018). Nor was it our intention to provide a complete overview – our aim was to clarify the choices faced by the Netherlands itself.

3.1 The United States

3.1.1 In brief

The US has always been a dominant actor in the development of ICT technology. The country was the architect of the internet and, with companies like Apple, Amazon, Google and Microsoft, is the major commercial pioneer in the production and sale of ICT products and services (Curran et al. 2012). Characteristic of the American approach to ICT technology is the opening up of the internet. This technology has become increasingly accessible for market actors since the 1980s,

with the management of the internet being delegated to private organisations such as the Internet Corporation for Assigned Names and Numbers (ICANN) (Klimburg 2017).

At the same time, the American government regards itself as the most powerful actor in this new environment – and is determined to retain that position (U.S. Cybercommand 2018b). It is not without reason that the American government regards cyberspace as a fifth domain of military conflict, in addition to land, sea, air and space. The American strategy can therefore be encapsulated as the desire to be the heavily-armed champion of the digital free world. It goes without saying that the two aspects of this desire can come into conflict: a free digital environment is not necessarily promoted by a champion that addresses threats with force. We will return to this contradiction later.

Box 4 The United States' offensive cyber capabilities

The US spends far more on defence than any other country in the world: the Stockholm International Peace Research Institute estimated the country's military expenditure in 2017 at $ 609 billion (SIPRI 2018). The level of spending increased from 2007 until 2013 and will rise again in the coming year. By comparison, China, the second-largest investor in military capacity, spent $ 228 billion on defence in 2017.

In 2009, the US established the U.S. Cyber Command (Graham 2016). This unit of the army initially reported to the higher Strategic Command, but since 2018 has been directly accountable to the Secretary of Defense. The Cyber Command has been fully operational since 17 May 2018 and its resources include 133 cyber mission teams, comprising more than 6,000 people, which are capable of performing both offensive and defensive tasks (U.S. Cybercommand 2018a).

The US has sixteen intelligence agencies, including the Central Intelligence Agency (CIA), the National Security Agency (NSA) and the Defense Intelligence Agency (DIA). All of these agencies carry out cyber activities. The NSA has special responsibility for gathering so-called Signals Intelligence (SINGINT) on communication and information systems (NSA 2018).

The American cyber budget in 2019 is approximately $ 15 billion (Nodurft 2018). More than half of that budget is allotted to the ministry of defense. Although various cutbacks have been made in recent years, the amount of money earmarked for cyber operations and cyber security has actually increased. However, it is important to note that contributions from the intelligence services' secret 'black budget' has to be added to the published figures. The existence of this budget was revealed by the Washington Post in 2013 with the help of the whistleblower Edward Snowden. Analyses by the Washington Post showed a sharp increase in the budget from 2001, in connection with the 9/11 attacks and the subsequent war on terrorism (Washington Post 2013). The total 'black budget' was $ 52.6 billion in 2013. The CIA and the NSA received the largest sums of money, and $ 4.3 billion of the $ 52.6 billion was earmarked for cyber operations.

3.1.2 Strategic development

The US developed its offensive cyber capacity from a very early stage. Although it has never been proved, the country allegedly sabotaged the industrial control system for gas pipelines in the Soviet Union in the early 1980s (Reed 2005). This operation reportedly caused an explosion that damaged the pipeline network. True or not, today the US wants to possess the capability to cause similar damage and might possibly already possess that capacity. For years the American government has spent more money than any other state in building cyber capabilities, both in the intelligence services and in other parts of the defence apparatus, and has profited for decades from its dominant role in cyberspace (see box 4). As with conventional weapons, an industry has grown up in the US around cyber weapons, generating sales of many billions of dollars in weapons for espionage and sabotage to defence organisations (Stockton & Golabek-Goldman 2013, The Economist 2018).

The US quickly made the link between information technology, intelligence gathering and defence. The defense department already invested in the 1990s in ‘network-centric warfare’, the capacity for rapid communication via electronic networks and to eliminate the enemy’s communications networks in wartime (Cebrowski & Garstka 1998). In the 1990s, gathering and analysing internet traffic, such as e-mails, was added to the intelligence toolbox (Wright 1998). Government agencies quickly came to realise that the emergence of cyberspace was creating new security risks, but also the possibility of exploiting those risks themselves. This trend accelerated after the terrorist attacks in 2001, whereupon intelligence services were given extensive powers to conduct surveillance on and gather information about citizens, whether or not they were suspects (Jaeger et al. 2003).

In the meantime there have been a number of strategic documents and statements to indicate the thinking of the US Defense Department and the intelligence services towards offensive cyber capabilities (U.S. Department of Defense 2018, U.S. Cybercommand 2018b, U.S. Secretary of Defense 2018, Clapper 2013). An important trend is that cyberspace is explicitly seen as the fifth domain of warfare – vital American interests can be harmed through cyber activities. The US has therefore developed powerful offensive cyber capabilities; see box 4.

The second trend involves the separation of economic intelligence gathering from non-economic espionage activities. Economic espionage is seen as illegal and provocative, but spying on foreign government institutions is not illegal (Clapper 2013). Consequently, during the 2000s and most of the present decade the US supported unregulated international non-economic cyber espionage.

Cyber sabotage has sometimes also been regarded as acceptable in the US, as illustrated by the example of Operation Olympic Games. This operation deserves closer examination. The United States and a large part of the international community have been engaged in a struggle to prevent Iran from acquiring a nuclear weapon. It is highly likely that the United States, supported by the Israeli government, infected Iran's enrichment centrifuges in Natanz with the Stuxnet virus. One after the other, the centrifuges broke down, initially without Iran understanding the reason. The virus later spread to other locations and the nature and origin of the virus was reconstructed by security companies (Zetter 2011). Iran discovered the attack and retaliated in 2012 by attacking financial institutions on Wall Street (Gorman & Barnes 2012). Iran also deployed its cyber capabilities against other countries, for example by launching a devastating attack on Saudi Aramco, Saudi Arabia's state-owned oil company, which needed five months to repair the damage (Sanger 2018). On 23 March 2018, the American Justice Department accused nine Iranians of being jointly responsible for infiltrating the networks of various institutions, including 144 American universities, the United Nations and the Department of Labour, since 2013 (U.S. Department of Justice 2018).

The events surrounding Stuxnet show that technological dominance enabled the US to carry out the cyber attack, but at the same time was unable to prevent the US from being attacked itself. Even with far fewer resources available to it, Iran was still able to retaliate.

The US has been successfully attacked many other times in the last fifteen years.

- Secret technology, including zero day vulnerabilities, have been stolen from the NSA;
- confidential personal data of hundreds of thousands of federal government employees have been disclosed; and
- even the free American presidential elections were undermined from Russia in 2016 (Zetter 2015, Schneider 2017).

Various sectors are vulnerable to cyber attacks precisely because of the US's leading position in the development and application of digital technology (Klimburg 2017). This vulnerability caused some to question the strategy of cyberspace dominance, particularly under the Obama administration. For example, there were proposals to reduce the prevalence of surveillance and to conceal zero days as seldom as possible (Zetter 2014). At two crucial moments, President Obama also opted for a diplomatic course: when commercial espionage by China started to assume substantial forms he concluded an agreement with President Xi of China to reduce the attacks (Klimburg 2017). And in the wake of the attacks in 2016 he decided to expel Russian diplomats (The New York Times Editorial Board 2016).

At the same time, there were very substantial espionage activities during the Obama administrations (2009-2017). The revelations by Edward Snowden (2013) showed that American agencies had carried out hundreds of infiltrations and had not only spied on adversaries, but had also monitored citizens and even allies such as Germany, Italy and the European Union (Poitras & Rosenbach 2013). There were also suggestions that the US had attacked North Korea's digital network in response to the hacking of Sony (Van der Meer 2018b). In other words, the US administration was caught in two minds during the Obama years.

More recently, the strategy of American cyberspace dominance again appears to be gaining the upper hand. In a strategy document in 2018, with the significant title 'Achieve and Maintain Cyberspace Superiority', the American Defense Department called for 'forward defence' (U.S. Cybercommand 2018b). This implies that the US must have rapid access to, and often have already infiltrated, the systems of potentially dangerous adversaries. In other words, many networks must already be hacked in advance in order to create the possibility of rapid retaliation.

The idea is that in those circumstances hackers will no longer dare to attack the US in the knowledge that there could be an immediate and powerful response to any infiltration of an American system. Absolute dominance therefore provides a high level of deterrence. Or as the recent National Cyber Strategy put it: 'preserve peace through strength' (White House 2018, 20). The US also wants to collaborate with like-minded countries in quickly fending off attacks and jointly retaliating. Furthermore, for some time there has been a discussion in political and business circles about giving companies the right to 'hack back' so that they can also deter attackers (Kallberg 2015).

The American government also seems to be increasingly willing to spread untruths, for example about the costs of the wall along the border with Mexico and the size of the crowd that attended President Trump's inauguration. It is not clear whether these statements are accompanied by campaigns to spread disinformation in other countries. His government is in any case considering more active information campaigns – such as intensifying broadcasting in Farsi to influence the people of Iran (Morello 2018).

Finally, the US is also adopting a tougher approach towards international technology companies connected with states that have attacked the US, in particular China's Huawei Technologies and Russia's Kaspersky Labs. The government does not wish to become dependent on these suppliers because of their suspected collaboration with their governments. Huawei, for example, might install spyware in the 5G networks that it is involved in constructing. Furthermore, at the request of the US, the Canadian authorities arrested Wanzhou Meng, Huawei's

chief financial officer, in 2018 for violation of the sanctions against Iran (Tweed & Martin 2018). Commentators see this action as a further step to damage Huawei, and by extension China's technological position.

By opting for cyberspace dominance, the US is adhering to the principle that it first adopted in the 1990s: the desire to be the armed champion of a free digital world. But it is questionable whether this threat will actually deter the adversary: China's cyber-espionage activities have actually increased during Trump's presidency and there seems to be little left of the diplomatic rapprochement between Obama and Xi (Sanger & Myers 2018).

It is therefore important to express a reservation here: various academics argue that the US's strategy of deterrence is ineffective, and is actually counter-productive (Libicki 2009, Van der Meer 2015, 2018a). 'Deterrence by retaliation' is effective if the potential cost of the attack exceeds the benefits for the attacker (Krepinevich, 2012). That is certainly the case with nuclear weapons, since they cause terrible damage and are difficult to defend against. That is why states reverted to the strategy of mutually assured destruction during the Cold War (Goodman 2010).

But cyber technology differs in important respects from nuclear arms technology.

1. First, cyber attacks are far less destructive, and malicious actors are therefore more willing to carry them out. The simple fact is that the threshold for launching a nuclear weapon is simply many times higher than the threshold for spreading disinformation.
2. Second, immediate cyber counter-attacks might not always be possible, in light of the possibility that it is the offensive cyber capabilities that are eliminated by the cyber attack (Goodman 2010).
3. Third, a state often does not know who has carried out an attack or what cyber capabilities a particular adversary actually possesses (Iasiello 2013). During the Cold War, both the US and the Soviet Union knew very well what the other side was capable of, but nowadays states generally keep their cyber capabilities secret for fear of sabotage (Clarke & Knake 2010, Libicki 2013). Once the adversary knows what cyber weapons you have, they can be neutralised or even copied.

All this uncertainty makes it difficult to formulate an effective deterrence strategy and creates a grey area in which states can actually get away with carrying out cyber attacks – even if the state that is attacked possesses powerful cyber weapons.

3.2 Russia

3.2.1 In brief

Russia also has a lengthy history with digital technology. From the 1940s until the 1970s, Soviet engineers made major advances in computer science and designed many prototypes of mainframe computers (Klimburg 2017). The Soviet Union, of which Russia was a part, was a totalitarian state that identified digital technology early on as a key element in controlling flows of information between citizens and the state and between citizens themselves. Nevertheless, it was not the communist Soviet Union but the United States that developed and rolled out the internet. Some experts say this was precisely because of the Russian state's tendency to tightly control the development of technology rather than letting go of the reins and allowing citizens, companies and a wider range of government agencies to do it (Klimburg 2017, Harari 2018).

In any case, when the Cold War ended in 1989 and 1990 Russia possessed both a lengthy tradition in digital science and a totalitarian past. These two elements have determined Russia's development in the digital world and explain why the current regime of President Putin endeavours to safeguard its internal and external interests by controlling flows of information. In the eyes of the Kremlin, information is a weapon with which you can wage war (Government of Russia 2014). By means of cyber espionage, cyber sabotage and above all by disseminating disinformation, the Russian government tries to keep its own people under its thumb and keep foreign powers off balance (Polyakova & Boyer 2018).

Box 5 Offensive cyber capacities of Russia

Russia's defence spending has risen sharply in recent years, from $ 27 billion in 2006 to $ 60 billion in 2016 (estimate DIA 2017, SIPRI has no figures). However, expenditure is declining again. In 2014, the army announced that it would spend $ 500 million on special cyber troops and to create a coordinating army unit reporting directly to the general staff – the American DIA (see box 4) believes that Russia has been working on the integration of cyber soldiers in the Russian army since 2010 (DIA 2017).

Russia's principal intelligence agency is the FSB. This agency's mandate is formally confined to gathering domestic intelligence, but it also operates in the former Soviet republics and elsewhere (Klimburg 2017). Information about the precise structure and financing of the FSB is scarce. The FSB comprises units that are similar to those of the American NSA. In addition to the FSB, the GRU should also be mentioned. This intelligence service is affiliated to the Russian army, but has a broader mandate than the American DIA (Klimburg 2017).

Various hacker groups have been linked to the Kremlin, including Advanced Persistent Threat (APT) 28 and 29 (FireEye 2018). APT 28, also known as Fancy Bear, or Sofacy, has been linked to an attack on the German parliament and played a role in the cyber attack on the Democratic National Committee in 2016 (Valance 2017). The AIVD linked APT 29, or Cozy Bear, to the cyber attacks during the US elections in 2016 (Modderkolk 2018).

Russia has a large criminal community on the internet (Klimburg 2017). For example, the organisation Russian Business Network (RBN) was allegedly responsible for 60% of the worldwide internet crime in 2007. Russian cyber criminals reportedly earned around $ 4.5 billion in 2012. It is highly likely that the Russian government uses these cyber actors to carry out indirect attacks or to develop dangerous software (Klimburg 2017). This collaboration makes it even easier for the Russian government to operate in the shadows.

3.2.2 Strategic development

Russia's role on the world stage became marginalised after the fall of the Soviet Union in the early 1990s. Former satellites became independent nations and large parts of the once powerful Soviet army were disbanded (DIA 2017). In the ensuing years the country changed into an oligarchy: a country where economic and political power was vested in a small group of Russians around President Vladimir Putin (Stoner & McFaul 2015). This marked the return of the authoritarian state, following a brief worldwide 'thaw' at the end of the 1990s, and with it control over the – now digital – flow of information.

Controlling the digital flow of information was also appealing for another reason. In the first Chechen war (1994-1996), the Russian authorities had tried, but failed, to close down independent media and to censor every report from the battlefield (Giles 2016). It was therefore unable to dispel the impression of brave Chechens fighting against cruel oppressors, whose military apparatus was also very old and compromised (DIA 2017). Russia therefore opted in the 2000s for an integrated security strategy, in which information technology plays a crucial role. Briefly, the doctrine is that Russia must use a seamless combination of military, political and economic instruments to represent the country's interests (Giles 2016, Conley et al. 2016). This strategy is known as hybrid warfare, and is called the Gerasimov doctrine after the head of the Russian army's general staff (Bartles 2016).

Russia has regularly put this doctrine into practice in recent years. Once again, the fall of the Soviet Union was one of the main reasons for this. With its collapse, the large union dominated by Russia broke up into independent states over which Moscow had far less control. Putin's Russia wants to restore its influence and has therefore intervened in the former satellite states in various ways (Conley et al. 2016). It has been a hit-and-miss process. For example, the armed conflict with Georgia in 2008 did end in a Russian victory, but at the same time demonstrated serious shortcomings in both its conventional military capabilities and its capacity in terms of information technology (Giles 2016).

Another important lesson was learned from the protests during the elections in 2011 and 2012. The Russian leadership then discovered that the information war could not be won with Twitter bots and D-Dos attacks alone and that dominating online public awareness requires the involvement of 'real people' who are good orators and can present considered arguments (Giles 2016). This led to the creation of the Internet Research Agency, also known as the Russian Troll Army, an organisation made up of people who disseminate online propaganda, and the establishment of communication channels such as RT (formerly Russia Today), Sputnik and Russia Direct, which add government propaganda with a sheen of objectivity to the public

debate. All of the elements of the Russian strategy converged in the conflict in Ukraine. Once again, a former satellite state wanted to free itself from Russian influence, and once again Putin wished to prevent it.

The precise operations are still being reconstructed today, but the contours are clear. Russia used various instruments simultaneously: it sent troops without insignia into East Ukraine and the Crimea, supplied weapons to rebels in East Ukraine and threatened to occupy the region with a large force of troops (Franke 2015). The troops in the Crimea then occupied essential communication infrastructure, including telephone networks and television stations, spread disinformation and used RT to circulate particular stories with fragments from tapped telephone calls made by individuals including American diplomats. Russia also used cyber weapons to attack power stations, hospitals and financial institutions with a view to further destabilising the state of Ukraine.

The ensuing information chaos was difficult to untangle, so Western media and the European Union, for example, did not know precisely what was happening and politicians were therefore unable to draw any firm conclusions (Franke 2015). Ukraine was attacked again on 27 June 2017, this time with the NotPetya virus. It is estimated that a thousand organisations, ranging from banks to hospitals, were affected, some of them far from the country itself. The American government attributed the attack to the GRU (Greenberg 2018).

The Russian disinformation was also disseminated outside the former satellite states. Sometimes directly via a channel like RT, but sometimes also using false profiles on social media to send messages in bulk or to specific targets. That brings us to Russia’s intervention in the American elections in 2016. In the last few years the FBI has investigated possible collusion between the Russian government and the Trump campaign. Twelve Russians were charged on 13 July 2018. The indictment drawn up by FBI prosecutor Robert Mueller says, among other things, that the Russians had spent years and tens of millions of dollars making preparations for a sophisticated campaign to influence the elections (District Court of Columbia 2018, Ward 2018).

It appears that Russia is continuing to spread disinformation. It is reportedly now targeting the American mid-term elections in 2018 (Chan & Nour 2018) and the Yellow Vests movement in France (Kool 2019, Avaaz 2019).

3.3 China

3.3.1 In brief

Since 1976, the communist, centrally led China has opened up its economy to foreign investors (Tisdell 2009). Since then, the Chinese economy has enjoyed awesome growth. Today, China is the second-largest economy in the world (Word Bank 2018). This growth has been accompanied by greater economic freedom and international cooperation, but not by the political freedom that is enjoyed in Western countries (Freedom House 2018).

This reflects China's perspective on digitisation: the communist party wants to be the strongest player in the increasingly digital global economy, while simultaneously ensuring that digital progress does not threaten its power, but actually reinforces it.

