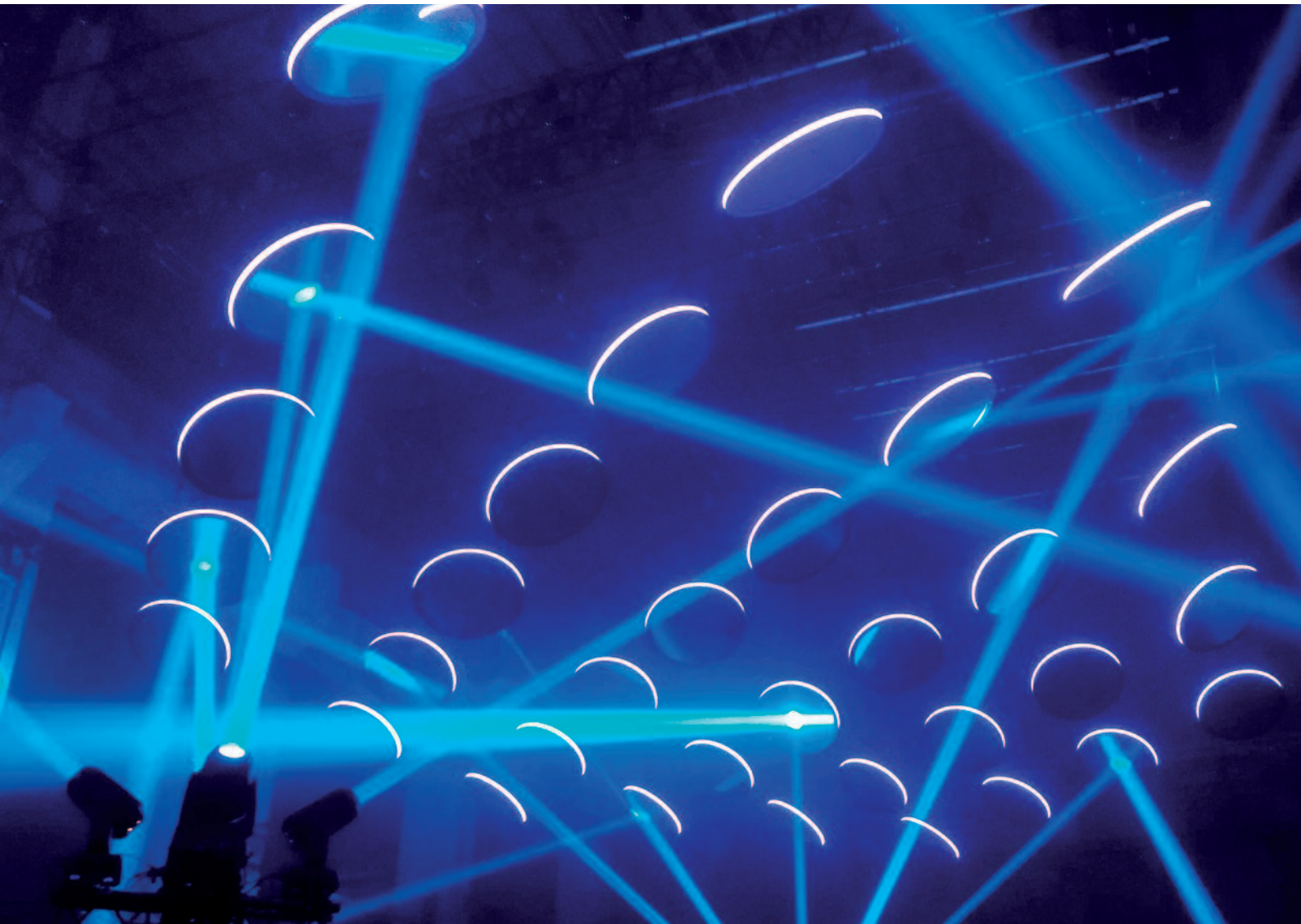
National Cyber Security Agenda

A cyber secure Netherlands



Contents

Foreword 5

Summary 7

Cyber security: the foundation for economic opportunity and social values 9

Espionage, sabotage and professional crime: threats in the digital domain 11

Strategic principles 13

The National Cyber Security Agenda 17

1. The Netherlands has adequate digital capabilities to detect, mitigate and respond decisively to cyber threats 19
2. The Netherlands contributes to international peace and security in the digital domain 23
3. The Netherlands is at the forefront of digitally secure hardware and software 27
4. The Netherlands has resilient digital processes and a robust infrastructure 31
5. The Netherlands has successful barriers against cybercrime 35
6. The Netherlands leads the way in the field of cybersecurity knowledge development 39
7. The Netherlands has an integrated and strong public-private approach to cybersecurity 43