3.3.2 Strategic development

The Chinese government is extremely active in the use of digital resources to control and monitor its own people (see also box 6). Like Russia, China censors online news environments and social media are also tightly monitored (see, *inter alia*, McDonald 2012, Hernandez & Mou 2018). Under the government of President Xi, there has been a tougher crackdown on dissidents, for example by arresting and imprisoning them (Schell 2016). Moreover, in 2020 the government will introduce the 'social credit system', under which Chinese citizens will be given a personal score (Kobie 2018). A person's score can be reduced because of 'bad behaviour', such as smoking where it is not permitted, posting overly critical messages on social media and for spending 'too much time' gaming. Although pilot versions are still being tested and the final system has not yet been introduced, the implications are already emerging. For example, people with a low score will no longer be allowed to travel on a plane, will only receive slow internet or will not be allowed to send their children to the best schools.

Such a system, in which citizens can be closely monitored online and sanctions can be applied automatically, is inconceivable and impractical without digital technology. The system seems like the embodiment of the government as a totalitarian Big Brother controlling and monitoring almost every aspect of people's lives.

Box 6 China's offensive cyber capabilities

With the growth of its economy, China has started investing far more in the army: from $ 31 billion in 1998 to $ 108 billion in 2008 and to $ 228 billion in 2017 (SIPRI 2018). The Chinese army has two million infantry soldiers. It is being heavily modernised, with aviation, maritime power, missile technology and especially cyber capabilities all becoming increasingly dominant (Chase et al. 2015, Klimburg 2017).

The army has a complex command structure. At least three units of the People's Liberation Army (PLA) are relevant for China's cyber capabilities: 3PLA, 4PLA and the Strategic Support Force (SSF). 3PLA is the Chinese equivalent of the American NSA (see box 4), but very probably has far more personnel – around 130,000 employees (compared with the NSA's 35,000 employees; estimate Klimburg 2017). 3PLA has various sub-bureaus, of which alone the '2nd bureau', which focuses on English-language intelligence and has been linked to espionage attacks against the American Department of Defense, employs thousands of people (FireEye 2014, Inkster 2016).

4PLA is the army unit with the task of carrying out cyber attacks in wartime. It is the centre of operations for reservists, militias and private actors who could help to carry out a cyber attack. This is important because China, the country with the largest number of internet users, probably has tens of thousands of people who could play a role in building and implementing an offensive cyber capability (Klimburg 2017), for example specialised hackers at a university. These patriots also play a key role in the censorship of the Chinese cyberspace and the spreading of propaganda.

At the same time, President Xi Jinping is seeking to modernise this enormous, hybrid complex of cyber fighters. The army must have more direct control over the ever-stronger and more advanced cyber capabilities (Klimburg 2017). In 2015, the Chinese government therefore established the Strategic Support Force (SSF), a unit that develops and implements space, cyber and electronic capabilities for the Chinese army as a whole (Pollpeter et al. 2017).

Over the last twenty years, China has succeeded in creating an alternative digital domain. Chinese internet companies Alibaba and Baidu have also grown into enormous enterprises with steadily expanding international operations (Economist 2017). Western companies like Facebook and Google are allowed to do business in China, but have to comply with numerous conditions (McDonald 2012). The companies usually meet those conditions, even though they amount to censorship.

Google, for example, was asked to filter out content unfriendly to the state from search results. Google initially agreed and was able to profit from the data of the enormous number of Chinese internet users. But in 2010 the Chinese government was found to be carrying out cyber attacks to hack the Gmail accounts of human rights activists (Branigan 2010). Google then gave Chinese users access to its uncensored search engine by means of a detour via the relatively free Hong Kong. Within a few months Google was no longer accessible to Chinese citizens. Since then Google has withdrawn entirely from China, although it is again trying to gain access to the Chinese market (see Deibert et al. 2018).

The Chinese digital business activities are not only entwined with internal espionage and censorship, but also with spying on foreign states. During the 2000s, the Chinese tried to steal economic and state secrets via digital infiltration on a large scale (Inkster 2016). These operations created so much friction with the US that in September 2015 President Obama and President Xi reached agreement that their governments would not consciously carry out and/or support economic cyber espionage (Zetter 2015).

China is increasingly engaged in a large-scale and more military-oriented build-up of offensive cyber capabilities (Klimburg 2017). Today, China possesses an enormous army of cyber soldiers. It controls large groups of volunteers who, for example in the name of the fatherland, can be used to organise joint D-DoS attacks (see box 6).

In their book entitled *Unrestricted warfare,* two Chinese colonels discuss a strategy by which China could defeat technologically superior states without using conventional weapons (Qiao & Xiangsui 2015). That is precisely the basis of China’s strategy: winning conflicts by means of efficient and overwhelming cyber attacks, without resorting to the use of conventional weapons and physical violence.

Other countries (in addition to the US) also report cyber attacks from China, including the regional rivals India and Taiwan (Wagstaff 2015, Yu 2018). The cyber security company FireEye has concluded that the government probably supports at least some of the many hacking activities. China is mainly engaged in cyber espionage in those countries. Taiwan also reports that China generally tries to

penetrate government systems and there are growing fears that China wants to build the capacity to carry out cyber attacks that cause physical damage (Yu 2018).

Finally, China also conducts an active propaganda campaign in other countries, although the emphasis is not on publishing false reports that undermine the public debate but on spreading a positive image of China (Recorded Future 2019). For example, the country has spent a lot of money on advertisements on Facebook, a platform that is largely blocked in China itself (Mozur 2017).

All in all, the Chinese government’s ambition is to become a digital superpower that maintains tight control – in military, economic and cultural terms.

3.4 The Netherlands and other European countries

3.4.1 In brief

In many respects, the development of the digital world in the Netherlands and other European countries is similar to that in the United States. These countries are among the most digitally connected countries in the world and have a large and growing digital economic sector. Cyber security is therefore high on the agenda in European countries and they are strengthening their cyber defence and intelligence services in order to defend their digital infrastructure.

Nevertheless, the European countries differ from the US in two respects. Firstly, they go further than the US in terms of regulating the digital industry. Secondly, there is increasingly intensive cooperation between European countries to promote cyber security, for example at EU level. Since we will discuss these international activities in the next chapter, they will only be described concisely here. We look at the Netherlands and give examples of developments in France, Germany and the UK. These countries are of particular importance in Europe because of their economic and, especially in the case of France and the United Kingdom, military strength.

3.4.2 Strategic development

The European economies, particularly the Dutch economy, are highly digitised. European countries already constitute an interesting market for American giants like Microsoft, Google and Apple (European Commission 2018a). Furthermore, there are a lot of digital companies in the countries themselves, for example in the domain of financial technology. However, Europe has no cyber giants on the scale of Facebook or Alibaba. This raises the question of what European countries can do to counter these economic powerhouses. The influence of large digital technology companies raises objections, for example in the context of Facebook and personal data (Solon 2018) and AirBnB and the hotel sector (Coldwell 2014). Numerous initiatives have been taken at European level to regulate the digital economy, a number of which are discussed in the following chapter.

Box 7 The European countries' offensive cyber capabilities

The Netherlands, France, Germany and the United Kingdom are all building offensive cyber capabilities. In 2014, for example, the Dutch government established the Defence Cyber Command, which falls directly under the Commander of the Armed Forces. The cyber command had a staff of 80 at the beginning of 2017; the current government plans to increase future investment in it (Rigter 2017, De Telegraaf 2018).

France's ambition is to have a 'fourth army' of 3,200 cyber soldiers by 2019 (Pennetier 2017) and Germany wants to have a defence-oriented army unit of 13,500 soldiers and civilian employees by 2021 (O'Conner 2017). Germany also recently announced that it plans to develop its own cyber defence technology rather than buying it from foreign companies (Delcker 2018). The United Kingdom has formed the 77th brigade comprising around 1,500 regular soldiers and reservists (MacAskill 2015, Sengupta 2015).

The intelligence services in the Netherlands and other European countries are also developing offensive cyber capabilities. The Netherlands has the AIVD and the MIVD. Substantial cuts were made in the AIVD's budget in 2013; the budget was reduced from € 195 to € 125 million (Versteegh 2017). But the budget has been increased again in the ensuing years, partly in response to the increasing cyber threat, to approximately € 250 million now (Rijksbegroting 2018). The agency's target in the coming years is to have a workforce of between the 2,000 and 2,200 FTEs and it is tightening its focus on cyber capacity. A similar trend is evident at the MIVD, which is investing more and more in cyber capabilities and whose budget had risen to around € 100 million in 2018 (Rijksbegroting 2018). By comparison, Britain's GCHQ, the equivalent of the AIVD, received around £ 1 billion (€ 1.11 billion) and employed around 6,100 people in 2013 (Hopkinds et al. 2013).

The same combination of participation and regulation is evident in relation to offensive cyber capabilities: like the United States, European countries such as the Netherlands, France, the United Kingdom and Germany want to possess the capacity to defend themselves in cyber conflicts. A lucrative market for offensive cyber capabilities has also grown up in the European Union, in which various companies offer their services (Stockton & Golabek-Goldman 2013). At the same

time, these countries want to embed their offensive capabilities in clear national and international regulatory frameworks (UK Government 2016, Federal Ministry of the Interior 2011, Ministry of Foreign Affairs 2017, France Diplomatie 2018, Mackenzie 2019).

One example of this is the Netherlands' new Intelligence and Security Services Act. The law expands the powers of the intelligence and security agencies, but also contains safeguards, for example in relation to the authorisation of hacking by the AIVD. The introduction of the law prompted an intensive public debate which led, among other things, to the organisation of a consultative referendum in which the electorate could vote for or against the law. A narrow majority of the voters voted against it, whereupon the government promised a number of additional safeguards and implemented the law. This process illustrated that Dutch politicians take the normative frameworks for offensive cyber capabilities seriously and that it is possible to organise a fruitful public debate on this subject.

The emphasis on formulating standards is also a feature of the embedding of offensive cyber capabilities in the Dutch army. For example, a military cyber doctrine has been drafted and is regularly updated. The ministry of defence has also published a cyber strategy (Ministry of Defence 2018). But the Netherlands takes the view that standards should not only be adopted at national level, but more especially also at the level of international alliances such as NATO and the UN (Ministry of Foreign Affairs 2017).

European intelligence services, like those of the UK and France, are increasingly capable of hacking digital systems, gathering information and carrying out cyber sabotage (see box 7). They also actively use those capabilities. For example, the revelations by Snowden showed that the British GCHQ, in association with the American NSA, intercepted a lot of e-mail traffic. The Dutch AIVD is also reported to have passed on crucial information about the perpetrators of the attacks during the American elections in November 2016 to their American counterparts (Modderkolk 2018).

There is no evidence that the Netherlands, Germany, France or the UK carry out disinformation campaigns, but that needs to qualified. The Snowden leaks revealed that the GCHQ has developed various tools for creating fake e-mails or influencing online polls (NBC 2014). It is therefore questionable whether the large European countries universally abstain from spreading disinformation.

Finally, it appears that the states investigated here do not carry out cyber attacks that cause serious sabotage. Naturally, it is also possible that some attacks of that nature are not reported. Jeremy Fleming, the GCHQ's director, threatened to

retaliate for the poisoning of the former KGB agent Sergei Skripal and his daughter with offensive cyber capabilities (Binding 2018). The Netherlands, France, Germany and the UK are still expanding their capabilities for carrying out cyber sabotage, but have not yet used this arsenal in a clearly observable manner.

3.5 The international attitude of the states: an overview

We will now present a brief survey of the activities of the states discussed.

The **United States** is highly active in gathering intelligence about other states and tries to establish structural and hidden access to hostile digital networks. As far as is known, the US has not carried out any targeted disinformation campaigns in other countries. Time will tell whether the current government's attitude culminates in the international spread of disinformation. The Stuxnet operation shows that the US has caused serious physical damage with cyber tools (Rid 2012). The attack on North Korea's digital infrastructure, in the wake of the Sony hack, demonstrates the willingness of the US to engage in cyber sabotage. But there are also signs that the government and the defence agencies are struggling with this capacity. There have been indications recently that the US is willing to use more severe forms of cyber sabotage if the country is provoked too much, for example by Iran.

As regards **Russia**, the conclusion is that the Russian government actively undermines the rule of law and free democracy both in the domestic political processes and the political processes of other states. Russia uses espionage and disinformation to undermine the democratic process and to destabilise a society. But Russia goes even further in its own region, where cyber sabotage has been used on numerous occasions to cause serious physical damage, for example with the attacks in Ukraine. Russia's cyber activities in Ukraine coincide with conventional military action.

Chinese government agencies very probably also try to hack the systems in other states on a large scale and have been guilty of economic espionage. The Chinese government also uses the digital environment to spread disinformation in China; the international information campaign is mainly intended to present a positive image of China. China also wants to be capable of carrying out more severe cyber sabotage, and even winning a war. However, in contrast to Russia, up to now it has made scarcely any use of these capabilities.

The intelligence services of **the Netherlands and other European countries such as the UK, France and Germany** also engage in cyber espionage. At the moment,

they very seldom seem to use targeted disinformation campaigns in other countries, although Britain's GCHQ has developed the capacity to conduct such campaigns. There are no known examples of European hack attacks that have caused sabotage with serious physical consequences. That does not rule out the possibility that such attacks, or less serious cyber sabotage, do occur. There is also a discrepancy in the scale of the intelligence activities of Britain's GCHQ and the Dutch AIVD, for example. Finally, there are no known examples of cyber attacks that have clearly led to a situation of war.

3.6 The cyber escalation ladder

3.6.1 The information conflict

A number of things stand out in this overview. States are becoming increasingly professional in the integration of their offensive cyber capabilities in their military and intelligence organisation. Various countries constantly dare to attack the military superpower, the United States. But the most striking fact is that these operations never lead to a declaration of war. For example, Russia has repeatedly attacked vital American infrastructure but is still not in a state of war with the US (Klimburg 2017). China has been spying on other countries for more than a decade, but at the same time peacefully conducts trade with them.

Accordingly, cyber attacks usually occur in a situation between war and peace. They create a new dimension of conflict and diplomacy, which we call **information conflict**. The objectives in this information conflict vary:

- a state sometimes uses espionage to gain an economic advantage;
- a state is sometimes actually trying to prepare the military battleground in its favour; and
- a state sometimes wants to influence or manipulate political decision-making in another state.

The information conflict has one crucial characteristic: citizens are in the firing line in the information conflict. A foreign power that wishes to gain access to a company's digital system can do so by hacking an employee's home network and hoping that he connects his work computer to it. Equally, disinformation campaigns are targeted at the information provided to citizens, for example by falsely accusing particular politicians and manipulating voters. Finally, public services – for example banks, the energy sector and even hospitals – suffer, intentionally or unintentionally, from cyber attacks and the consequences of an attack affect citizens.

Accordingly, cyber attacks strike at the vital heart of society. This raises the comparison with conventional warfare: one of the main objectives of international humanitarian law is to ensure that civil facilities are spared and to ensure that parties to the conflict exclusively target participants in the military conflict. This raises the question of whether cyber attacks should not have to comply with the same rules. We return to this question in chapter 4.

3.6.2 Cyber peace and cyber-physical warfare

The information conflict can be described as a conflict between peace and war and therefore has implications for how we think about peacetime and wartime. Peacetime is distinguishable from **cyber peace**, and we can understand war as **cyber-physical war**.

This is because a period of cyber peace is not just a period of peace, but also a period when there is no information conflict with a particular state. Countries are not conducting cyber espionage against one another and are not using cyber weapons to cause damage in another country. Nor are they conducting disinformation campaigns. The emphasis in this situation is on strengthening cyber security. A country can even choose for pacifism and, for example, decide not to build up offensive capabilities and release as many zero day vulnerabilities as possible. But states can also train cyber soldiers and purchase weapons. However, the capacity to build up offensive cyber capabilities in peacetime is limited: gathering intelligence about the adversary's cyber capabilities and systems is necessary both to establish one's own defence and to create offensive capabilities.

Nuance is also required in our understanding of war. Offensive cyber capabilities will probably play an important role in wartime: more and more military materiel is digitised and it can be extremely advantageous to confound the adversary's air defences through disinformation, for example. It is therefore useful to speak of **cyber-physical warfare**, where digital applications are integrated into the conventional military arsenal, for example in the form of remote-controlled drones that can drop explosives.

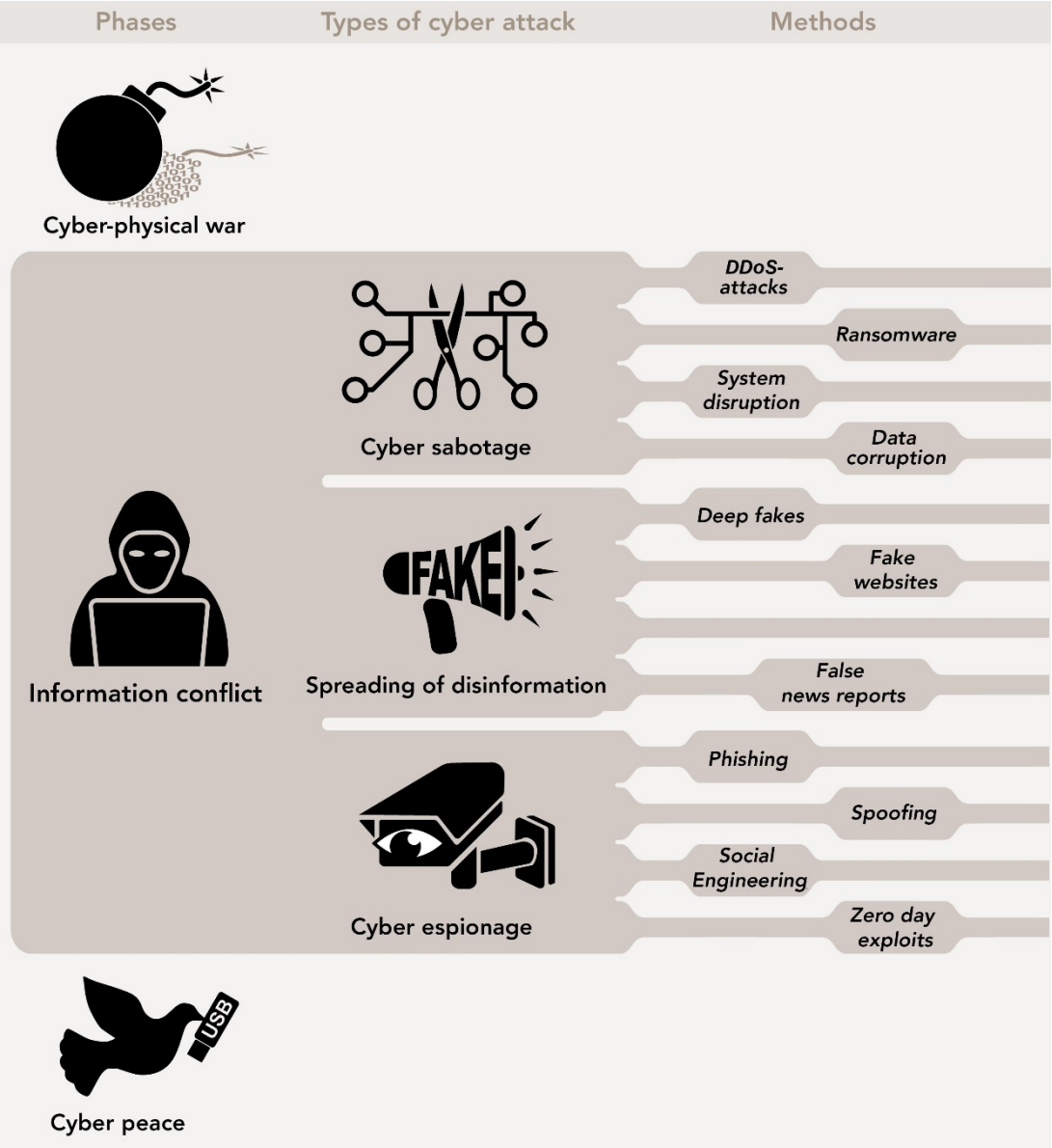
Table 2 The cyber escalation ladder

Rung	Situation	Intention	Damage	Characteristic of conflict
3	**Cyber-physical war** *- in wartime*	Military victory	Damage caused is defined as an armed attack	Integration of cyber in military operations
2	**Information conflict** *- in peacetime*	- experiments with weapons, - political pressure, - preparation of digital battlefield, - political destabilisation, - strengthening own cyber defences	Serious physical damage caused, undesired dissemination of information, manipulation through disinformation	New form of conflict
1	**Cyber peace** *- in peacetime*	Peace / neutrality	No damage	Pursuit of permanent peace

To sum up, we refer to an **escalation ladder**. This ladder embraces the three phases of international relations that were mentioned above: phases between states of cyber peace, information conflict and cyber-physical warfare (see table 2). These phases can be seen as rungs on a ladder. In ascending order, the phases become increasingly hazardous for society: an escalation can occur from peace to information conflict, and from information conflict to cyber-physical warfare.

Given the actions and strategies of the states that were investigated, the current international situation can best be described as an information conflict. Figure 3 illustrates the information conflict.

Figure 3 The information conflict



3.7 Conclusion

This chapter outlined the international situation in terms of offensive cyber capabilities on the basis of a survey of the major powers and European countries. These are the main findings:

- The traditional military superpowers, the United States and Russia, the new global power China and European countries acknowledge that the digital domain forms a new, fifth dimension of conflict and war. These countries all want to be capable of defending themselves against attacks in the digital world and carrying out attacks of their own. **A worldwide build-up of offensive cyber capabilities is therefore underway and we can speak of a militarisation of the digital world**. All of the countries discussed have greatly expanded their capacity to carry out cyber espionage and sabotage in the last few years, and most have acquired the capacity to spread disinformation.

- **This build-up can be described as an arms race**. China, Russia, the US and European countries all want to be able to defeat cyber attackers and to possess superior offensive cyber capabilities. This has led to an arms race, in which the build-up of capabilities in China, say, prompts the US to build further capabilities, which in turn prompts China to buy even better cyber weapons, and so on.

- **Almost every state engages extensively in cyber espionage, sometimes even secretly gathering intelligence about allies.** In this respect, China stands out for the extent of its economic espionage. The many hacks carried out by the country are anything but harmless – they demand a response in terms of improvements to security measures, the closing of software leaks, etc. Depending on the attack, these measures can be very expensive.

- **Some countries, and Russia in particular, launch disinformation campaigns in other countries.** It is also clear that authoritarian, anti-democratic regimes such as the governments of China and Hungary conduct domestic disinformation campaigns – and the US government also regularly spreads disinformation. But it is questionable whether these campaigns are also consciously used against and in other states.

- **It is plausible that Russia and the US have engaged in severe cyber sabotage.** This idea is prompted mainly by the NotPetya attack in Ukraine and the Stuxnet attack in Iran, although the states have not confirmed these attacks. China and European countries seldom if ever resort to serious cyber sabotage – or are capable of doing it without being exposed. Finally, the Russian operations in Ukraine go beyond the information conflict, since they also involve conventional military attacks.

- **The large states have varying strategic perspectives**. Russia, a state that does not have a functioning democratic legal order, tries to destabilise foreign democracies and pollute the public debate with untruths. On the other hand,

the US and European states like Germany and France see themselves as the guardians of the democratic legal order. In China, finally, the control of information and propaganda is primarily internally oriented and the country's priority, in addition to building up its defensive capabilities, is economic espionage. **None of the investigated states embrace an explicitly peace-oriented perspective**, aimed at continuing to act as far as possible on the rung of cyber peace, with little espionage and little build-up of offensive cyber capabilities.

- **Citizens and civil facilities constitute key targets of cyber attacks**. From disinformation campaigns to the infiltration of power stations and bombardment of financial services: citizens constitute an important target of cyber attacks. States hope to influence other countries by misleading citizens, stealing their secrets and frustrating their services.

- **There is no cyber war per se**. Our research failed to reveal a single situation where an individual cyber attack was followed by a declaration of war by a state.

4 International cooperation for a safe and free digital world

This chapter surveys how the Netherlands and the other countries discussed earlier work together to create a safe and free digital world. We look at the most important international alliances, such as NATO, the EU and the United Nations. We begin by discussing the most important worldwide organisations and then consider the regional alliances. We will again also outline the environment in which the Netherlands finds itself. It is not our intention to provide a comprehensive picture of every international initiative.

4.1 Worldwide organisations

Numerous international organisations contribute to international cyber security and cyber peace. The most important are:

- the United Nations (UN);
- the International Telecommunication Union (ITU);
- worldwide public-private alliances, such as:
    a. the International Multilateral Partnership Against Cyber Threats (IMPACT);
    b. the Internet Corporation for Assigned Names and Numbers (ICANN);
    c. the Global Forum on Cyber Expertise;
    d. the Paris Call for Trust and Security in Cyberspace;
    e. the Cyber Security Tech Accord;
    f. the Global Forum on Cyber Expertise;
    g. the Global Commission on the Stability of Cyberspace; and
    h. the global Forum of Incident Response and Security Teams (FIRST).

4.1.1 United Nations (UN)

The United Nations is a logical forum for making worldwide agreements on offensive cyber capabilities and has in fact endeavoured to do so in recent years.

Since 2001, initially at the initiative of Russia in the **Disarmament and International Security Committee**, various sessions of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (abbreviated as **UN**

GGE) have been organised. The group consists of representatives from fifteen states, which are together geographically representative of the entire world. The aim of the group is to reach a consensus on the principles, measures and standards that countries should observe in dealing with information technology in the context of security.

The group is given a new mandate every few years and had mixed success from 2001 onwards. Between 2009 and 2015, successive UN GGEs appeared to be making good progress. For example, they stipulated that countries should not permit malevolent cyber activities in their territory and that countries should not attack critical infrastructure with cyber capabilities, unless it was permitted by international law (for example, if the country was the victim of an armed attack) (UN GGE 2015). Although the agreements were voluntary, they provided more guidance for responsible conduct by states in the digital environment.

However, since 2015 progress has been slow. In 2017, the fifth UN GGE was unable to submit a report containing any agreements to the UN General Assembly. The sticking point was the precise application of international law, and in particular international humanitarian law, to cyber operations (Soesanto & D'Incau 2017). For example, the United States wanted an agreement that a country that suffers a cyber attack is entitled to retaliate. Cuba, and probably also Russia and China, objected to this proposal. Cuba warned of the militarisation of cyberspace and argued that the application of international humanitarian law would legitimise a war scenario in cyberspace. It is possible that Russia and China feared the superior capabilities of the US and wanted to build up and test their own capabilities, preferably under the radar and without too many repercussions. Whatever the case may be, the dispute negated a lot of progress that had been made, because the earlier agreements are now also in jeopardy (Soesanto & D'Incau 2017).

At the end of 2018, the diplomatic process split into two parallel trajectories, illustrating the international differences. On the one hand, a U.S.-led group of mostly western countries, among which the Netherlands, France and Germany, pushed for a sixth GGE that began its work in 2019 (UN General Assembly 2018a). This GGE again consists of representatives of a select group of 25 states, and is meant to function as the primary forum for diplomatic discussions about cyberspace and international security. In this edition, the Netherlands is also a member. On the other hand, a Russia-led group of states, among which China and Pakistan, proposed to set up an open-ended working group (OEWG) in which all UN-member states can participate (UN General Assembly 2018b). This working group also started to operate in 2019. The open-ended working group has been criticized by the United States and other Western states for misrepresenting the work of previous GGE's and for making it much harder to achieve a global consensus in the

future (Grisby 2018b). This fear might be well-founded, especially if the two groups will ultimately propose different norms for state behaviour in cyber space.

Cyber security is also investigated and discussed in other UN bodies, which can also submit resolutions to the General Assembly.

- The **Economic and Financial Committee** adopted resolutions in 2002, 2003 and 2009 to promote a 'global culture of cyber security'.
- The **Social, Humanitarian and Cultural Committee** has mainly discussed privacy issues.
- The **Economic and Social Council** devotes growing attention to combating cyber crime (UN ECOSOC 2011).
- Issues of international peace and security are naturally also discussed in the **Security Council**.

However, none of these forums have offered more specific suggestions for dealing with the cyber capabilities of states than the proposals made by the UN GGE.

4.1.2 International Telecommunication Union (ITU)

The International Telecommunication Union (ITU) is the UN's specialised agency for information and communication technology. The organisation has 193 member states and roughly 700 important players in the ICT sector participate in its activities. The ITU has three official tasks:

1. allocating radio frequencies and regulating satellite technology;
2. developing ICT standards; and
3. promoting access to ICT (ITU 2018).

The ITU has taken various initiatives to promote worldwide cyber security.

In 2007, the ITU launched the **Global Cybersecurity Agenda** (GCA), a project designed to promote confidence and security in the digital context (ITU 2018). Among other things, the GCA promotes the collection and discussion of legal and technical measures and forms of international cooperation. To give the GCA more substance, a High-Level Expert Group (HLEG) has been established, which is also comprised of cyber-security experts from around the world. In 2008, for example, the HLEG published a report with numerous proposals for improving cyber security (ITU 2008). The HLEG mainly facilitates the exchange of good ideas; it does not propose measures to be imposed universally.

The ITU also organises the annual **World Summit on the Information Society Forum** (WSIS forum). The conference has very broad goals: making ICT

accessible to everyone, anywhere in the world, and properly guiding that process. In that context, cyber security is also discussed at the WSIS forums. The WSIS forum is attended by a great many participants from civil society, business and governments and is one of the most important annual conferences on ICT governance.

The ITU also monitors the level of cyber security in countries. According to the ITU, for example, in 2017 the Netherlands was ranked 17th on the **Global Cybersecurity Index,** an international table measuring countries' commitment to cyber security (ITU 2018). The GCI's table ranks 193 countries on the basis of aspects such as national policy, legal approach and the existence and expertise of organisations engaged in cyber security.

Finally, the ITU assists national **Cyber Emergency Incident Response Teams** (CERTs), provides support for countries on issues relating to legislation on cyber security, and informs developing countries about cyber crime (see also FIRST below).

4.1.3 Public-private global alliances

International Multilateral Partnership Against Cyber Threats (IMPACT)
The International Multilateral Partnership Against Cyber Threats (IMPACT) is the first cyber security alliance supported by the United Nations. IMPACT's task is to provide assistance and support in the area of cyber security to the 193 member states of the ITU and to other organisations within the UN on the basis of a cooperation agreement (IMPACT 2018).

With a total of 152 countries that are now formally members of the ITU-IMPACT coalition and with strong support from multinationals, partners in the academic community and international organisations, IMPACT is the largest cyber-security alliance of its kind.

Internet Corporation for Assigned Names and Numbers (ICANN)
The Internet Corporation for Assigned Names and Numbers performs what is perhaps the most important task in the digital world, that of managing what is known as the Domain Name System (DNS, ICANN 2018a). This system is described as the internet's address book and records all domain names and ensures that when a person enters a particular name or a particular number in the browser, the browser will actually navigate to the correct address (Klimburg 2017).

The importance of this agency for the functioning of the internet is beyond question: disruption of this navigation would make surfing impossible. And if malicious individuals disrupt the navigation, users could suddenly be directed to other sites. The cyber security of this system is therefore a very high priority for ICANN. In 2010, ICANN and the American government introduced improved security extensions, which have since been adopted by many important internet domains, such as .com and .de (ICANN 2018b).

ICANN is a so-called multi-stakeholder organisation, in which the business community, the public sector, governments, technological experts and various civil-society organisations are represented (ICANN 2018a). Its philosophy is that if the internet belongs to everyone, everyone must also be able to participate in the bottom-up management of the internet. ICANN also recently became an entirely independent organisation. The authority to manage the Domain Name System was based on the IANA contract between ICANN and the American government (ICANN 2018a). As a result, the internet was to a certain extent more the property of the United States than of other states. But after a lengthy process, the competence to manage the DNS was assigned to ICANN in October 2016.

Not all states are equally enthusiastic about the broad social embedding of the authority for managing the DNS. Russia and China, for example, proposed transferring competence to the ITU so that states would have a stronger role in managing the internet and, for example, would be able to monitor dissidents even more closely (Klimburg 2017). But this scenario has become very unlikely since the American government surrendered its jurisdiction over the DNS. Nevertheless, Russia and China regard the existing governance situation as being to their disadvantage and oriented towards the West (Klimburg 2017). They are therefore looking for alternatives to ICANN. Russia reportedly wants to develop a separate internet with the other so-called BRICS countries (Brazil, India, China and South Africa), with its own DNS system (UAWIRE 2017). According to the Russian government, this would make their digital capabilities less vulnerable to Western attacks.

Paris Call for Trust and Security in Cyberspace

The Paris Call for Trust and Security in Cyberspace was published at a conference in Paris on 12 November 2018. The document contains principles for a safe cyberspace (France Diplomatie 2018, Matsakis 2018). It explicitly states that international law applies to information and communication technology and stresses the importance of the standards that have been adopted at UN level. Although the document does not have the status of a binding international treaty, the signatories have again given those standards of responsible state behaviour greater authority.

After all, the UN GGE process had come to a standstill. The negotiations that this document has initiated could also culminate in binding international agreements.

The document speaks out against back-hacking by non-state actors, calls for measures to prevent the proliferation of dangerous ICT tools, and announces that further meetings will be held in 2019 to flesh out the basic principles. The document was signed by more than 50 states, including France, the United Kingdom, the Netherlands, Germany, Canada and Japan, as well as many African and Asian countries.

A number of important countries have not signed the Paris Call for Trust and Security in Cyberspace, including China, Iran, Israel, the United States, Russia and North Korea. This is significant, since these are precisely the countries that possess very extensive offensive cyber programmes and have actually used them. It shows that although there is a growing consensus on the need to regulate offensive cyber capabilities, there is still a long way to go before a genuine worldwide approach, with the cooperation of the current cyber superpowers, can be reached.

Finally, numerous civil-society organisations and universities have also signed up to the Paris Call. The agreement is therefore supported by a large proportion of the major players in the cyber domain.

The Cybersecurity Tech Accord

The Paris Call was also widely embraced by the international business community. For example, the document is endorsed by the signatories of the Cybersecurity Tech Accord (CTA 2018), a cooperation agreement concluded between more than 60 multinational companies, including Microsoft, Facebook, Dell and KPN. Companies like Google and Samsung have also endorsed the Paris Call.

The Cybersecurity Tech Accord contains a set of joint commitments with consequences for the relationship between these companies and governments. Examples include the commitment never to help governments to launch cyber attacks against innocent civilians and companies or the promise to protect their products against clandestine influence and sabotage. Although the impact and precise practical significance of the agreement remains to be seen, this alliance could impair the capacity of governments to launch espionage and sabotage operations with the help of companies. The message that resonates in a number of passages in the agreement is that the companies are aware of recent international developments and wish to avoid being involved in the build-up of offensive cyber capabilities by states.

The agreement is based on four key principles: strong defence, no offence, capacity building and collective response. The first two are particularly significant for the position taken by the companies.

Global Forum on Cyber Expertise
The Global Forum on Cyber Expertise is a joint organisation of governments, businesses and civil-society organisations that emerged from the fourth Global Conference on Cyber Space in The Hague in 2015. The organisation's goal is to improve cyber capacity and expertise worldwide by promoting access to internet, safeguarding online rights and providing cyber security. These ambitions are set out in the Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building (GFCE 2017).

The GFCE's activities centre mainly on knowledge exchange. The organisation continues to organise an annual conference and has formed working groups specifically dedicated to a particular aspect of cyber security, such as cybercrime, protecting vital infrastructure and the development of cyber capabilities.

The Global Commission on the Stability of Cyberspace (GCSC)
The Global Commission on the Stability of Cyberspace is a commission that supports the development of policy and norms related to the stability and security in and of cyberspace (GCSC 2019). The commission was initiated by the *The Hague* center for strategic studies and the EastWest Institute and is supported by public actors such as the Dutch, French and Singaporese governments and private actors such as Microsoft. It has published several norm packages, proposing norms on for instance the protection of electoral infrastructure and the public core of the internet.

Forum of Incident Response and Security Teams (FIRST)
The Forum of Incident Response and Security Teams (FIRST) is a worldwide consortium of Computer Emergency Response Teams (CERTs) or Cyber Emergency Incident Response Teams (CSIRTs) (FIRST 2018). These teams are also referred to as the 'internet's fire brigade' because they provide assistance in restarting digital systems in the event of major incidents. The teams come from both the public and the private sector and can learn from FIRST's best-practice documents and by attending the technical colloquia and the annual conference it organises.

The Dutch ministry of defence's CERT, DefCERT, has joined FIRST, as have the teams from ING, KPN, Rabobank and SIDN, among others.

4.2 Regional organisations

Regional organisations are at least as important as global organisations and partnerships for the Netherlands, particularly because the Netherlands usually operates internationally under the auspices of the EU and NATO. We also discuss the Shanghai Cooperation Organisation (SCO), the Organisation for Security and Cooperation in Europe (OSCE), the Five Eyes alliance and SIGINT Seniors.

4.2.1 European Union (EU)

Cyber security is a central theme in the European Union's general security strategy and the European Commission has published various strategic documents on the theme (EC 2013). More specifically, in April 2016, the High Representative of the Union for Foreign Affairs and Security Policy proposed actions to make Europe more resilient against hybrid threats, of which cyber attacks are a key component (EC 2016). The document proposed a total of 22 actions, a significant number of which have already been translated into specific policies.

Here we review the four EU initiatives that are most relevant for cyber security:
1. the Network and Information Security Directive, adopted in 2016;
2. the Cyber Security Act, adopted in 2019;
3. the instruments for cyber diplomacy drafted in 2017 and adopted in 2019; and
4. the EU initiatives against disinformation.