Foreword

Security in the digital domain is a top priority for the cabinet. This is why we committed to a structural investment of 95 million euros in cybersecurity in the coalition agreement. In recent months, various departments, in close cooperation with parties in the public and private sectors, the scientific community and society, have been hard at work on an ambitious, government wide National Cyber Security Agenda. As the coordinating Minister for cybersecurity, I am proud to present the product of this successful cooperation!

We have formulated seven challenging ambitions which collectively will contribute to a secure, digital Netherlands. What is crucial to all of this is that the Netherlands has adequate digital capabilities to detect, mitigate and respond decisively to cyber threats . Government bodies and private organisations in the Netherlands must cooperate on for an effective integrated approach to cybersecurity. If all parties fulfil their responsibilities and have adequate capabilities and resources, then we can react decisively to digital threats.

For the government, this means above all: a strong coordinating role which stimulates and creates the necessary preconditions. This is to ensure that the business community and the citizens can shape their own digital security and resilience because, after all, they remain responsible for this themselves. If we are to continue to be able to exploit the opportunities of digitalisation in the long-term we must be able to securely navigate the digital world. Cybersecurity is the foundation for all successful entrepreneurship and administration and for confidence in the digital domain: this shared interest means that we are mutually dependent and share responsibility for national security. Because national borders play hardly any role at all in the digital world, the approach will also have to be strongly internationally oriented. The Netherlands must therefore also continue to work on strengthening digital security at the EU and NATO level.

Over the coming months, we will further elaborate the ambitions from the National Cyber Security Agenda into concrete measures in close cooperation with the departments and other partners involved.

Of course, this agenda is not set in stone. Over the coming years, it will be important to keep a finger on the pulse to closely follow technological and social developments to see where new digital vulnerabilities and threats may occur.

In presenting this National Cyber Security Agenda we are taking a crucial step towards a more secure digital Netherlands. This is the basis upon which we can continue to build towards a secure digital domain in which citizens, businesses and government agencies can capitalize on the economic and social opportunities offered by digitalisation!

Ferd Grapperhaus
Minister of Justice and Security

Summary

The Netherlands is in an outstanding position to capitalize on the economic and social opportunities of digitalisation. At the same time, vulnerabilities and threats in the digital domain are increasing. The threat from professional criminals is growing and continues to develop. State actors focus on digital economic and political espionage and on making preparations for digital sabotage. Not only are the number of countries that are developing digital attack capabilities increasing, the attacks that are carried out are also becoming increasingly complex. This forms a direct threat to our economic interests and national security.

These developments call for an increased effort to strengthen the approach to cybersecurity and thereby better protect the vital interests of the Netherlands. The National Cyber Security Agenda (NCSA) sets out the framework for the next step required in cybersecurity. The joint direction is laid out and various measures are considered collectively. This enhances the impact of public and private actions. The following principles are leading here:

- Cybersecurity is inextricably linked to national security: as a result of digitalisation, national security interests are vulnerable to digital attacks.
- Security in the digital domain can only be shaped in cooperation with and in part by the business community. Public-private cooperation therefore forms the basis for the Dutch approach to cybersecurity.
- The government represents public interests: a digital secure Netherlands, by recognizing threats to vital interests and by strengthening resilience. The business community and citizens are encouraged to shape their own responsibilities and security. In addition, the government, as a public body, is obliged to have the cybersecurity of its own processes in order and to set a good example as a launching customer.
- Knowledge is crucial to cybersecurity: sharing the available knowledge and promoting information sharing by the public and private sector is needed to strengthen cybersecurity across the board. In addition, it is necessary to (continue to) stimulate both fundamental and applied research into cybersecurity, to develop the Dutch cybersecurity knowledge position.
- The objective is the mainstreaming of cybersecurity: digital security must be part of the everyday processes of every organisation.
- The digital domain is not confined by national borders. A Dutch approach to cybersecurity must take the international dimension into account of data, connections, internet governance and actors who carry out digital attacks. A more secure digital domain is therefore one of the Netherlands' priorities in, amongst others, NATO and the EU.
- Finally: the tension between the interests of freedom, security and economic growth is inherent in the development of cybersecurity. By taking this into account, we want to weigh the dilemmas in cybersecurity more explicitly and set the course based on transparent and substantiated decision-making.