The Network and Information Security Directive (NIS Directive)
The directive is the outcome of more than three years of work by the European Commission, the European Council and the European Parliament, in association with stakeholders from Europe and the rest of the world. The aim of the NIS Directive is to provide a uniform response to the growing concerns about cyber threats. In the Netherlands, a law has been drafted to implement the directive and has been approved by both Houses of the States-General.

The directive consists of two parts. The first part requires suppliers of essential services, such as energy companies and care institutions, to take responsibility for cyber security. It imposes less stringent requirements on suppliers of digital services, such as online market places and online search engines. It is left mainly to the member states to specify precisely what those responsibilities entail.

The second part concerns the formulation by the member states of a national security strategy and obliges member states to establish Computer Security Incident Response Teams (CSIRTs, which have the same purpose as CERTs)

capable of detecting, preventing and tackling cyber incidents and risks. This latter requirement is particularly important for international cooperation, since these teams can also assist one another at international level.

CSIRTs deal with security emergencies, promote the use of validated security technology and safeguard the continuity of important networks. In practice, this means that CSIRTs concentrate mainly on identifying vulnerabilities and improving the communication between security firms, users and private organisations. Although the majority of the CSIRTs were founded as non-profit organisations, many have become public-private partnerships in recent years (Choucri et. al. 2014). There are now more than 200 CSIRTs in 43 countries, including a large number in the Netherlands.

There used to be little effective cooperation between the CSIRTs because the methods of data collection were not streamlined and therefore the availability and reliability of reported information varied greatly (Choucri et. al. 2014). The NIS Directive therefore emphasises the need for effective coordination between the member states and provides that a CSIRT network will be established, including a CSIRT at EU level. The CERT-EU will be given the task of ensuring coordinated and effective action at European level if European institutions and organisations are confronted with cyber attacks. The CERT-EU will work closely with the CSIRTs of the EU member states, with ICT security companies in Europe and with NATO.

The hope is that by sharing information throughout the EU it will become increasingly difficult for networks to be attacked and easier to identify and prosecute perpetrators, and that this will serve as a deterrent. In the words of the Commission:

> ‘As long as the perpetrators of cyber-attacks – both non-state and state – have nothing to fear besides failure, they will have little incentive to stop trying. A more effective law enforcement response focusing on detection, traceability and prosecution of cyber criminals is central to building effective deterrence. (European Commission 2017a, 3)

The Cybersecurity Act

In June 2018, the European Union intensified its policy in relation to cyber security. It drafted the Cybersecurity Act, a regulation that contains two important elements: expansion of the mandate and the tasks of the European Agency for Network and Information Security (ENISA) and the introduction of an EU-wide certification system for digital services and products (European Commission 2017b). Since regulations have direct effect and therefore leave little room for interpretation by the member states, with this instrument Europe’s digital environment will be more explicitly governed by the Union. The regulation was passed by the European

Parliament and formally approved by the European Council and entered into force on 27 june 2019.

Certification is intended to ensure that digital products and services comply with minimum security requirements throughout the Union and thus remedy numerous weak links in the Internet of Things (IoT). Chapter 2 already showed that the emergence of the Internet of Things is accompanied by numerous security risks and with this regulation the Commission is taking an important step to address that problem.

The expansion of ENISA is intended to emphasise the agency's status as the most important European body in the domain of cyber security. When the regulation enters into force, ENISA will be the European Commission's principal advisory body in the area of cyber security. ENISA will also be required to provide powerful support for member states in creating and tightening up the CSIRT structure that has been created on the basis of the NIS Directive. The enlargement of ENISA seems to be a response to the desire to bring more clarity to the extensive governance structure that the EU has established in the domain of cyber security (see box 8).

Box 8 Other EU cyber security initiatives

Within the EU's intelligence and situation centre (IntCen), which is itself part of the European External Action Service (EEAS), a special 'Hybrid Fusion Cell' has been created to analyse cyber incidents and to provide a platform for sharing intelligence. The European Commission recently called for a further expansion of the platform's capacity (European Commission 2017a).

In October 2017, the European Centre of Excellence for hybrid threats was officially opened in Helsinki, where research is conducted into the nature of hybrid threats and how they can be prevented. Membership of the centre is open to all EU and NATO member states; the Netherlands and a number of mainly North European countries and the United States have joined.

Since 2010, ENISA has been organising large cyber-security exercises, the fifth of which was held in June 2018. That exercise involved a simulation of escalating cyber attacks in the aviation sector. During the exercise, 900 cyber security professionals from 30 European countries had to neutralise the attacks (ENISA 2018).

Cyber diplomacy toolbox and Council Decision against cyber attacks

The Foreign Affairs Council, comprising the ministers of foreign affairs of the EU member states, has approved a framework for a joint EU diplomatic response to malicious cyber activities (European Council 2017). This framework is also known as the EU Cyber Diplomacy Toolbox and builds on existing diplomatic frameworks in the European Foreign and Security Policy. For example, restrictive measures can be taken in response to cyber attacks, such as imposing trade sanctions, freezing financial assets and breaking off diplomatic relations.

This toolbox laid the foundation for the binding decision and regulation he European Council published respectively on 14 and 17 May 2019, which sets up a regime for taking restrictive measures against cyber attacks threatening the EU and its member states (European Council 2019a and 2019b). It mainly provides rules for freezing funds and for preventing attackers from travelling to or through the territories of member states.

The EU initiatives against disinformation
Tackling the spread of disinformation is high on the EU's agenda and various measures have already been adopted (EC 2018c). For example, the European Centre for Press and Media Freedom invests in international investigative journalism and the European Commission has established a special anti-disinformation task force: the EU vs. disinformation campaign (IJ4EU 2018, EUvsDisinfo 2018). One aspect of this campaign is the maintenance of a unique and publicly accessible database containing examples of disinformation – more than 3,800 cases of disinformation were added between September 2015 and the spring of 2018. The campaign also includes training for member states and EU institutions in dealing with disinformation.

Finally, a Code of Practice on Disinformation has been developed. This non-binding document provides suggestions on how parties such as online platforms, social networks and advertisers can prevent disinformation (EC 2018b). Various large tech companies, including Twitter, Google and Facebook, have said they will adhere to the code and have presented plans to implement it successfully (Euractiv 2018). The code requires, for example, that companies must not accept money from advertisers who wish to place misleading information about themselves and is also aimed at significantly improving the monitoring of advertisements.

Some of the Commission's initiatives are controversial. Some media, including Dutch newspapers and websites, fear that the measures will lead to censorship. There is particular criticism of the anti-disinformation task force, for example because it described articles in Dutch publications such as De Gelderlander and The Post Online as fake news – these accusations have since been withdrawn. In March 2018, the Dutch House of Representatives adopted a motion calling for the abolition of EUvsDisinfo, which the government adopted after some resistance (NOS 2018).

The EU is pursuing many more initiatives to promote cyber security, the most important of which we present in Box 8.

4.2.2 North Atlantic Treaty Organisation (NATO)

Cooperation is also sought within NATO. We discuss this cooperation in more detail here because of its importance for the Netherlands.

In the wake of the cyber attacks on vital institutions in Estonia in 2007, cyber security became an important issue on NATO's agenda (Healey & van Bochhoven 2011). After all, a member state had sustained serious damage that was very

probably caused, or at least permitted, by another state: the Russian government. Since then, NATO has taken numerous initiatives. They have followed two tracks: strengthening defensive cyber capabilities and regulating the use of offensive cyber capabilities.

Strengthening defensive cyber capabilities

The North Atlantic Treaty Organisation (NATO) has traditionally been a defensive organisation with the task of supporting and coordinating the capacity of the member states to defend themselves against hostile attacks and to retaliate effectively. Since the NATO conference on the subject in Prague in 2002, NATO has issued various declarations at conferences and published factsheets and strategic visions indicating how it tries to achieve those objectives in cyberspace (see, *inter alia*, NATO 2002, 2008, 2011, 2016a). Various specific measures have been adopted, of which the following three are the most important.

The first was the establishment in 2008, by the North Atlantic Council, NATO's primary executive body, of the **Cyber Defence Management Authority** (CDMA, NATO CCDCOE 2018) to coordinate, assess and suggest improvements in the defence capabilities of the member states (Burton 2015). This is done in close consultation with the member states, since the soldiers and tanks, and the cyber troops and cyber technology, belong to or are the property of the member states themselves. The CDMA makes specific agreements with the governments of member states on improvements in cyber capabilities and documents them in memoranda that are signed by both parties.

Secondly, in 2012, various NATO units were merged to form the **NATO Communication and Information Agency** (NCI Agency 2018). This broad-based agency is very important for the cyber capabilities of the member states. For example, it is responsible for the digital communication between NATO troops and for the security of digital networks; it supplies the IT structure for the NATO institutions; and it certifies the IT technology used by the armies of the member states (NCI Agency 2018). The agency also manages the NATO Computer Incident Response Capability (NCIRC), NATO's CSIRT teams, which have to be able to provide rapid assistance in the event of cyber incidents in one or more member states. Finally, the agency provides a forum for the exchange of intelligence and organises major conferences where politicians, army staff and private partners discuss issues relating to cyber security.

Thirdly, in 2004, Estonia proposed setting up a centre of expertise on cyber defence within NATO. In October 2008, the **Cooperative Cyber Defence Centre of Excellence** (NATO CCDCOE) in Tallinn was fully accredited as a NATO organisation. The centre is now sponsored by most NATO member states, including

the United States, the United Kingdom, France, Germany and the Netherlands. Experts from more than twenty countries collaborate in the centre generating knowledge about cyber security and disseminating it among the centre's partners. The centre also organises the technical cyber-defence exercise Locked Shields and the CyCon conference. A very important aspect of the centre's work is the development of the Tallinn Manuals (Schmitt 2013, 2017), in which a special group of experts makes proposals relating to the application of international law to cyber operations. This initiative brings us to the second track of NATO activities: the regulation of the use of offensive cyber capabilities.

Regulation of the use of offensive cyber capacities

As already mentioned, the emphasis of NATO's cyber policy lies in strengthening the defences of the NATO member states: 'The keynote is defence, whether an attack comes from state, criminal or other sources', a NATO spokesman has said (Grant 2008). NATO's defensive doctrine is based mainly on dissuasion or passive deterrence: 'deterrence by denial'. This means that security measures must be strengthened in such a way as to make it practically impossible, or in any case very expensive, for attackers to infiltrate systems (Healey & van Bochoven 2012). However, it is questionable whether passive deterrence is sufficient. Time and again, sophisticated or persistent hackers have demonstrated the ability to penetrate highly secured systems. Could NATO then adopt a more offensive role? Although it is possible that NATO's political and military command will be informed if a NATO member is involved in carrying out offensive cyber operations, particularly if they are part of a broader NATO mission, NATO's cyber command is not expected to perform an offensive role (Burton 2015).

Nevertheless, the question is whether the emergence of offensive cyber capabilities will alter anything in NATO's defensive character. The most important article of the NATO Treaty is article 5:

> 'The parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the party or parties so attacked by taking forthwith, immediately and in concert with the other parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.' (North Atlantic Treaty, Art. 5).

The previous chapter showed that Russia, China and countries such as Iran and North Korea regularly attack the digital networks of NATO countries. Is it not

therefore conceivable that article 5 could be activated? The NATO countries would then have to take collective offensive action to assist the country that was attacked.

This question prompted a lengthy debate within the alliance. The key question was whether a cyber attack can be deemed an 'armed attack'. In 2007, Estonia's minister of defence acknowledged that '[at] present, NATO does not define cyber-attacks as a clear military action. This means that the provisions of Article 5 of the North Atlantic Treaty, or, in other words collective self-defense, will not automatically be extended to the attacked country' (Traynor 2007). However, the major cyber attack on government institutions in Estonia in 2007 was generally seen as a security matter that concerned NATO (Traynor 2007). NATO's institutional adaptation with respect to the threat of cyber attacks continued in 2011 with the adoption of a revised Cyber Defence Policy, in which the emphasis was placed on minimum requirements for cyber defence of national networks, on an integrated system of cyber governance within NATO and on the need for a pragmatic response to cyber attacks (NATO 2011).

Finally, at a NATO summit in Cardiff in 2014 it was decided that a cyber attack could also trigger the defence mechanism of article 5 (NATO 2014). The alliance agreed to respond purposefully and proportionately to every significant cyber attack, depending on the scale of the damage, the degree of attribution and the motives and identity of the attackers (Abrial 2011). NATO defined significant cyber attacks as attacks with serious consequences for the economy, vital infrastructure and national security of NATO members. Precisely what a proportionate response by NATO would entail is unclear, however. Is a cyber counterattack proportionate? Or a conventional military attack? In other words, no specific plan of action is prescribed. But some member states, including the United States, are increasingly adopting a firm position – for example by suggesting that a conventional counterattack, and even a nuclear counterattack, is conceivable (U.S. Secretary of Defense 2018).

NATO has invested particularly in developing a common regulatory framework. With the involvement of the Netherlands, the Tallinn Manual was drawn up, which explains how international law applies to cyber operations. The manual, a second edition of which has been published (Schmitt 2017a), has promoted the legal and strategic thinking in NATO about important aspects of cyber security, although various problems and questions of interpretation remain (see, *inter alia*, Lucas 2017; Yoo 2015). This is due, among other things, to the fact that digital attacks that are not connected to conventional warfare are often difficult to describe as armed attacks (Fleck 2013). We discuss the Tallinn Manual in more detail in section 4.3.

To sum up, we can say that NATO takes its defensive task in relation to the threat of cyber attacks very seriously and has taken relevant steps to clarify its role with respect to offensive cyber capabilities. However, there are still many questions that need to be answered.

4.2.3 The Group of Seven (G7)

The Group of Seven, or G7, is an interstate consultative body (G7 2019a). The current members of the group are France, Germany, Italy, the United Kingdom, the United States, Japan and Canada. Delegates from the EU also attend all of its meetings. Russia was a member of the group until 2014, but was expelled because of its annexation of the Crimea. The group mainly discusses issues of international security, economic policy and energy policy. This distinguishes it from the Group of Twenty, the G20, which focuses mainly on economic affairs. Although major industrial powers such as China, Brazil and Mexico are not members of the group, talks are held between the G7 and these countries.

The subject of cyber security has occupied an increasingly prominent place on the agenda in recent years. In 2017, for example, the G7 published a Declaration on Responsible States Behaviour in Cyberspace, which suggested the possibility that states that are attacked could take counter-measures, including cyber counterattacks (G7 2017).

In 2018, the Charlevoix Commitment on Defending Democracy from Foreign Threats was published, with a list of action points designed to make the states more resilient against attacks that could undermine democratic processes – including cyber attacks (G7 2018). Among other things, it called for the creation of a Rapid Response Mechanism, a procedure that would enable states to quickly coordinate a joint response to an attack. The precise details of this mechanism have still to be fleshed out.

The most recent G7 meeting in April 2019 also produced concrete results. The joint ministers of foreign affairs published the Dinard Declaration on the Cyber Norm Initiative (G7 2019b). This non-binding declaration endorsed the agreements made at UN level by the GGEs in 2010, 2013 and 2015 and called on states to share relevant information and to cooperate more closely. The ministers of foreign affairs also issued a communiqué in which they referred to the Rapid Response Mechanism and expressed the desire for a joint deterrent against cyber attacks (G7 2019c).

4.2.4 Shanghai Cooperation Organisation (SCO)

The Shanghai Cooperation Organisation, also known as the Shanghai Pact, is an international organisation of Asian and Eurasian countries. It has eight members: China, Russia, India, Pakistan, Kyrgyzstan, Tajikistan, Uzbekistan and Kazakhstan (SCO 2017). These countries meet regularly for talks and collaborate in numerous areas, including defence and security, and on combating the so-called ‘three evils’: extremism, separatism and terrorism (SCO 2006).

Two initiatives of the SCO are particularly important. In June 2009, the member states (which included India and Pakistan at the time) signed an agreement ‘on Cooperation in the Field of International Information Security’. The same countries also submitted an International code of conduct for information security to the UN General Assembly (CCDCOE 2018).

The former document mainly contains commitments to improve cyber security throughout the SCO region, for example in relation to protecting vital infrastructure and investigating cyber criminals.

The second document is a code of conduct for states. Among other things, it provides that states must respect each other’s sovereignty and not interfere in the affairs of other states or undermine the political stability of another country.

The term information security appears prominently in both documents. It is a controversial term because it is associated with censorship and control of the content of digital information (Klimburg 2017). For example, a dictatorial regime could prohibit unwelcome criticism and imprison dissidents under the guise of information security. These practices are not alien to the governments of some SCO member states, including China and Russia.

4.2.5 Organisation for Security and Cooperation in Europe (OSCE)

This international alliance is the largest regional organisation in the field of security and has 57 member states, including many countries from outside Europe, such as the United States and Russia. The OSCE was formed in the mid-1970s and served as a platform for consultation between the West and East during the Cold War. According to the OSCE, ‘security’ embraces a wide range of issues, including sustainability, democracy and cyber security. The organisation organises many activities designed to create security in this broad sense in all the member states (OSCE 2018).

In the area of cyber security, the OSCE actually focuses on the use of information technology between member states. The OSCE warns of the dangers of escalating cyber conflict and calls for more dialogue (OSCE 2016, De Gruyter 2018). In 2016, it adopted a number of 'confidence-building measures', including organising lines of communication and regular meetings between the member states and promoting transparency in the terminology that member states use to describe issues relating to cyber capabilities (OSCE 2016). The agreements also urge member states to deal responsibly with knowledge of digital vulnerabilities and to draw up a transparent classification of cyber attacks. Almost all of these measures were agreed on a voluntary basis. The OSCE cannot apply any sanctions if any of its member state fails to respect them or refuses to attend regular meetings, for instance. This reflects the OSCE's desire to be primarily a forum for dialogue rather than an organisation where member states make enforceable agreements.

4.2.6 Five Eyes alliance and SIGINT Seniors

After the Second World War, the US, the UK, Canada, New Zealand and Australia formed the Five Eyes alliance, primarily to share SIGINT intelligence (SIGINT stands for signals intelligence, or intelligence gathered on the basis of electronic signals) (Farrell 2013).

The American National Security Agency (NSA) and the British Government Communications Headquarters (GCHQ) are probably the most powerful agencies in the Five Eyes alliance. In the 1980s, the Five Eyes group was expanded to embrace other European countries, including the Netherlands, France, Italy and Germany (Gallagher 2018). This larger group of fourteen countries is called the SIGINT Seniors Europe; there is also a SIGINT Seniors Pacific. The countries all have military and general intelligence agencies that share information with each other. The Snowden leaks revealed that not only the NSA, but also the GCHQ, the German *Bundesnachrichtendienst* (BND) and the Dutch intelligence services actively gather and share intelligence (see, *inter alia*, Modderkolk 2018, Gallagher 2017). In June 2018, the powers of the intelligence services in the Netherlands to intercept communication were expanded by the new Intelligence and Security Services Act.