The NCSA comprises seven ambitions that contribute towards the following objective: ***The Netherlands is capable of capitalizing on the economic and social opportunities of digitalisation in a secure way and of protecting national security in the digital domain.***

1. The Netherlands has adequate digital capabilities to detect, mitigate and respond decisively to cyber threats
2. The Netherlands contributes to international peace and security in the digital domain
3. The Netherlands is at the forefront of digitally secure hardware and software
4. The Netherlands has resilient digital processes and a robust infrastructure
5. The Netherlands has successful barriers against cybercrime
6. The Netherlands leads the way in the field of cybersecurity knowledge development
7. The Netherlands has an integrated and strong public-private approach to cybersecurity

These seven ambitions have been elaborated into objectives and measures that will be implemented in close public-private cooperation. To ensure this, a cybersecurity alliance will be formed between government bodies and businesses in which they will commit to jointly strengthening the Dutch approach to cybersecurity.

Cyber security

the foundation for economic opportunities and social values in the digital domain

The Netherlands is one of the most digitalized countries in the world. This offers us outstanding conditions to be an international leader in securely, freely and quickly adopting and using new technologies. These new technologies play an increasingly significant role in our daily lives. One example is e-commerce, others include digital communication with our doctor, school and the public authorities. Moreover, far-reaching digitalisation in care (e-health), mobility (e-automotive), the growth in internet-connected devices and appliances (Internet of Things), key technologies such as *big data*, 5G, quantum computers and artificial intelligence ensures that the digital domain and the physical domain are becoming more closely interwoven. These developments also raise ethical questions in regard to privacy and dealing with data. Protecting values and fundamental rights in the digital domain is also an important component of cybersecurity. Citizens must be able to count on the fact their fundamental rights are assured both online and offline and that their privacy is also being guaranteed in the digital domain.

These technological and social developments have also led to an increase in the vulnerabilities in the digital domain, a trend that is expected to continue in coming years. It is precisely because every aspect of society – social and economic – increasingly depends on digital processes that digital attacks can directly damage our economy and threaten national security. After all, social processes are easier to disrupt on a large scale. The increased vulnerability is apparent from the successive Cyber Security Assessments Netherlands, in which Dutch intelligence and security services, the National Coordinator for Security and Counterterrorism (NCTV), the National Cyber Security Center (NCSC) and the police indicate a worrying increase in digital threats. Moreover, resilience is lagging behind the development of the threat. This situation requires additional efforts from public authorities, the business community and citizens to protect Dutch interests and to strengthen the Dutch approach to cybersecurity in the interests of national security.

Definition of cybersecurity
Cybersecurity is the entirety of measures to prevent damage caused by disruption, failure or misuse of ICT and to recover should damage occur.

At the same time, cybersecurity as a business sector also provides economic and social opportunities: a strong Dutch cybersecurity sector stimulates the development of knowledge, the labour market and employment opportunities and contributes to the Netherlands' international profile in the economic, military and security fields. Moreover, a strong Dutch cybersecurity sector contributes towards digital autonomy: public authorities and the business community can rely on their own solutions for digital security and they also foster digital security in the broadest sense by acquiring cybersecurity services for their own processes. This incentive also fosters the export of Dutch values such as an open, free and secure internet. In this way, the Netherlands also improves its position internationally as a known and recognized collaboration partner and cybersecurity authority.

THE SCOPE OF CYBERSECURITY: A CYBER SECURE NETHERLANDS

The Minister of Justice and Security is the coordinating Minister for cybersecurity and coordinates the implementation of the NCSA. Within the framework all parties have their own tasks and responsibilities. However, also in the digital domain a 100% security is not realistic. This broad Dutch approach to cybersecurity is implemented as part of protecting national security, which is coordinated by the NCTV.

POLICY RESPONSIBILITIES IN THE DIGITAL DOMAIN

The cybersecurity policy field focuses on preventing damage caused by disruption, failure and misuse of ICT. Various policy issues are related to this; responsibility for addressing them lies with other ministers. This concerns in particular the Ministry of the Interior and Kingdom Relations (BZK) because of the responsibility for digital government and the General Intelligence and Security Service (AIVD), the Ministry of Economic Affairs and Climate Policy (EZK) in connection with digitalisation, the Ministry of Foreign Affairs (BZ) because of the coordinating role in international peace and security and finally the Ministry of Defence (Def) in relation to the constitutional duties of the armed forces in the digital domain. The NCSA is closely related to the following strategic documents: The Digitalisation Strategy (*Digitaliseringsstrategie*under development), the Broad Agenda for Digital Government *Brede Agenda Digitale Overheid*under development), the Defence Memorandum (*Defensienota*) and the Integrated Foreign and Security Strategy (*Geïntegreerde Buitenland- en Veiligheidsstrategie*) and the International Cyber Strategy and Defence Strategy (*Internationale Cyberstrategie en Defensie Cyberstrategie*under development).

From National Cyber Security Strategy 2011 to National Cyber Security Agenda 2018

The NCSA builds further upon the effects that were realised with previous the National Cyber Security Strategies from 2011 and 2013. The vision from these strategies is still leading: *'The Netherlands, together with her international partners, is committed to a secure and open cyber domain in which the opportunities offered to our society by digitalisation are fully exploited, threats are mitigated, and fundamental rights and values are protected.'* The agenda indicates a joint course which clarifies what government bodies and private parties can focus their (joint) activities on. The NCSA reviews various measures in conjunction, links them in guiding objectives and in doing so reinforces their impact.

Espionage, sabotage and professional crime

threats in the digital domain

Digital sabotage or disruption can directly lead to damage to national security. The greatest threat in the digital field comes from criminals and state actors. Digitalisation has permeated into all levels of Dutch society and the economy. Consequently, our society has become fully dependent on digital resources. The undisturbed functioning of these resources is essential to vital processes in business and government, the earning power of companies and the daily lives of citizens. Incidents in recent years have made it clear that digital attacks can have a major impact on society and can lead to damage to physical and national security. The threat from professional criminals is growing and continues to develop. Successful criminal revenue models, such as ransomware continue to develop and are being expanded. The almost cost-free scalability of digital attacks is of particular interest to criminals.

It is not only consumers who fall victim. Businesses and financial institutions are also targets for criminals. More complex methods of attack are becoming more widely available due to developments such as cybercrime as a service. As a result of this, more and more actors with limited knowledge and resources can carry out attacks that in some cases have direct social impact.

State actors are structurally targeting Dutch government agencies and companies in the Netherlands for digital espionage.For instance, multinationals and research institutes in the de energy, hightech, and chemical sectors have been victims of digital espionage. In these digital break-ins, terabytes of confidential information was stolen which represents a substantial economic value. State actors focus on digital economic and political espionage and on making preparations for digital sabotage. Not only are the number of countries that are developing digital attack capabilities increasing, the attacks that are carried out are also becoming increasingly complex. In addition, last year state actors also focused on digitally influencing democratic processes for geopolitical gain. To safeguard geopolitical interests, nations are investing in civilian and military cyber capabilities.

Example: Cybercrime as a service and ransomware

Cybercriminals do not by any means perform all steps in an attack themselves. They often buy services and expertise. An example of this is ransomware: a type of malicious software that blocks systems and/or the information they contain and only makes them accessible again against payment of a ransom. If a criminal wants to distribute ransomware they pay someone to develop it, for instance, and someone else to distribute the *ransomware* by email to millions of addressees. These services are provided very professionally and completely: from technical resources to infrastructure and helpdesk functionality.

Cyber attacks impact on our society. For example, citizens have to contend with the consequences of identity theft or the loss of personal photos due to a ransomware infection. Such attacks have the potential to undermine trust in the digital society. Cyber attacks by criminals or state actors can undermine the Dutch economy through theft of sensitive or valuable information and thereby damage confidence in economic activity.