However, the cooperation between the intelligence services does not mean they share all of the available intelligence, that they always share information about methods of espionage, including sensitive software vulnerabilities, or that these countries do not spy on one another. For example, the French and German governments were outraged when it was revealed that the NSA had tapped

France's president François Hollande when he was in office, and the German Chancellor Angela Merkel (Agence France-Presse 2016).

4.3 The state of international regulation

Various collaborative efforts have been made in recent years to formulate rules for the development and use of offensive cyber capabilities. The results have been modest. Initially fruitful talks at UN level ultimately broke down; at NATO level, a number of important declarations were issued after lengthy deliberations; NATO also drafted the Tallinn Manual; the SCO also proposed a code, but it was greeted with little enthusiasm in the UN. What precisely do all these initiatives entail and precisely what rules apply between states? It is essential to answer that question for a proper understanding of the current international situation.

4.3.1 The nature of international law

To answer the question, it is necessary to make a number of remarks about the nature of international law. The law is clear when practically all countries have reached a mutual agreement, that agreement is interpreted in the same way by all the countries, the countries adhere to that agreement in practice, and there is a source of judicial rulings in which the details of the agreement are further explained and reaffirmed. In such a situation, if a state violates the rule, other states can hold the government in question accountable for a violation of international law. One example is the provisions of the EU treaties regulating the European elections. Those agreements are generally interpreted, enforced and complied with in a uniform fashion.

However, a lot of international law, including the international law on offensive cyber capabilities, is not so clear. It can and is interpreted differently by different states, starting with the most basic of questions: does international law actually apply to offensive cyber capabilities?

At UN level, the countries in the UN GGE – United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security – initially appeared to have reached agreement on this point (UN GGE 2015). For example, they found that international law does apply to information and communication technology and that principles such as humanity, necessity and proportionality should be respected in relation to the use of that technology. But the status of this earlier report in 2015 is now uncertain

because the most recent UN GGE expert group was unable to reach agreement on a final report (Soesanto & D'incau 2017).

Nevertheless, there is a growing consensus among states and legal experts that international law does have something to say about the use of offensive cyber capabilities (see, *inter alia*, the Paris Call 2018). But precisely what that means is less clear. In the following section we present a concise summary of the discussion that has been conducted among experts, primarily on the basis of the second edition of the Tallinn Manual (Schmitt 2017a). Note: the manual does not directly represent the views of the NATO member states – on a number of points, the member states still have to announce their interpretations of general obligations. It is also important to mention that the drafting of the Tallinn Manual was promoted by the Netherlands and is based, among other things, on the authoritative AIV/CAVV advisory report[9] on digital warfare that was published in 2011 – which underlines the fact that the debate about the legal significance of cyber attacks was successfully initiated by the Netherlands (AIV/CAVV 2011).

4.3.2 Cyber attacks as violations of state sovereignty

The discussion centres mainly on one of the core principles of international law: respect for the national sovereignty of other states (Schmitt 2017a). This principle states that a country has the right to exercise 'the functions of a state' in a particular part of the world independently of other states. These functions would include levying taxes, promulgating laws and forming an army. Sovereignty is also connected with territoriality – states are sovereign in their own territory – but the concept can extend further. For example, every state has the right to pursue a foreign policy and to enter into trade relations with other states.

The international group of experts agrees that the principle of sovereignty applies to cyberspace (Schmitt 2017a). The sovereignty of states extends, in any case, to the physical infrastructure in a country's territory, the data, applications and protocols on the physical hardware and the persons in that territory who perform acts in cyberspace. Furthermore, cyber attacks impair the sovereignty of a state if they have a kinetic effect on the territory of the state – if they set something in motion.

Accordingly, cyber attacks can in theory violate a state's sovereignty in various ways. The following three ways are the most important:

9 The Advisory Council on International Affairs (AIV) is an independent body that advises both houses of the Dutch parliament on foreign policy. The Advisory Committee on Issues of Public International Law (CAVV) is an independent body that advises the government and both houses of the Dutch parliament on issues of international law.

1. A state may not use force or threaten to use force against persons or physical objects belonging to another state. This prohibition is partially fleshed out in the body of public international law known as *ius ad bellum*.
2. A state may not intervene with force in the affairs of another state.
3. A state may not limit the sovereignty of another state in a general sense; we can regard this principle as a residual category.

The question is whether cyber attacks can violate these three principles. The vast majority of cyber attacks are not regarded by experts as a violent or forceful interventions (Schmitt & Vihul 2017b). We will explain this point in more detail, starting with the prohibition of the use of force.

Re 1. Cyber attacks as forms of the use of force?
The prohibition of the use of force refers to force that has certain 'physical effects' (Schmitt 2013). Consequently, under international law one can only speak of force if the action leads to an actual or potential harmful physical effect on the state that is the target. The law defines these physical effects as death, physical injury or significant destruction of or damage to vital infrastructures, military installations or civil goods (Schmitt 2017a). The state that employs such force can therefore be in breach of both the general prohibition of the use of force in article 2(4) of the UN Charter and the prohibition of 'armed attacks' in article 51 of the UN Charter.

This distinction is very important because carrying out an armed attack triggers the right to interstate self-defence (*ius ad bellum*) and the law regulating behaviour in war (*ius in bello*). In other words, if a state chooses to carry out an armed attack, there are various rules that the state has to observe, such as being able to put forward a valid reason for carrying out the attack.

The problem is that the distinction between an armed attack and other examples of the use of force is sometimes difficult to make. Armed attacks are serious and disruptive uses of force, such as carrying out a missile attack, dropping a nuclear bomb or an attack that causes the entire financial system to crash (AIV/CAVV 2011). But it is difficult to say when an attack with force is so much less serious that it 'only' constitutes the use of force. What if you cause the financial system to crash, but it is up and running again the next day? International law is ultimately a collection of mainly general rules and principles; it is up to states themselves to propose how they should be interpreted.

What does this imply for cyber attacks? Firstly, it is clear that what counts is the consequences of cyber attacks, not their digital nature – according to the Tallinn Manual, international law does not preclude the use of any weapon (AIV/CAVV

2011, Schmitt 2013, 2017a). Secondly, it is conceivable that cyber attacks could cause civilian victims or significant damage to infrastructure, for example as a result of a lengthy shut-down of power stations. In other words, such an attack could in theory be regarded as the use of force, or even as an armed attack (Condron 2007, Jensen 2002, Benatar 2009, Schmitt 2013).

However, it is difficult to find examples of cyber attacks that meet the criteria of an armed attack (Rid 2012, Schmitt 2013). Cyber attacks for the purposes of sabotage do not usually cause civilian victims – at least not directly. And the vast majority of cyber attacks aimed at sabotage cause social disruption, but do not destroy vital infrastructure. For example, cyber sabotage attacks regularly disrupt the service provided by banks, but none has ever shut down an entire financial system. Equally, in Ukraine the energy supply has occasionally been shut off, but the lights were back on again a few hours later. Even the attack on the centrifuges in Natanz prompted a discussion, although the majority of experts ultimately concluded that it was an armed attack (Schmitt 2017a). The AIV/CAVV therefore concluded that a ‘cyber war’, consisting of separate digital armed attacks, is barely conceivable (AIV/CAVV 2011).

That conclusion puts certain assertions made about cyber conflicts into perspective. For example, we have seen that some countries regularly use bellicose language in the context of cyber attacks – American generals have warned of a ‘cyber Pearl Harbour’ and have literally declared the US to be in a state of war (see, *inter alia*, Stavridis 2017) – but there is almost never a war within the meaning of international law in relation to cyber attacks.

However, this does not mean that international humanitarian law is never applicable to cyber attacks: once countries are in a state of war, cyber attacks that form part of the military campaign must comply with the *ius in bello*. This explains why, according to the Tallinn Manual 2.0, the cyber attacks on Estonia did not fall under international humanitarian law, but the cyber attacks on Ukraine did. The cyber attacks on Ukraine took place in the context of the military occupation of parts of East Ukraine and the Crimea.

Is it easier to define cyber attacks as a ‘normal’ use of force? This concept is sometimes clear, especially if experts start to wonder whether the attack itself could perhaps be regarded as an armed attack. The Stuxnet attack, for example, was clearly a use of force because the turbines in Natanz sustained physical damage. Equally, a cyber attack on a power station would be a use of force if important installations are destroyed. But cyber attacks are more difficult to define as a use of force because they do not directly cause physical damage, but only disrupt a digital system. The Tallinn experts therefore present a number of criteria that must be

taken into account, such as the seriousness, immediacy and intrusiveness of the cyber attack (Schmitt 2017a). Once again, the states will have to provide the interpretation of these terms.

Re 2: Cyber attacks as forms of forceful intervention?
Given the limited physical damage that cyber attacks cause, one has to look at the prohibition of forceful intervention and of the limitation of sovereignty for the regulation of the information conflict. These categories are defined in even more general terms than the prohibition of the use of force. The prohibition of forceful intervention will seldom be violated by cyber attacks, because cyber attacks are usually not so powerful or so intrusive as to effectively compel a state to pursue a particular policy (Schmitt & Vihul 2017). That could change: cyber attacks could in future become more serious and more effective in exerting pressure on governments. But that is not the case at present. What remains therefore is the general prohibition on limiting another state's sovereignty.

Re 3: Cyber attacks as forms of limitation of sovereignty?
The experts explain that a finding of a violation of sovereignty depends on (1) the degree to which the state's territorial integrity has been violated and (2) the degree to which the principal functions of one state have been impaired or assumed by another state (Schmitt 2017a). With respect to the first point, one could think of an act of violence or causing damage to infrastructural systems. On the second point, one might think of the organisation of elections, the levying of taxes or the pursuit of a particular economic policy. It will not come as a surprise to learn that many cyber sabotage attacks appear to violate this principle, such as DDoS attacks on the websites of banks or the crippling of a power station.

Cyber espionage would also appear to limit the sovereignty of states, but the experts do not share that view: there is too little support for this principle in international practice, where countries are permanently spying on one another (Schmitt 2017a). Cyber espionage only constitutes a violation of a state's sovereignty if the spying is accompanied by a form of damage: the corruption of data, the loss of a system's functionality or the installation of backdoors. Therefore, since a lot of cyber espionage leaves harmful traces, such as opened digital backdoors, the principle of violation of sovereignty does still apply to a lot of cyber espionage.

It is not clear whether spreading disinformation can be regarded as a violation of state sovereignty; the experts do not express an opinion on this point. But we could imagine that the debate would be similar. One could assert that such campaigns impair sovereignty because the organisation of a constructive public debate and the holding of fair elections are among the core functions of a state governed by the

rule of law, and those activities are impaired by chaos in the flow of information. But one could also assert that states have always spread propaganda to some extent and that lies alone are not enough to impair the effective functioning of a state. This is a debate that will continue.

All in all, the principle of violation of sovereignty could provide a framework for a critical analysis of many cyber attacks and even for declaring them to be in breach of international law. However, the principle is formulated in very general terms and a violation of sovereignty in itself forms a less serious transgression than the use of force or an armed attack. A breach of the prohibition of the use of force justifies a stronger reaction than a general violation of sovereignty – and it is entirely possible that in some situations states will actually want to employ a strong counter-measure.

4.3.3 International law that requires considerable interpretation

Our conclusion is that the international law that applies to cyber attacks is often general in nature and still requires considerable interpretation. This is not surprising given the recent origin of cyber attacks. It takes time to translate abstract principles into new practice. States are already taking steps in this direction in various forums.

Meanwhile, there is still a lot of uncertainty about the characterisation of cyber attacks and the formulation of a legally valid reaction. In many respects, states still have to determine their position and have not yet succeeded in reaching comprehensive and specific global agreements.

There is therefore cause for optimism and for pessimism. The next step is to draw up a regulatory framework that reflects the specific characteristics of the information conflict.

4.4 Conclusion

The preceding sections covered the international alliances in the area of offensive cyber capabilities, with special attention to the international regulation of offensive cyber capabilities. We reached the following conclusions.

- **At both global and regional level countries are working ever more closely with each other and with businesses and civil-society organisations to improve the cyber security of their systems**. See the IMPACT and FIRST alliances, but also the initiatives that have been taken at EU and NATO level,

such as the creation of the network of CERTs, the certification of IoT products and defence software, and the various military and civil exercises. The need to constantly enhance cyber security is clearly recognised and discussed at international level and is increasingly being reflected in political decisions and specific policy.

- **These regional alliances display far less coordination of the build-up of offensive cyber capabilities by states**. Countries, including EU member states, are expanding their offensive cyber capabilities and buying their own cyber weapons as they see fit. Despite the louder calls for closer cooperation, and even for a European army, offensive capabilities are still being built up according to the traditional idea of individual state sovereignty. In preparing for both the information conflict and a cyber-physical war, what we see in the cyber domain is a mix of cooperation and individual management of capabilities. For example, the EU member states have developed a common diplomatic response to cyber attacks, including the adoption of the sanctions that the EU can impose, with the cyber diplomacy toolbox (see 4.2.1). But at present those sanctions do not include the EU's own use of offensive cyber weapons.

- Although the sources here are limited, the same tension is apparent in cooperation in the area of intelligence gathering. **Western intelligence services do work together, also in an offensive context, but at the same time regularly keep their cards close to their chest**. There are various known alliances and states acknowledge that it is essential to share information with allies. We also know of some joint espionage and sabotage operations, such as Operation Olympic Games and the leaked collaboration between the American NSA and the British GCHQ (Sanger 2018). But intelligence services rarely tell each other everything they know.

- The situation is different with respect to disinformation. **International alliances in the West place the emphasis on combating the spread of disinformation – particularly at EU level**. There is no discussion of a coordinated build-up of capabilities for disseminating disinformation – which does not mean that EU or NATO member states do not spread disinformation (see the discussion in 3.6). There is some opposition to certain preventive measures; in particular the anti-disinformation task force has been accused of state censorship.

- The tension between international cooperation and individual use of offensive capabilities is also apparent in the worldwide development of standards governing cyber attacks. On the one hand, standards are being discussed in many forums, including the UN GGE, the Paris Call, the Global Tech Accord

and the OSCE. These deliberations have not been fruitless: the various UN GGE conferences have produced a series of measures designed to increase trust and have issued declarations on the relevant international law – and publications by the G7, the Paris Call and the Tech Accord have also proposed standards and shown that international law also applies to cyber attacks in various ways. But the discussions in these bodies have not led to worldwide agreements. The diplomatic talks in the UN have led to two parallel discussion groups: the new GGE and the OEWG. The most ambitious alternative to those talks seems to be the Paris Call, given the very diverse and worldwide group of social actors that have signed this document. However, some cyber superpowers, including the United States and China, have not signed up to this initiative. **The development of standards has therefore been initiated, but there is no worldwide cooperation.** Furthermore, the discussion in the Tallinn Manual shows that the existing international law standards require further interpretation.

5 Conclusion

A growing number of countries can carry out cyber attacks that cause enormous damage to businesses, humans and government institutions. Almost every country uses cyber weapons. They spy on one another and try to infiltrate each other's digital systems; some states even engage in cyber sabotage or spread disinformation. The use of information technology is creating a new conflict. In this report, we refer to this as an information conflict.

The question asked in this study is how the Netherlands can contribute to the de-escalation of this information conflict. In this final chapter, we suggest five possible solutions and refer to Dutch initiatives that correspond with these prospective solutions. But first we summarise, on the basis of the preceding chapters, the current international situation.

5.1 The international situation

The preceding chapters provide an overview of recent developments in the area of offensive cyber capabilities. Chapter 2 showed that the digitisation of society is accompanied by various security risks. For example, malicious persons can hack mobile telephones and gain access to private photos or camera images, and they can use the computers of smart devices to carry out a DDoS-attack.

Because of the scale and continuing growth of the potential damage, one increasingly refers to 'cyber weapons', 'cyber attacks' and 'cyber operations'. These new concepts are described in this report. We have made a distinction between three forms of cyber attacks: **cyber espionage**, **cyber sabotage** and the **spread of disinformation**. A number of things stand out:

- Cyber attacks can usually be carried out from a great distance and from the shadows, without the perpetrator having to fear any repercussions.
- Cyber weapons can spread very quickly and when they are used can cause damage in unexpected places.
- Cyber attacks can be both technologically advanced and relatively simple. Advanced attacks are reserved for powerful cyber actors such as intelligence services and well-organised criminals. Simpler attacks can be carried out or even bought to order by practically anyone.

- Cyber weapons can be disarmed by updating systems. This is only possible if the digital vulnerability is known.
- The spread of disinformation is increasingly difficult to identify, for example because of the high quality of falsifications of images and sound.

Three rungs on an escalation ladder

Cyber attacks occur on a daily basis. In chapter 3 we described who carries them out; in the process we stressed the role of the major cyber powers – the United States, Russia and China – and also discussed the Netherlands and a number of other European countries. We did this by plotting the activities on a so-called cyber escalation ladder which has three rungs:

1. A rung that represents **cyber peace**, a situation in which countries do use digital resources to spy or to conduct sabotage or to spread disinformation.
2. A rung that represents **information conflict**, a situation in which states resort to cyber espionage and, in some cases, to spreading disinformation and to sabotaging digital systems.
3. A third rung that represents **cyber-physical war**, where the damage that states cause is so severe that one could speak of armed attacks. During a cyber-physical war, every type of cyber attack are in fact covered by international law, not just the few cyber attacks that in themselves constitute an armed attack.

Most current actions by influential states fall into the situation that we described above as the information conflict. Countries build up their cyber security during peacetime and try to infiltrate the digital systems of other countries as clandestinely as possible. A characteristic of Russia's activities is that it also actively tries to spread disinformation. This is a strategy that other autocratic countries do not seem to apply widely, at least with respect to other countries, but that does fit in seamlessly with their desire to manage, censor and manipulate the information that reaches citizens. There are also some examples of serious cyber sabotage, such as Operation Olympic Games, which is attributed to Israel and the United States, and the WannaCry attack, which is attributed to North Korea. Up to now, cyber attacks have never caused a cyber-physical war; in that regard, there is no question of a 'cyber war'. However, cyber is increasingly an element of warfare, as can be clearly seen in the conflict in Ukraine.

International cooperation

Chapter 4 added the perspective of international cooperation to the analysis. In international and regional forums, states are endeavouring to create a safe and free digital world. States have not yet succeeded in making clear agreements on cyber attacks. There is a striking difference between the cooperation in the field of cyber security and the cooperation in the field of offensive cyber capabilities. The cyber

security initiatives, within the EU and within international organisations such as IMPACT and FIRST, go beyond discussion of issues and yield policies that are implemented in practice and are widely supported. The same cannot be said for the initiatives in relation to offensive cyber capabilities. Although intelligence services share information and take joint action, particularly in bilateral relations, states have not been able to agree on binding rules specifically tailored to the information conflict. The only exception here seems to be the EU Council's decision on restrictive measures against cyber attacks – but that decision does not authorize using offensive cyber capacities, does not have global authority and is limited to imposing a travel ban and an asset freeze.

This does not mean that there are no rules governing cyber attacks. However, because these attacks seldom exceed the threshold of an 'armed attack', and hence activate international humanitarian law, only general standards apply, such as the prohibition of the use of force. And at the moment those standards can be interpreted in different ways. Efforts are being made to reach new agreements, but so far without success.

The information conflict could escalate. As our report shows, the current international situation is risky and worrying. States are continually carrying out cyber attacks, and there is a significant chance that they do so with the intention of causing damage to citizens and that this activity will escalate. This is connected with four factors that we discuss below.

1. **The vulnerability of digital systems**
   In chapters 2 and 3 we provided examples of effective cyber attacks. Practically no defence is totally effective against advanced cyber attacks and many targets are relatively easy to infiltrate. Improving cyber defence is worthwhile: a lot of suffering can be avoided with relatively simple measures. But for the time being there are no impregnable fortresses that can effectively discourage these attackers.

2. **The proliferation of cyber weapons**
   In addition to the possibility of carrying out cyber attacks, cyber weapons are also widely available. Our survey shows that large and small states have built up offensive cyber capabilities. They wish to possess a high-class arsenal with which to carry out complex espionage and sabotage operations and to spread disinformation, and master simpler methods of carrying out cyber attacks. This trend has led to the emergence of a private industry that supplies these weapons. Criminals also develop cyber weapons and some collaborate with particular governments.

This means that an enormous number of cyber weapons are being developed and distributed. An additional point is that cyber weapons can be stolen even from powerful cyber actors, that adversaries can analyse and reuse cyber weapons that have been used and that, once fired, cyber weapons can appear in every corner of the world. It goes without saying that with the number of cyber weapons growing, the chance of cyber attacks is also increasing.

3. **Uncertainty about the origin and nature of cyber attacks**
It is also difficult to discover the origin of cyber attacks and to define their precise nature. It is still often difficult to quickly and convincingly identify the perpetrators of cyber attacks: for example, an attacker can mask the operation by transmitting malware via hacked computers. Intelligence services regularly name specific perpetrators, but that can require a lengthy investigation. The accused state needs few arguments to deny any involvement (plausible deniability). Furthermore, it is difficult to determine the precise design of the cyber attack.

We have seen that cyber operations have multiple layers: sabotaging something often first requires intelligence gathering and infiltration. But intelligence gathering and infiltration can also occur independently rather than as part of a serious cyber attack. This can create misunderstandings, because countries that observe that a system is being infiltrated are often unable to determine the purpose of the infiltration, never mind being able to immediately determine what effects particular malware will have on a digital system.

This all creates uncertainty and could prompt states to defer a response or perhaps underestimate or overestimate the threat and react too strongly or too weakly.

4. **The lack of detailed rules**
The current international situation in relation to cyber attacks is characterised by a lack of detailed rules: states have negotiated almost no binding international rules in relation to offensive cyber capabilities in situations of information conflict that are specifically tailored to the cyber domain. They can therefore only use abstract principles of international law, which still require a great deal of interpretation, especially in the context of cyber attacks. This means that it is not clear to a state that is attacked what response is warranted under international law. Once again, the only exception here is the EU Council’s decision on restrictive measures against cyber attacks – but that

decision of course has no global authority, and is limited to the use of travel bans and asset freezes.

These four factors have led to a risky information conflict, in which attackers have the resources and the opportunity to attack vulnerable systems and seldom face the risk of retaliation. In this international situation, countries are likely to continue suffering from cyber attacks by other states. In light of the four factors mentioned above, there is a risk that the cyber attacks will escalate, both in the sense of the harm they cause and the frequency with which they occur.

5.2 Five possible solutions for de-escalation

Because of the threat to the security of the digital environment in the Netherlands and elsewhere, it is important for the international community to work towards effective de-escalation of cyber attacks. Steps should be taken to reduce the frequency of cyber attacks and the seriousness of the impact of cyber attacks on society. The question is how the current trend can be reversed and how responsibility for bringing about that reversal should be assigned. We formulate five possible solutions that could help to achieve this de-escalation below.

We also discuss and comment on a number of policy options. Although the Netherlands has taken useful steps in various respects, there is still a lot of work to be done at international level.

5.2.1 Continue the cooperation to enhance international cyber security

In addition to the national steps that have been taken to increase resilience and cyber security, which the Rathenau Institute explored in *A never-ending race* (Munnichs et al. 2017), it is important for the Netherlands to continue investing in international cooperation in the field of cyber security.

This new study shows that there is intensive cooperation to further improve digital security at EU and NATO level. For example, a broad network of Cyber Emergency Incident Response Teams (the CERT network) is being rolled out and legislation is being prepared governing security for devices connected to the internet (the Internet of Things). The organisations are also investing in research, public information and training. The EU and NATO also consult to learn from one another and to develop a joint strategy.

But these international developments do not mean that the defenders are winning the race with the attackers. The attackers still have regular successes. International cooperation therefore remains essential. That has also been the basic principle up to now: the Netherlands has always joined and often started international cyber security initiatives and adopts a constructive and critical attitude towards those initiatives, for example by warning against duplication in the initiatives taken by the EU (Minister of Foreign Affairs 2018).

Of all the measures that can be taken to avert the threat of cyber attacks, increasing the country's own cyber security remains the most effective: discouraging an adversary and preventing information conflict is less risky than using threats as a deterrent.

5.2.2 Make clear international agreements for de-escalation in the areas of cyber sabotage, disinformation and cyber espionage

The vast majority of cyber attacks take place in the phase that we refer to as the information conflict. As we have described, only general international rules and standards are applicable during this phase and countries can interpret them differently. This benefits cyber attackers, who flourish in the uncertainty created by the absence of specific rules and principles.

If these rules and principles were spelled out, the international community could give a quicker and clearer response to a cyber attack. Knowing that, a country would weigh the benefits of the attack against the costs before deciding to attack.

The question is: precisely what rules and principles are needed? There are important choices to be made in that regard. We will discuss the options open to politicians. It is in any case important that the rules are specific and are supported in practice and that states comply with and flesh out the agreements. We will first discuss three ideas about the **form** these agreements could take.

- A frequently mentioned idea is a 'Geneva convention for cyber conflict' (see, *inter alia*, Smith 2017). Just as the Geneva Conventions lay down rules for conventional warfare, a cyber convention could formulate principles for cyber conflicts. The question is to what extent such a treaty is internationally feasible: most of the Geneva Conventions were signed by China and Russia, but it is unlikely that these states would support a cyber convention at this time. Nevertheless, a treaty could also be concluded by a smaller group of states. Given the general and sometimes unwritten nature of the relevant international

law, laying down more specific principles in writing would establish stronger grounds for condemning a state's conduct and taking measures against it.

- In addition to such a legal instrument, more voluntary agreements could also be concluded in the context of confidence-building measures. These measures could enhance the cooperation and transparency between states and so limit the risk of misunderstandings, escalation and conflicts arising from cyber threats (Van der Meer 2015). Both bilateral and multilateral measures could be adopted. One example might be intensifying the sharing of intelligence about attacks on vital infrastructure.

- Another possibility is for states to declare independently how they will react to violations of their sovereignty. This could stabilise mutual expectations, particularly when states adopt the same position. One aspect of that independent position could be a classification of cyber attacks showing which are felt to be more serious than others and what response attackers can expect to each type of attack. Such classifications have already been developed by the American government and were recently also drawn up by a French think tank (US-CERT 2018, Grisby 2018a). Western countries could in this way establish common boundaries, for example.

Important choices also have to be made in terms of the **content** of international agreements. Prominent issues include how to deal with espionage, the appraisal of the dissemination of disinformation and the various possible countermeasures.

- Espionage has traditionally between accepted by governments as part of the deal, provided the espionage does not extend to stealing from private organisations. However, given the nature of cyber attacks it is questionable whether this traditional agreement is tenable in the current information age – once inside a system, a hacker can sabotage it. It would instil confidence, for example, if countries were to agree with each other that vital systems will not be infiltrated during peacetime. This would naturally represent a diminution of the strength of cyber powers like the United States and the United Kingdom. Our research has shown that a situation in which countries are allowed to destroy each other's cyber defences but are then expected not to abuse the access they have gained in the process is unsustainable.

- The spread of disinformation can often undermine the functioning of the democratic rule of law, both at particular critical moments and more stealthily in the longer term. Destabilisation is generally also the intended purpose of the disinformation campaign. Our research has shown that this type of cyber attack can be compared with the use of chemical weapons: an impermissible weapon

for a civilised democratic state to use. In states like Russia, Iran and China there is scarcely any open and critical information available and it is inappropriate for a state governed by the rule of law to further disrupt the supply of information in another country. It might at best be legitimate to provide support for independent journalism in a country like Russia. But spreading disinformation that weakens the legal order is not a tool that a civilised state can use.

- Finally, there is a fundamental choice to be made in the type of counter-measures that can be taken in response to a cyber attack. One could fight fire with fire and retaliate with a similar attack. As we have said earlier, this is irresponsible if it undermines a democratic legal order. Many other cyber attacks also directly affect civil institutions and services – targets that, under the rules of international humanitarian law, should be spared as far as possible even in wartime. It is therefore questionable whether democratic countries like the Netherlands can respond with similar weapons; they could also respond with other instruments, such as the asset freeze and travel ban instruments put forward by the EU Council's decision on restrictive measures against cyber attacks. Unmasking a cyber operation and expelling spies, as occurred in the Netherlands in April 2018, is another example of an alternative type of sanction (Boere 2018).

  Consideration of these alternative measures raises the question of whether cyber counter-attacks would structurally improve cyber security. Every attack contributes to the proliferation of weapons and no cyber conflicts have ever been ended by a decisive counter-attack. Furthermore, serious reservations are expressed in the literature about the effectiveness of such a strategy of deterrence (Goodman 2010, Iasiello 2013, Clarke & Knake 2010). If it is decided to carry out a cyber counter-attack, it is essential that it is conducted immediately and in association with allies. If a threat is not followed up, the deterrent effect will disappear.

The Netherlands, which is traditionally in the vanguard of international cooperation, has already taken many steps with respect to international agreements. For example, the Netherlands helped to draft the Tallinn Manual, it is a member of the latest UN GGE and the Dutch government has announced that it will invest in the development of cyber diplomacy (Ministry of Foreign Affairs 2017, 2018). But it is precisely in the domain of international laws and principles that many questions remain; it is important for the Netherlands to intensify its efforts.

5.2.3 Ensure that the cyber arsenal is managed responsibly

As already mentioned, malware can spread throughout the world in seconds: it is the price we pay for a global internet. Anyone who uses a cyber weapon can expect the code that is used to fall into unexpected hands, and perhaps also return as a boomerang. This is why it is important to use cyber weapons carefully and to report vulnerabilities as soon as they are discovered. There is a major role for programmers in the de-escalation of cyber conflicts; they can disarm a lot of malware.

It is important for international intelligence services and defence units to cooperate with software producers and computer chip manufacturers in implementing security updates and distributing them among users. In that context, it would be useful for intelligence services and defence units to constantly ask themselves what does more to enhance cyber security: owning a certain type of weapon or releasing it. If international allies are more open towards each other, they can jointly monitor the management of vulnerabilities.

The long-term interest in having safe and reliable digital applications ultimately weighs more heavily than the short-term interest of permitting the use of unsafe software to facilitate specific operations.

Responsible management of the cyber arsenal also has implications for the cooperation with private parties. There is a risk that a strong private or rogue weapons industry will ultimately contribute to arms proliferation and provide adversaries with access to offensive cyber capabilities. Moreover, there is always the risk that cyber weapons will be stolen from private parties. It is not without reason that the German government recently decided to establish its own state agency to develop cyber weapons (Delcker 2018).

A clear framework for considering these factors could help the Dutch government to determine which private partners should be involved in developing offensive cyber capabilities or to take greater control of developments. If the government collaborates with private partners, it is important to set conditions that ensure that dangerous technology does not fall into the hands of dangerous regimes. An international lobby for an updated system of export licences could help in that regard (Ministry of Foreign Affairs 2018).

5.2.4 Protect the independence of technology companies

Technology companies like Microsoft, Google and IBM perform a crucial role in the security of the digital environment. They seal the holes in their software and can bring more robust digital applications onto the market. These companies must therefore be able to retain their independence and must not be extensions of national governments.

It is important to assist companies in making their operations as safe as possible. Governments are taking a risk if they insist that companies secretly weaken the security of their products. Governments must therefore regulate both the technology and the technology companies in a sensible manner.

Kaspersky Labs and Huawei Technologies are under enormous pressure because of their close relationship with the Russian and Chinese governments, respectively. The governments of Russia and China regularly use their power to intervene in companies openly and behind the scenes (Klimburg 2017, Kharpal 2019). And American companies sometimes also work intensively with intelligence services, under compulsion or otherwise, as in the NSA's recently renewed PRISM programme (Volz 2018, Zetter 2013).

Precisely how the Dutch government will deal with companies like Huawei and Kaspersky in the future depends on the extent to which the Chinese and Russian governments influence these companies. It is important that technology companies can operate reliably and independently and that they accept their responsibility for security – both within prescribed frameworks and proactively. Via the Global Tech Accord, companies have signed up to the Paris Call for Trust and Security in Cyberspace, together with countries like the Netherlands. The relationship between governments and companies is naturally different when it comes to manufacturers of cyber weapons – the production of cyber weapons falls under a unique norm regime.

5.2.5 Engage in a public debate on international cyber security

The information conflict should be subjected to democratic debate: it is citizens who are affected by cyber attacks. Even more than in other conflicts, they are the target; they are misled by disinformation, vital facilities are hacked and companies like banks are spied upon. Consequently, fundamental rights, such as the right to privacy, the right to security and our democratic rights, are at stake. We must be resilient. It is also up to citizens to provide direction for the digital future. The

decision on whether to buy particular weapons and to authorise particular operations is not just a matter for experts and civil servants with special powers.

De-escalation of the information conflict therefore calls for a public and political debate about this enduring conflict and the Netherlands' position in it. Each of the four possible solutions mentioned above is an important topic to be discussed in that debate.

The importance of confidentiality for the intelligence services and defence must therefore be weighed in every case against the interests of Dutch citizens in receiving information about the government's cyber operations. The greater the impact of the international cyber conflict on society, the greater the importance of facilitating a relevant public debate on the subject.

To be resilient, citizens badly need information: informed citizens can recognise and reveal disinformation and take the necessary security measures. The Rathenau Institute has previously called for the promotion of technological citizenship (Van Est 2017, Van Keulen et al. 2018), and all of the elements discussed there return in the discussion about offensive cyber capabilities. Citizens who can understand how technology influences their lives and can provide input for the political choices that need to be made in the area of new technologies are more resilient against subversive cyber attacks than citizens who cannot.

The government therefore has a special responsibility to facilitate this technological citizenship. The government is already taking effective steps, especially in terms of providing information about and education in media wisdom (Rijksoverheid 2018) – but more is needed. It is important to conduct a public debate on the choices and dilemmas set out in this report. The Netherlands will then be able to deal in a democratic manner with international cyber threats and generate public support for its international efforts, both through diplomacy and through other agreements.

Bibliography

Adkins, G. (2013). Red Teaming the Red Team: Utilizing Cyber Espionage to Combat Terrorism. In: Journal of Strategic Security 6(3), 1-9.

Adviesraad Internationale Vraagstukken (AIV), Commissie van Advies inzake Volkenrechtelijke Vraagstukken (CAVV) (2011), Digitale Oorlogvoering. Available online at: https://aiv-advies.nl/download/9fc55422-c96d-4563-9279-f434803c0afd.pdf.

Agence France-Presse (2016). 'Germany to further curb activities of spy agency in wake of NSA scandal'. The Guardian 28 juni 2016. Available online at: https://www.theguardian.com/world/2016/jun/28/germany-curb-spy-agency-nsa-scandal-angela-merkel.

Algemene Inlichtingen- en Veiligheidsdienst, Militaire Inlichtingen- en Veiligheidsdienst (2017). Cyberespionage: Are you aware of the risks?.

Algemene Inlichtingen- en Veiligheidsdienst (2019). Cyberdreiging. Available online at: https://www.aivd.nl/onderwerpen/cyberdreiging.

Andress, J. & S. Winterfeld (2011), Cyber Warfare, Techniques, Tactics and Tools for Practitioners, Syngress.

Avaaz (2019). 'Social media reports fail to address scale of threat: Avaaz calls for emergency steps to issue corrections for disinformation'. Avaaz website. Available online at: https://secure.avaaz.org/act/media.php?press_id=930.

Ball, J., J. Borger & G. Greenwald (2013). 'Revealed: how US en UK spy agencies defeat internet privacy and security'. The Guardian 6 september 2013. Available online at: https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

Bartles, C.K. (2016). Getting Gerasimov Right. In: Military Review, januari-februari: 30-38.

Benatar, M. (2009) The use of cyber force: Need for legal justification? In: Goettingen Journal of International Law 1, 375-396.

Bilge, L. & T. Dumitras, (2012), Before we knew it, an empirical study of zero-day attacks in the real world, In: Proceedings of the 2012 ACM conference on Computer and communications security, 833-844.

Binding, L. (2018). ‘GCHQ intelligence chief threatens 'brazen' Russia with UK's 'tools'. Sky News 7 september 2018. Available online at: https://news.sky.com/story/gchq-intelligence-chief-threatens-brazen-russia-with-uks-tools-11492237.

Boere, R. (2018), ‘Ontluisterend inkijkje in het werk van vier Russische spionnen’. Algemeen Dagblad 4 oktober 2018. Available online at: https://www.ad.nl/binnenland/ontluisterend-inkijkje-in-het-werk-van-vier-russische-spionnen~a86c66f1/.

Boffey, D. (2018). ‘British spies 'hacked into Belgian telecoms firm on ministers' orders'. The Guardian 21 september 2018. Available online at: https://www.theguardian.com/uk-news/2018/sep/21/british-spies-hacked-into-belgacom-on-ministers-orders-claims-report.

Bowcott, O., ‘China's hackers stealing US defence secrets, says congressional panel’. The Guardian 20 november 2008. Available online at: https://www.theguardian.com/world/2008/nov/20/america-china-hacking-security-obama.

Branigan, T. (2010). ‘Google to end censorship in China over cyber attacks’. The Guardian 13 januari 2010. Available online at: https://www.theguardian.com/technology/2010/jan/12/google-china-ends-censorship.

Burton, J. (2015), NATO ’s cyber defence: strategic challenges and institutional adaptation. In: Defence Studies, november, 1-22.

Cebrowski, A.K. & J.H. Garstka (1998). Network-Centric Warfare: Its Origin and Future. In: US Naval Institute Proceedings, 124(1), 28-35.

Chan, E. & A. Nour (2018). ‘Microsoft Thwarts Russia Hackers Targeting GOP Critics of Trump’. Bloomberg 21 augustus 2018. Available online at: https://www.bloomberg.com/news/articles/2018-08-21/microsoft-finds-new-russian-effort-to-hack-u-s-political-groups.