Example: *NotPetya*
The *NotPetya* case is an example of a digital attack with considerable consequences for Dutch businesses. In June 2017, organisations across the globe fell victim to a ransomware attack. In the Netherlands, this ransomware affected the business operations of APM's container terminal and TNT's parcel deliveries, among others. Container processing at APM was halted for several days and TNT's deliveries were also delayed as a result of the attack. Although the Ukraine seemed to be the primary target of this attack, there were significant consequences for Dutch businesses.

Strategic principles

An effective approach to cybersecurity also takes the dynamics that are specific to the digital domain into account. This requires strategic principles for determining ambitions and measures.

CYBERSECURITY IS AN INTEGRAL PART OF NATIONAL SECURITY

Cybersecurity is inextricably linked to national security and the smooth functioning of society. As a result of digitalisation, society has become vulnerable to disruptions from digital attacks. Because of the connectivity of the digital society, simple digital attacks can quickly disrupt digital processes. A basic level of cybersecurity is needed to increase resilience against these kind of attacks. Citizens, businesses and public authorities must endeavour to improve their digital security and the government must also be able to fulfil its protective duty in the digital domain. Capabilities and resources to address threats should be in order. Finally, national security and cybersecurity should be a basic consideration in the further development of the government's digital processes. This means that the government will develop cybersecurity requirements for procuring its own ICT resources. These requirements will also include economic security considerations to improve resilience against state actors.

PUBLIC-PRIVATE COOPERATION IS THE BASIS

Security in the digital domain can only be shaped in cooperation with, and to a significant extent by, the business community. Public-private cooperation therefore forms the basis for the Dutch approach to cybersecurity. Current practice in this cooperation shows that there is a need for a clear division of responsibilities in the digital domain. Those responsibilities will, in part, be based on existing laws and regulations on security, assurances of supply and market organisation. However, new issues will also arise where the responsibilities between public authorities, the business community and citizens will have to be established (or re-established). This is why this Agenda favours an integrated approach to cybersecurity, which requires joint efforts from the business community, social organisations and the various government bodies.

GOVERNMENT REPRESENTS PUBLIC INTERESTS, STIMULATES ACCEPTANCE OF OWN RESPONSIBILITIES AND SETS A GOOD EXAMPLE

A key task of the government is to take the lead in the commitment to a secure and stable Netherlands by recognizing threats to vital interests and increasing the resilience of those interests. This means that the government ensures an appropriate approach to and preparations for crises and incidents that threaten social continuity, even though 100% security is not possible in the digital domain either. Approximately 80% of the critical infrastructure is in private hands. The government therefore encourages the business community and citizens to shape their own responsibilities in the best possible way. Where necessary, stimuli will be provided or frameworks will be set up to create the preconditions for secure behaviour in the digital domain. The open nature of the internet can lead to widespread vulnerabilities. Where the misuse of products, services or processes puts the continuity of society at risk, the government sets special requirements for producers, purchasers, consumers and service providers. Finally, the government, as a public body, is obliged to have the cybersecurity of its own processes in order and thereby, as a launching customer, also sets a good example.

KNOWLEDGE DEVELOPMENT AND INFORMATION SHARING ARE CRUCIAL

Knowledge is crucial to cybersecurity: sharing the available knowledge and promoting information sharing by the public and private sector is needed to strengthen cybersecurity and resilience across the board. In addition, it is necessary to (continue to) stimulate both fundamental and applied research into cybersecurity, to develop the Dutch cybersecurity knowledge position. Having our own high-quality scientific knowledge and applications will contribute to the digital autonomy of the Netherlands and/or Europe.