Chase, M.S., J. Engstrom, T.M. Cheung, K.A. Gunnes, S.W. Harold, S. Puska & S.K. Berkowitz (2015). China's Incomplete military transformation. Rand corporation.

Choucri, N., S. Madnick, & J. Ferwerda (2013), Institutions for Cyber Security: International Responses and Global Imperatives. In: Information Technology for Development 20(2), 96-121.

Clapper, J.R. (2013). Statement by Director of National Intelligence James R. Clapper on Allegations of Economic Espionage, Office of the Director of National Intelligence.

Clarke, R.A. & R. Knake (2010). Cyber War. HarperCollins.

Codron, S.M. (2007). Getting it right: Protecting American critical infrastructure in cyberspace. In: Harvard Journal of Law & Technology 20(2), 404-422. Available online at: http://jolt.law.harvard.edu/articles/pdf/v20/20HarvJLTech403.pdf.
Colarik, A.M. & L.J. Janczewski (Eds.) (2007), Cyber Warfare and Cyber Terrorism, IGI Global

Coldwell, W. (2014). 'Airbnb's legal troubles: what are the issues?'. The Guardian 8 juli 2014. Available online at: https://www.theguardian.com/travel/2014/jul/08/airbnb-legal-troubles-what-are-the-issues.

Conley, H.A., J. Mina, R. Stefanov & M. Vladimirov (2016). The Kremlin Playbook. Center for Strategic & International Studies.

Crawford, J. (2016), 'Massive IRS data breach much bigger than first thought', CBS news 29 februari 2016. Available online at: https://www.cbsnews.com/news/irs-identity-theft-online-hackers-social-security-number-get-transcript/.

Crowell, C. (2017). 'Our approach to bots and misinformation'. Twitter 14 juni 2017. Available online at: https://blog.twitter.com/official/en_us/topics/company/2017/Our-Approach-Bots-Misinformation.html.

Curran, J., N. Fenton & D. Freedman (2012). Misunderstanding the Internet. Routledge.

Cybersecurity Tech Accord (2018). Available online at: https://cybertechaccord.org/.

Ducheine, P. & J. Van Haaster (2014). Fighting Power, Targeting and Cyber Operations. In: P. Brangetto, M. Maybaum & J. Stinissen (eds.), 6th international conference on cyber conflict, Tallinn: NATO Publications.

Ducheine, P. (2018). Veiligheid en Cyberspace. In: Blind 49.

Defense Intelligence Agency (2017). Russia Military Power. Available online at: http://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Russia%20Military%20Power%20Report%202017.pdf.

Deibert, R., R. McKinnon, X. Qiang & T. Lokman, 'Open letter to Google on reported plans to launch a censored search engine in China'. Available online at: https://www.documentcloud.org/documents/4792329-Google-Dragonfly-Open-Letter.html.

Delcker, J. (2018). 'Germany to launch US-style agency to develop cyberdefense'. Politico 29 augustus 2018. Available online at: https://www.politico.eu/article/germany-to-launch-darpa-style-agency-to-develop-cyber-defense/.

DHS, ODNI, FBI (2016), 'Joint DHS, ODNI, FBI Statement on Russian Malicious Cyber Activity'. Available online at: https://www.dhs.gov/news/2016/12/29/joint-dhs-odni-fbi-statement-russian-malicious-cyber-activity.

District Court of Columbia, Indictment 13 juli 2018. Available online at: https://d3i6fh83elv35t.cloudfront.net/static/2018/07/Muellerindictment.pdf.
The Economist (2010). Special report on cyberwar: War in the fifth domain. 1 juli 2010.

The Economist (2017). China's internet giants go global. 20 april 2017. Available online at: https://www.economist.com/business/2017/04/20/chinas-internet-giants-go-global.

The Economist (2018). Defence companies target the cyber-security market. 26 juli. Available online at: https://www.economist.com/business/2018/07/26/defence-companies-target-the-cyber-security-market.

Ehrenfeld, J.M. (2017). Wannacry, Cybersecurity and Health Information Technology: a Time to Act. In: Journal of Medical Systems 41, 104.

Electricity Information Sharing and Analysis Center (E-ISAC), SANS Industrial Control Systems (SANS ICS) (2016). Analysis of the Cyber Attack on the Ukrainian

Power Grid. Available online at: zie https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf).

Epstein, R. (2015). ‘How Google Could Rig the 2016 Election’. Politico 19 augustus 2015. Available online at: https://www.politico.com/magazine/story/2015/08/how-google-could-rig-the-2016-election-121548.

Est, van, R. (2017). Technologisch burgerschap, Den Haag: Rathenau Instituut. Available online at: https://www.rathenau.nl/nl/digitale-samenleving/technologisch-burgerschap-de-democratische-uitdaging-van-de-eenentwintigste.

Euractiv (2018). ‘EU code of practice on fake news: Tech giants sign the dotted line’. Available online at: https://www.euractiv.com/section/digital/news/eu-code-of-practice-on-fake-news-tech-giants-sign-the-dotted-line/.

Europese Commissie (2013). Strategie inzake cyberbeveiliging van de Europese Unie: Een open, veilige en beveiligde cyberspace. Available online at: https://www.eumonitor.nl/9353000/1/j9vvik7m1c3gyxp/vj6ytdiaomzb.

Europese Commissie (2016). Joint Framework on countering hybrid threats: a European Union response. Available online at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=SV.

Europese Commissie (2017a). Joint Communication to the European Parliament and the Council. Available online at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450.

Europese Commissie (2017b). Review of ENISA Regulation and laying down a EU ICT security certification and labelling. Available online at: https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3436811_en.

Europese Commissie (2018a). Digital Single Market. Available online at: https://ec.europa.eu/digital-single-market/.

Europese Commissie (2018b). Code of Practice on Disinformation. Available online at: https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.

Europese Commissie (2018c). Fake news and online disinformation. Available online at: https://ec.europa.eu/digital-single-market/en/fake-news-disinformation.

Europese Raad (2017). Cyber attacks: EU ready to respond with a range of measures, including sanctions. Available online at: http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf.

European Council (2019a). COUNCIL DECISION concerning restrictive measures against cyber-attacks threatening the Union or its Member States. Available online at: http://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/en/pdf.

European Council (2019b). COUNCIL REGULATION (EU) 2019/796. Available online at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0796&from=EN.

EU vs Disinfo (2018). website: https://euvsdisinfo.eu/about/.

Faris, R.M., H. Roberts, B. Etling, N. Bourassa, E. Zuckerman & Y. Benkler (2017), Partisanship, Propaganda,and Disinformation: Online Media and the 2016 U.S. Presidential Election. Berkman Klein Center for Internet & Society Research Paper.

Farrell, P. (2013), ‘History of 5-Eyes – explainer’. The Guardian 2 december 2013. Available online at: https://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer.

Farwell, J. & R. Rohozinski (2012). The new reality of cyber war. In: Survival: Global Politics and Strategy 54(4), 107-120.

Ferrara, E. (2017). Disinformation and Social Bot Operations in the Run Up to the 2017 French Presidential Election. Available online at: https://arxiv.org/abs/1707.00086.

FireEye (2014). The PLA and the 8:00am-5:00pm Work Day: FireEye Confirms DOJ's Findings on APT1 Intrusion Activity. Available online at: https://www.fireeye.com/blog/threat-research/2014/05/the-pla-and-the-800am-500pm-work-day-fireeye-confirms-dojs-findings-on-apt1-intrusion-activity.html.

FireEye (2018). Advanced Persistent Threat Groups. Available online at: https://www.fireeye.com/current-threats/apt-groups.html#apt29.

Fleck, D. (2013). Searching for International Rules Applicable to Cyber Warfare—A Critical First Assessment of the New Tallinn Manual. Journal of Conflict and Security Law 18(2), 331–351.

Forum of Incident Response and Security Teams (2018), website: https://www.first.org/.

France Diplomatie (2018). Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace. Available online at: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in.

Franke, U. (2015). War by non-military means. Swedish Defense Research Agency.

Freedom House (2018. Freedom in the World 2018: Democracy in crisis. Available online at: https://freedomhouse.org/report/freedom-world/freedom-world-2018.

Gallagher, R. (2017). 'NSA's Quiet Presence at a Base in England's Countryside Revealed in Snowden Documents'. The Intercept 13 september 2017. Available online at: https://theintercept.com/2017/09/13/digby-uk-nsa-gchq-surveillance/.

Gallagher, R. (2018). 'The Powerful Global Spy Alliance You Never Knew Existed'. The Intercept 1 maart 2018. Available online at: https://theintercept.com/2018/03/01/nsa-global-surveillance-sigint-seniors/.

Garamone, J. (2018) 'Cyber Tops List of Threats to U.S., Director of National Intelligence Says'. United States Department of Defense 13 februari 2018. Available online at: https://dod.defense.gov/News/Article/Article/1440838/cyber-tops-list-of-threats-to-us-director-of-national-intelligence-says/.

German Federal Ministry of the Interior (2011). Cyber Security Strategy for Germany. Available online at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/cyber-security-strategy-for-germany.

Giles, K. (2016). Russia's 'new' tools for confronting the west, Chatham House research paper. Available online at: https://www.chathamhouse.org/sites/default/files/publications/2016-03-russia-new-tools-giles.pdf.

The Global Commission on the Stability of Cyberspace (2019). Website: https://cyberstability.org/.

Global Forum on Cyber Expertise (2017), Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building. Available online at: https://www.thegfce.com/documents/publications/2017/11/24/delhi-communique.

Goodman, W. (2010). Cyber Deterrence. Tougher in Theory than in Practice? In: Strategic Studies Quarterly 2010 (3), 102-135.

Gorman, S. & J.E. Barnes (2012). ‘Iran Blamed for Cyberattacks’. The Wall Street Journal 12 oktober 2012. Available online at: https://www.wsj.com/articles/SB10000872396390444657804578052931555576700.

Government of Russia (2014), Military doctrine of the Russian Federation. Available online at: http://static.kremlin.ru/media/events/files/41d527556bec8deb3530.pdf.

Greenberg, A. (2018). ‘The White House Blames Russia for NotPetya, the 'Most Costly Cyberattack In History'. Wired 15 februari 2018,. Available online at: https://www.wired.com/story/white-house-russia-notpetya-attribution/.

Graham, M. (2016). U.S. Cyber Force: One War Away. In: Military Review 96(3), 111.

Grant, I. (2008). ‘Nato sets up Cyber Defence Management Authority in Brussels’. Computer Weekly 4 april 2008. Available online at: https://www.computerweekly.com/news/2240085580/Nato-sets-up-Cyber-Defence-Management-Authority-in-Brussels.

Grisby, A. (2018a). Three Takeaways from the French Cyber Defense Review. Council on Foreign Relations. Available online at: https://www.cfr.org/blog/three-takeaways-french-cyber-defense-review.

Grisby, A. (2018b). The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased. Available online at: https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased.

Group of Seven (2017). G7 Declaration on Responsible States Behavior in Cyberspace. Available online at: https://www.mofa.go.jp/files/000246367.pdf.

Group of Seven (2018). Charlevoix Commitment on Defending Democracy from Foreign Threats. Available online at: https://www.mofa.go.jp/files/000373846.pdf.

Group of Seven (2019a). Website: http://www.g7italy.it/en/history/.

Group of Seven (2019b). Dinard Declaration on the Cyber Norm Initiative. Foreign Ministers Meeting 6 april 2019. Available online at:

https://www.diplomatie.gouv.fr/IMG/pdf/g7_-_dinard_declaration_on_cyber_initiative_cle811175.pdf.

Group of Seven (2019c). Foreign Ministers Communiqué. Foreign Ministers Meeting 6 april 2019. Available online at: https://www.diplomatie.gouv.fr/IMG/pdf/g7_-_foreign_ministers_communique_cle8245be.pdf.

Gross, M. (2011a). ‘The fog of cyber-war’. Vanity Fair april 2011, 155–198.

Gruyter, de, C. (2018). ‘De koude oorlog was voorspelbaarder, dit kan escaleren’. NRC 17 maart 2018. Available online at: : https://www.nrc.nl/nieuws/2018/03/27/de-koude-oorlog-was-vo

Haberman, C. (2017). ‘Who’s Fueling Conspiracy Whisperers’ Falsehoods?’. The New York Times 20 april 2017. Available online at: www.nytimes.com/2017/04/30/us/retro-report-conspiracy-theories-kennedy-trump.html.

Harambam, J. (2017). De politisering van de waarheid. Sociologie 13(1), 73-92.

Harari, Y.(2018). ‘Why technology favors tyranny’, The Atlantic oktober 2018. Available online at: https://www.theatlantic.com/magazine/archive/2018/10/yuval-noah-harari-technology-tyranny/568330/.

Healey, J. & L. van Bochhoven (2011). NATO’s Cyber Capabilities: Yesterday, Today, and Tomorrow, Issue Brief Atlantic Council. Available online at: https://www.files.ethz.ch/isn/169072/022712_ACUS_NATOSmarter_IBM.pdf.

Hernandez, J.C. & Z. Mou (2018). ‘I Am Gay, Not a Pervert’ Furor in China as Sina Weibo Bans Gay Content’. The New York Times 15 april 2018. Available online at: https://www.nytimes.com/2018/04/15/world/asia/china-gay-ban-sina-weibo-.html

Herr, T. & P. Rozenzweig (2013). Cyber Weapons and Export Control: Incorporating Dual Use with the PrEp Model. In: Journal of National Security Law and Policy 8, 301.

Hopkins, N., J. Borger & L. Harding (2013). ‘GCHQ: inside the top secret world of Britain's biggest spy agency’. The Guardian 2 augustus 2013. Available online at: https://www.theguardian.com/world/2013/aug/02/gchq-spy-agency-nsa-snowden.

Iasiello, E. (2015). Are Cyber Weapons Effective Military Tools? In: Military and Strategic Affairs 7(1), 23-40.

Inkster, N. (2016). China's Cyber Power. Adelphi Series.

Insikt Group (2019). Beyond Hybrid War: How China Exploits Social Media to Sway American Opinion. Recorded Future. Available online at: https://www.recordedfuture.com/china-social-media-operations/.

International Journalism for EU (2018), IJ4EU: Funding cross-border investigative reporting in Europe. Available online at: https://www.investigativejournalismforeu.net/guidelines/.

International Multilateral Partnership Against Cyber Threats (2018). Website: http://www.impact-alliance.org/home/index.html.

International Telecommunications Union (2008). High-Level Experts Group Global Strategic Report. Available online at: https://ccdcoe.org/sites/default/files/documents/ITU-080801-HLEGreport.pdf.

International Telecommunications Union (2018), website: see ww.itu.int.

The Internet Corporation for Assigned Names and Numbers (2018a). Welcome to ICANN!, Available online at: https://www.icann.org/resources/pages/welcome-2012-02-25-en.

The Internet Corporation for Assigned Names and Numbers (2018b). Root DNSSEC. Available online at: http://www.root-dnssec.org.

Jaeger, P.T., J.C. Bertot & C.R. McClure (2003), The impact of the USA Patriot Act on collection and analysis of personal information under the Foreign Intelligence Surveillance Act. In: Government Information Quarterly 20, 295-314.

Jensen, E.T. (2002). Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right to Self-Defense. In: Stanford Journal of International Law 38, 207-240.

Kallberg, J., A Right to Cybercounter Strikes: The Risks of Legalizing Hack Backs. In: IT Professional 17(1), 30-35.

Kaplan, C. (2015). Air power's visual legacy: Operation Orchard and aerial reconnaissance imagery as ruses de guerre. In: Critical Military Studies 1(1), pp. 61-78.

Karatzogianni, A. (ed.) (2008). Cyber-conflict and global politics. London: Routledge.

Kaspersky Lab (2016). Measuring the Financial Impact of IT-security on Businesses. Available online at: https://media.kaspersky.com/en/business-security/kaspersky-it-security-risks-report-2016.pdf.

Keulen, van, I., I. Korthagen, P. Diederen & P. van Boheemen (2018). Digitalisering van het nieuws – Online nieuwsgedrag, desinformatie en personalisatie in Nederland. Den Haag: Rathenau Instituut.

Khalip, A. (2018). 'U.N. chief urges global rules for cyber warfare'. Reuters 19 februari 2018. Available online at: https://www.reuters.com/article/us-un-guterres-cyber/u-n-chief-urges-global-rules-for-cyber-warfare-idUSKCN1G31Q4.

Kharpal, A. (2019). 'Huawei says it would never hand data to China's government. Experts say it wouldn't have a choice'. CNBC 5 maart 2019. Available online at: https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html.

Klimburg, A. (2017). The Darkening Web. New York: Penguin Press.

Kobie, N. (2018). 'The odd reality of life under China's all-seeing credit score system'. Wired 5 juni 2018. Available online at: https://www.wired.co.uk/article/china-social-credit.

Kool, Daan (2019), 'Franse gelehesjesbeweging deelt veelvuldig nepnieuws'. De Volkskrant 13 maart 2019. Available online at: https://www.volkskrant.nl/nieuws-achtergrond/franse-gelehesjesbeweging-deelt-veelvuldig-nepnieuws~b6c0b4a4/.

Krepinevich, A.F. (2012). Strategy in a time of Austerity. In: Foreign Affairs november/december 2012. Available online at: https://www.foreignaffairs.com/articles/global-commons/2012-11-01/strategy-time-austerity.

Libicki, M.C. (2016). Cyberspace in War and Peace. Annapolis: Naval Institute Press.

Lucas, G.R. (2017). Ethics and cyber warfare: The quest for responsible security in the age of digital warfare. Oxford: Oxford University Press.

MacAskill, E. (2015). ‘Britain creates team of Facebook warriors’. The Guardian 31 januari 2015. Available online at: https://www.theguardian.com/uk-news/2015/jan/31/british-army-facebook-warriors-77th-brigade.

Mackenzie, C. (2019). ‘French defense chief touts offensive tack in new cyber strategy’. Fifth Domain 18 januari 2019. Available online at: https://www.fifthdomain.com/global/europe/2019/01/18/french-defense-chief-touts-offensive-tack-in-new-cyber-strategy/.

Markushin, D. (2017). ‘The cost of launching a ddos attack’. Securelist 23 maart 2017. Available online at: https://securelist.com/the-cost-of-launching-a-ddos-attack/77784/.

Matishak, M. (2018). ‘What we know about Russia’s election hacking’. Politico 19 juli 2018. Available online at: https://www.politico.eu/article/russia-hacking-us-election-what-we-know/.

Matsakis, L. (2018). ‘The US Sits out an International Cybersecurity Agreement’. Wired 11 november 2018. Available online at: https://www.wired.com/story/paris-call-cybersecurity-united-states-microsoft/.

McAfee (2011). Global Energy Cyberattacks: ‘Night Dragon’. Available online at: https://thanatosdotme.files.wordpress.com/2016/04/wp-global-energy-cyberattacks-night-dragon.pdf.

McDonald, M. (2012). ‘Adding more bricks to the great firewall of China’. The New York Times 23 december 2012. Available online at: https://rendezvous.blogs.nytimes.com/2012/12/23/adding-more-bricks-to-the-great-firewall-of-china/.

Meer, van der, S. (2015). Enhancing international cyber security. A key role for diplomacy. In: Security and Human Rights 26, 193-205.

Meer, van der, S. (2018a). ‘Nederland, gun de VS niet het recht van de sterkste in digitale oorlogvoering’. Trouw 12 april 2018.

Meer, van der, S. (2018b). State-level responses to massive cyber-attacks: a policy toolbox. Den Haag: Clingendael. Available online at: https://www.clingendael.org/sites/default/files/2018-12/PB_cyber_responses.pdf.

Mele, S. (2013). Cyber-weapons: Legal and Strategic Aspects, Version 2.0. Italian Institute of Strategic Studies.

Minister van Buitenlandse Zaken (2018). ‘Fiche: Mededeling weerbaarheid vergroten, versterken capaciteiten om hybride dreigingen aan te pakken’. Brief van de minister van buitenlandse zaken nr. 2693.

Ministerie van Buitenlandse Zaken (2017). Internationale Cyberstrategie Digitaal Bruggen Slaan. Available online at: https://www.rijksoverheid.nl/documenten/rapporten/2017/02/12/internationale-cyberstrategie-naar-een-geintegreerd-internationaal-cyberbeleid-getitield-digitaal-bruggen-slaan.

Ministerie van Buitenlandse Zaken (2018). Wereldwijd voor een veilig Nederland. Oline beschikbaar: https://www.rijksoverheid.nl/documenten/rapporten/2018/03/19/notitie-geintegreerde-buitenland--en-veiligheidsstrategie-gbvs.

Modderkolk, H. (2018). ‘Dutch agencies provide crucial intel about Russia's interference in US-elections’. De Volkskrant 25 januari 2018. Available online at: https://www.volkskrant.nl/wetenschap/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~b4f8111b/.

Modderkolk, H. (2018). ‘In gesprek met Jesse S. (18), die met ddos-aanvallen de Belastingdienst en banken zou hebben platgelegd’. De Volkskrant 6 februari 2018. Available online at: https://www.volkskrant.nl/tech/in-gesprek-met-jelle-s-18-die-met-ddos-aanvallen-de-belastingdienst-en-banken-zou-hebben-platgelegd~a4567183/.

Morello, C. (2018). ‘Mike Pompeo announces US government to increase broadcasting in Iran while likening country’s rulers to the mafia’. Independent 23 juli 2018. Available online at: https://www.independent.co.uk/news/world/americas/mike-pompeo-iran-mafia-sanctions-rouhani-trump-twitter-a8459561.html.

Mozur, P. (2017). ‘China spreads propaganda to U.S. on Facebook, a platform it bans at home’. The New York Times 8 november 2017. Available online at: https://www.nytimes.com/2017/11/08/technology/china-facebook.html.

Munnichs, G.M., M. Kouw & L. Kool (2017). Een nooit gelopen race: over cyberdreigingen en versterking van weerbaarheid. Den Haag: Rathenau Instituut.

Nationaal Coördinator Terrorismebestrijding en Veiligheid. Cybersecurity beeld Nederland 2018.

National Security Agency (2018), website: https://www.nsa.gov/.

NBC (2014). ‘Exclusive: Snowden Docs Show British Spies Used Sex and ‘Dirty Tricks’’. 7 februari 2014. Available online at: https://www.nbcnews.com/feature/edward-snowden-interview/exclusive-snowden-docs-show-british-spies-used-sex-dirty-tricks-n23091.

The New York Times Editorial Board (2016). ‘President Obama punishes Russia, at last’. New York Times 29 december 2016. Available online at: https://www.nytimes.com/2016/12/29/opinion/president-obama-punishes-russia-at-last.html.

Noord-Atlantische Verdragsorganisatie (NAVO) Communications and Information Agency (2018). website: https://www.ncia.nato.int/Pages/homepage.aspx.

NAVO (2002). Prague Summit Declaration. Available online at: http://www.ccdcoe.org/sites/default/files/documents/NATO-021121-PragueSummitDeclaration.pdf.

NAVO (2008). Bucharest Summit Declaration. Available online at: https://www.nato.int/cps/us/natohq/official_texts_8443.htm.

NAVO (2011). Defending the Networks, the NATO policy on cyber defence. Available online at: https://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf.

NAVO (2014). Wales Summit Declaration. Available online at: https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

NAVO (2016a). NATO cyber defence. Available online at: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf.

NAVO (2016b). Warsaw Summit Communiqué. Available online at: https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

NAVO Cooperative Cyber Defence Center of Excellence (NAVO CCDCOE) (2018). Organisations: NATO. Available online at: https://ccdcoe.org/nato.html.

NAVO CCDCOE (2018), Shanghai Cooperation Organisation. Available online at: https://ccdcoe.org/sco.html.

Nodurft, R. (2018). ‘Breaking down the numbers in Trump's proposed cyber budget’. The Hill 27 februari 2018. Available online at: https://thehill.com/opinion/cybersecurity/375812-breaking-down-the-numbers-in-trumps-proposed-cyber-budget.

NOS (2018), ‘Ook Ollongren wil nu af van Europese waakhond nepnieuws’. NOS 9 maart 2018. Available online at: https://nos.nl/artikel/2221353-ook-ollongren-wil-nu-af-van-europese-waakhond-nepnieuws.html.

O’Conner, T. (2017). ‘German military battles foreign hacking with new cyber soldiers’. Newsweek 4 mei 2017. Available online at: https://www.newsweek.com/german-military-launches-new-cyber-division-amid-russian-hacking-claims-579573.

Organisatie voor Vrede en Veiligheid in Europa (2018). Website: https://www.osce.org/.

Organisatie voor Vrede en Veiligheid in Europa (2016). OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies. Decision no. 1202.

Os, van, P. (2017). ‘Het Poolse journaal bedrijft ongekende propaganda’, De Groene Amsterdammer 51-52.

Pennetier, M. (2017). ‘Under threat, France grooms army hackers for cyber warfare’. Reuters 5 april 2017. Available online at: https://www.reuters.com/article/us-france-cyber/under-threat-france-grooms-army-hackers-for-cyber-warfare-idUSKBN1771B2.

Peterson, A. (2013). ‘The NSA has its own team of elite hackers’. The Washington Post 29 augustus 2013. Available online at: https://www.washingtonpost.com/gdpr-consent/?destination=%2fnews%2fthe-switch%2fwp%2f2013%2f08%2f29%2fthe-nsa-has-its-own-team-of-elite-hackers%2f%3f&utm_term=.db94d0e0dd26.

Poitras, L. & M. Rosenbach (2013). ‘NSA Spied on European Union Offices’. Spiegel 29 juni 2013. Available online at:

http://www.spiegel.de/international/europe/nsa-spied-on-european-union-offices-a-908590.html.

Politie (2018). Phishing. Website: https://www.politie.nl/themas/phishing.html.

Pollpeter, K., M. Chase & E. Heginbotham (2017). The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations. Rand Corporation.

Polyakova, A. & S. Boyer (2018). The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition. Brookings-Robert Bosch Foundation.

Qiao, L. & W. Xiangsui (2015). Unrestricted Warfare. Shadow Lawn Press.

Rathenau Instituut (2018). Zo werken de bots in Nederland. Available online at: https://www.rathenau.nl/nl/digitale-samenleving/digitalisering-van-het-nieuws/desinformatie-zo-werken-bots-nederland
.
Rathenau Instituut (2019). Desinformatie in Nederland. Bericht aan het parlement. Available online at: https://www.rathenau.nl/nl/digitale-samenleving/desinformatie-nederland.

Rauscher, K.F. & Korotkov, A. (2011). Towards rules for governing cyber conflict. Rendering the Geneva and Hague conventions in cyberspace. Brussel: EastWest Institute.

Reed, T. (2005). At the Abyss: an insider's history of the cold war. Presidio Press.
Rid, T. (2012). Cyberwar will not take place. In: Journal of Strategic Studies 35, 5-32.

Rid, T. (2013). Cyberwar and Peace: Hacking Can Reduce Real-World Violence. In: Foreign Affairs 92, 77-87.

Rigter, N. (2017). 'Cybercommando nu al overvraagd'. De Telegraaf 17 februari 2017. Available online at: https://www.telegraaf.nl/nieuws/1319419/cybercommando-nu-al-overvraagd.

Rijksbegroting 2018. Available online at: http://www.rijksbegroting.nl/2018/voorbereiding/begroting.

Rijksoverheid 2019. Campagne 'Desinformatie en nepnieuws'. Available online at: https://www.rijksoverheid.nl/onderwerpen/campagnes/lopende-campagnes/campagne-desinformatie-en-nepnieuws.

Ritchie. H. (2016), ‘Fake News stories of 2016’. CNBC 30 december 2016. Available online at: https://www.cnbc.com/2016/12/30/read-all-about-it-the-biggest-fake-news-stories-of-2016.html.

Roden, L. (2017). ‘Swedish kids to learn computer coding and how to spot fake news in primary school’. The Local 13 maart 2017. Available online at: https://www.thelocal.se/20170313/swedish-kids-to-learn-computer-coding-and-how-to-spot-fake-news-in-primary-school.

Royakkers, L. & R. van Est (2016). Just Ordinary Robots: Automation from Love to War. CRC Press.

Sanger, D. (2018). The Perfect Weapon. Crown Publishing.

Sanger, D.E. & S.L. Myers (2018). ‘After a Hiatus, China Accelerates Cyberspying Efforts to Obtain U.S. Technology’. The New York Times 29 november 2018. Available online at: https://www.nytimes.com/2018/11/29/us/politics/china-trump-cyberespionage.html.

Sargentini, J. (2018). Report on a proposal calling on the Council to determine, pursuant to Article 7(1) of the Treaty on European Union, the existence of a clear risk of a serious breach by Hungary of the values on which the Union is founded. A8-0250/2018.

Schell, O. (2016). ‘Crackdown in China: Worse and Worse’. The New York Review of Books 21 april 2016. Available online at: https://www.nybooks.com/articles/2016/04/21/crackdown-in-china-worse-and-worse/.

Schmitt, M. (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press.

Schmitt, M. & L. Vihul (eds.) (2017a). Tallinn Manual 2.0 on the international law applicable to cyber operations. Cambridge University Press.

Schmitt, M. & L. Vihul (2017b). Sovereignty in Cyberspace: Lex Lata Vel Non?. American Journal of International Law 111, 213-218.

Schneider, B. (2017), ‘Who are the Shadow Brokers?’. The Atlantic 23 mei 2017. Available online at: https://www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778/.

Sengupta, K. (2015). ‘New British Army unit 'Brigade 77' to use Facebook and Twitter in psychological warfare’. Independent 31 januari 2015. Available online at: https://www.independent.co.uk/news/uk/home-news/return-of-the-chindits-mod-reveals-cunning-defence-plan-10014608.html.

The Shanghai Cooperation Organisation (2006). Declaration on the Fifth Anniversary of SCO. Available online at: http://www.chinadaily.com.cn/china/2006-06/15/content_618177_3.htm.

The Shanghai Cooperation Organisation (2017), The Shanghai Cooperation Organisation. Available online at: http://eng.sectsco.org/about_sco/20170109/190857.html.

Smith, B. (2017). ‘The need for a Digital Geneva Convention’. Microsoft 14 februari 2017. Available online at: https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.0001hkfw5aob5evwum620jqwsabzv.

Soesanto, S. & F. D’Incau (2017). ‘The UN GGE is dead: Time to fall forward’, European Council on Foreign Relations 15 augustus 2017. Available online at: https://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance.

Solon, O. (2018). ‘A grand illusion’: seven days that shattered Facebook’s façade’. The Guardian 24 maart 2018. Available online at: https://www.theguardian.com/technology/2018/mar/24/cambridge-analytica-week-that-shattered-facebook-privacy.

Stavridis, J. (2017). ‘The United States Is Not Ready for a Cyber-Pearl Harbor’. Foreign Policy 15 mei 2017. Available online at: https://foreignpolicy.com/2017/05/15/the-united-states-is-not-ready-for-cyber-pearl-harbor-ransomware-hackers-wannacry/.
Stockholm International Peace Research Institute (2018). SIPRI Military Expenditure Database. Available online at: https://www.sipri.org/databases/milex.

Stockton, P. & M.Golabek-Goldman. Curbing the Market for Cyber Weapons. In: Yale Law and Policy Review 32(1), 239-266.

Stoner, K. & M. McFaul (2015). Who Lost Russia (This Time)? Vladimir Putin. In: The Washington Quarterly 38(2), 167-187.

De Telegraaf (2018). ‘Defensie komt met toekomstplannen’. De Telegraaf 26 maart 2018. Available online at: https://www.telegraaf.nl/nieuws/1836707/defensie-komt-met-toekomstplannen.

Tisdell, C. (2009). Economic reform and openness in China: China’s development policies in the last 30 years. University of Queensland working paper no. 55.

Trautman, L.J. (2016). Is Cyberattack the Next Pearl Harbor? In: North Carolina Journal of Law and Technology 18(2), 233-289.

Traynor, I., ‘Russia accused of unleashing cyberwar to disable Estonia’. The Guardian 17 mei 2007. Available online at: https://www.theguardian.com/world/2007/may/17/topstories3.russia.

Tweed, D. & P. Martin (2018). ‘‘Shocking’ Huawei Arrest Threatens to Upend Trump-Xi Trade Truce’. Bloomberg 6 december 2018,. Available online at: https://www.bloomberg.com/news/articles/2018-12-06/-shocking-huawei-arrest-threatens-to-upend-trump-xi-trade-truce.

UAWIRE (2017). ‘Russia proposes to place root Internet name servers in BRICS countries’. UAWIRE 28 november 2017. Available online at: https://uawire.org/russia-offers-to-deploy-root-name-servers-in-brics-countries.

United Kingdom Government (2016). National Cyber Security Strategy 2016-2021. Available online at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

United Nations Economic and Social Council (2011). Cybersecurity: A global issue demanding a global approach. Available online at: http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html.

United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2015). A/70/174.

United Nations General Assembly (2018a). Resolution A/Res/73/266.

United Nations General Assembly (2018b). Resolution A/Res/73/27.

United States Cybercommand (2018a). website: https://www.cybercom.mil/About/History/.

United States Cybercommand (2018b). Achieve and Maintain Cyberspace Superiority. Available online at: https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

United States Cyber Emergency Response Team. NCCIC Cyber Incident Scoring System. Available online at: https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System.

United States Department of Defense (2018). Cyber Strategy 2018. Available online at: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

United States Department of Justice (2018), 'Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps'. U.S. Department of Justice 23 maart 2018. Available online at: https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary.

United States Secretary of Defense (2018). Nuclear Posture Review. Available online at: https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF.

Valance, C. (2017). 'Russian Fancy Bear hackers UK link revealed'. BBC 23 november 2017. Available online at: https://www.bbc.co.uk/news/technology-42056555.

Varol, O., F. Emilio, C.A. Davis, F. Menczer & A.Flammini (2017). Online Human-Bot Interactions: Detection, Estimation, and Characterization. Conference paper, International AAAI Conference on Web and Social Media. Available online at: arxiv.org/abs/1703.03107.

Versteegh, K. (2017). 'De AIVD groeit als kool'. NRC 4 april 2017. Available online at: https://www.nrc.nl/nieuws/2017/04/04/de-aivd-groeit-als-kool-7916563-a1553167.

Volz, D. (2018). ‘Trump signs bill renewing NSA's internet surveillance program’. Reuters 19 januari 2018. Available online at: https://www.reuters.com/article/us-usa-trump-cyber-surveillance/trump-signs-bill-renewing-nsas-internet-surveillance-program-idUSKBN1F82MK.

Wagstaff, J. (2015). ‘Chinese hackers target Southeast Asia, India, researchers say’. Reuters 13 april 2015. Available online at: https://www.reuters.com/article/us-cybersecurity-fireeye-report-idUSKBN0N40AD20150413.

Ward, A. (2018). ‘Read: Mueller indictment against 12 Russian spies for DNC hack’. Vox 13 juli 2018. Available online at: https://www.vox.com/2018/7/13/17568806/mueller-russia-intelligence-indictment-full-text.

Wardle, C. & H. Derakhshan (2017). Information Disorder, Toward an Interdisciplinary framework for Research and Policy Making. Council of Europe Report.

Westcott, B. (2018). ‘International cyber crime ring smashed after more than $530 million stolen’. CNN 8 februari 2018. Available online at: https://edition.cnn.com/2018/02/08/world/us-cyber-crime-ring-arrests-intl/index.html.

The Washington Post (2013). ‘Inside the 2013 U.S. Intelligence ‘black budget’. The Washington Post 29 augustus 2013. Available online at: https://www.washingtonpost.com/gdpr-consent/?destination=%2fapps%2fg%2fpage%2fnational%2finside-the-2013-us-intelligence-black-budget%2f420%2f%3f&utm_term=.d22792fa0970.

The White House (2018). National Cyber Strategy. Available online at: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

World Bank (2018). website: https://www.worldbank.org/en/country/china/overview.

Wright, S. (1998). An appraisal of the technology of political control. STOA.

Yoo, C.S. (2015). Cyber espionage or cyberwar? International law, domestic law, and self-protective measures. In: J.D. Ohlin, K. Govern & C. Finkelstein (eds.). Cyberwar: Law and Ethics for Virtual Conflicts. Oxford University Press, 175-194.

Yu, J.M. (2018). ‘Chinese cyber attacks on Taiwan government becoming harder to detect: source’. Reuters 15 juni 2018. Available online at:

https://www.reuters.com/article/us-taiwan-china-cybersecurity/chinese-cyber-attacks-on-taiwan-government-becoming-harder-to-detect-source-idUSKBN1JB17L.

Zerodium (2018). Website: https://zerodium.com/

Zetter, K. (2011). ‘How digital detectives deciphered stuxnet, the most menacing malware in history’. Wired 7 juli 2011. Available online at: https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.

Zetter, K. (2013). ‘Google's Real Secret Spy Program? Secure FTP’. Wired 6 november 2013. Available online at: https://www.wired.com/2013/06/google-uses-secure-ftp-to-feds/.

Zetter, K. (2014). ‘Obama: NSA Must Reveal Bugs Like Heartbleed, Unless They Help the NSA’. Wired 15 april 2014. Available online at: https://www.wired.com/2014/04/obama-zero-day/#comments.

Zetter, K. (2015). ‘US and China Reach Historic Agreement on Economic Espionage’. Wired 24 september 2015. Available online at: https://www.wired.com/2015/09/us-china-reach-historic-agreement-economic-espionage/.

Zetter, K. (2016). ‘Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid’. Wired 3 maart 2016. Available online at: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

Contact details
Anna van Saksenlaan 51
P.O. Box 95366
NL-2509 CJ The Hague
+31 (0)70-342 15 42
info@rathenau.nl
www.rathenau.nl

The Rathenau Instituut 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