MAINSTREAMING OF CYBERSECURITY IS A PRECONDITION

Digitalisation permeates through to all facets of society. Cybersecurity forms the basis for successful entrepreneurship, administration and participation in

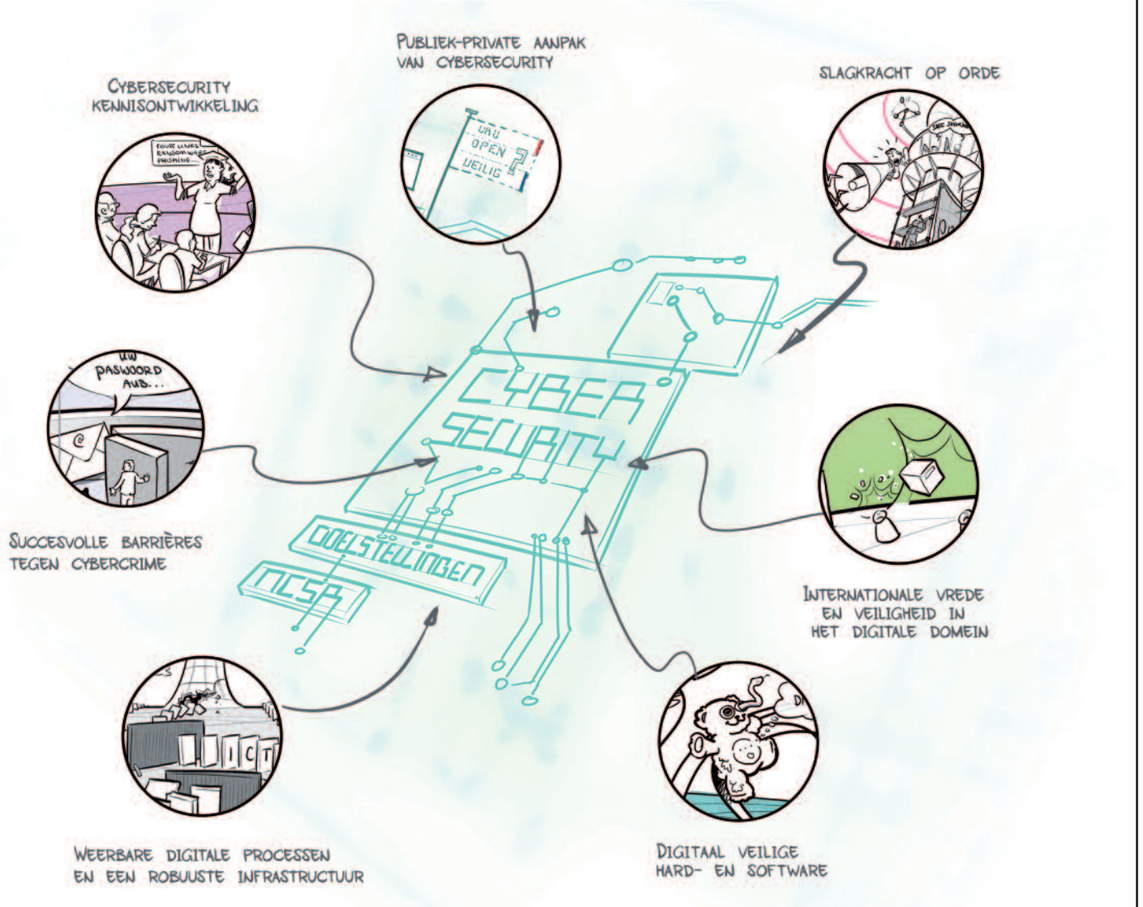
society. There is a need for public authorities and businesses to be better able to or enabled to organise their digital security and make that digital security part of their daily processes, products and services (the mainstreaming of cyber security). Citizens and/or end users also have a responsibility in safeguarding their own digital security: a basic level of cyber ecurity should be part of secure behaviour in everyday life.

THE DIGITAL DOMAIN HAS NO NATIONAL BORDERS

The digital domain is, by definition, not confined by national borders. A Dutch approach to cybersecurity must take the international dimension of data, connections, internet governance and actors who carry out digital attacks into account. This is why a more secure digital domain is one of the Netherlands' priorities at the EU and NATO level. After all, an alliance that can also fulfil its collective defence duties in the digital domain makes a direct and essential contribution to the national (digital) security of the member states. In addition, it will only be possible to achieve some of the objectives of the NCSA through international legislation, the formation of coalitions or the international development of norms and standards, at European level in particular. The cross-border nature of threats creates a need to commit strongly to international cooperation. The National Cyber Security Agenda, in combination with the Integrated Foreign and Security Strategy (*Geïntegreerde Buitenland- en Veiligheidsstrategie*) and the Defence Memorandum (*Defensienota*) provide guidance for the further development of Dutch efforts in international forums. On the one hand, this applies to those effects and results that can only be achieved at international level and on the other hand the international developments will also have to be taken into account in the effective shaping of Dutch policy. Key examples are European developments in the field of certification, developing standards and stimulating the European Digital Single Market, of which cybersecurity is a part. The Netherlands continues to play its role of internet pioneer in topics such as the fragility of open source software.

TENSION BETWEEN INTEREST REQUIRE CAREFUL CONSIDERATION

Far-reaching digitalisation often puts pressure on the balance between the core values of security, freedom and economic growth. The Netherlands is committed to clear consideration of the interests in making (policy) choices and tries to be transparent when doing so. In the wider social and political debates about digitalisation, cybersecurity cannot be approached in isolation but must expressly be considered in conjunction with topics such as fundamental rights and values and social growth. Clear and transparent consideration of the tension between interest results in better decision-making.



The Netherlands is capable of capitalizing on the economic and social opportunities of digitalisation in a secure way and of protecting national interests in the digital domain

The National Cyber Security Agenda

The Dutch approach to cybersecurity has the following objective:
The Netherlands is capable of capitalizing on the economic and social opportunities of digitalisation in a secure way and of protecting national security in the digital domain.

We are therefore committed to the following ambitions:

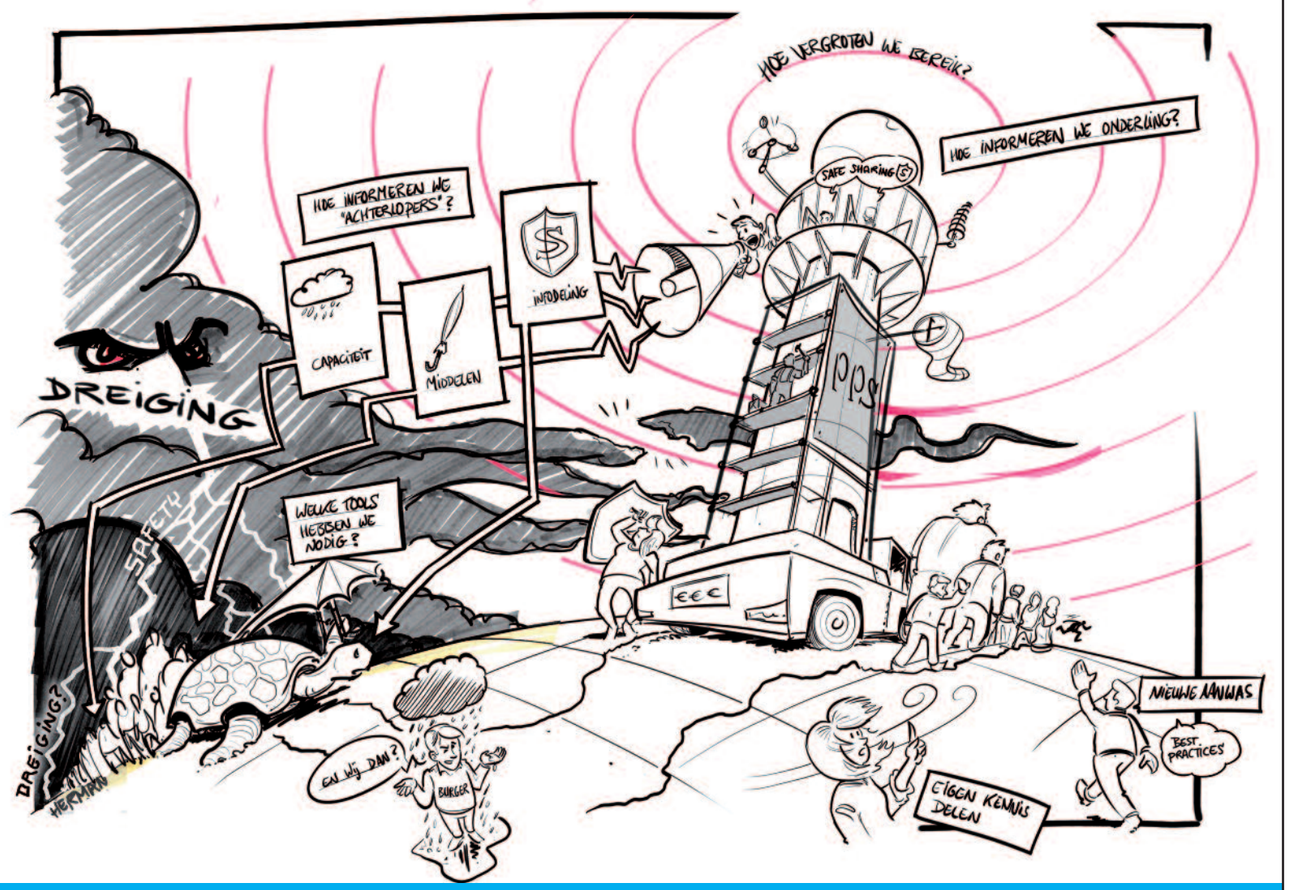
1. The Netherlands has adequate digital capabilities to detect, mitigate and respond decisively to cyber threats
2. The Netherlands contributes to international peace and security in the digital domain
3. The Netherlands is at the forefront of digitally secure hardware and software
4. The Netherlands has resilient digital processes and a robust infrastructure
5. The Netherlands has successful barriers against cybercrime
6. The Netherlands leads the way in the field of cybersecurity knowledge development
7. The Netherlands has an integrated and strong public-private approach to cybersecurity

The impact of technological and social developments and the digital threat are developing at different speeds and this requires a dynamic, long-term approach to cybersecurity. Many of these measures require a government contribution. Some other measures can only be taken with or by the market parties. This requires close cooperation in the development of the NCSA. The measures are not exhaustive. There is scope for additions. This leads to a dynamic approach that can be adjusted to match the development of the threat. It is also why the annual Cyber Security Assessment Netherlands will consider if this approach needs to be recalibrated and if policy instruments contribute to the realisation of the ambitions. The Agenda will be evaluated in 2021 and revised where necessary.

Coalition agreement
An ambitious cybersecurity agenda will be formulated with, among other things, standards for *internet of Things* devices, software liability, strengthening the NCSC, promoting cybersecurity research and improving information campaigns.

Ninety-five million euros of structural funding is being reserved for cybersecurity. The resources will be used for, among other things, improving staff capacity and expanding ICT facilities and will be shared by the departments of Justice and Security (NCTV), Defence (MIVD), Interior and Kingdom Relations (AIVD), Foreign Affairs, Infrastructure and the Environment and Economic Affairs.

The structural intensification of cybersecurity has been integrated into the measures in this NCSA.



The Netherlands has adequate digital capabilities to detect, mitigate and respond decisively to cyber threats

1. The Netherlands has adequate digital capabilities to detect, mitigate and respond decisively to cyber threats

To respond effectively to the growing digital threat, government bodies and private organisations in the Netherlands must cooperate and have appropriate capacities and resources. A number of these organisations are still developing those capacities and they are at various levels of maturity. While some (larger) businesses and organisations are arranging their own security operations center or computer crisis team, other (smaller) businesses or organisations are only just or not sufficiently aware of digital risks. Protection of their own digital systems and information by these public and private parties is not yet a given and basic security regulations have not yet been implemented .

Sufficient capabilities also include the capacity of security organisations which must be able to carry out their tasks for national security in the digital as well as the physical domains. This is closely tied-in with the offensive capabilities of Defence, which are covered under Ambition 2.

There is an urgent need to build up capabilities, for more and better tailor-made information about digital threats, which is available to government bodies and private organisations more swiftly and for perspective for action for mitigating those threats. The exchange of information between organisations and businesses in the Netherlands has improved greatly in recent years as a result of cooperation on incidents or because parties have come to know each other and started trusting each other. Although this is a step in the right direction, it still does not provide sufficient guarantees that we can address digital threats now and in the future. The next step is to structurally guarantee the exchange of information and existing cooperation while at the same time expand the range, for instance by promoting cross-sector analyses. There is a need to improve the detection and response capabilities of government organisations and providers of critical services. By doing so, we will increase the digital capabilities of these parties as a whole. We must adopt a practice in which customers and suppliers encourage each other to arrange their digital security. In this way, we will work towards a cyber ecosystem in which all parties build up capacities and

share information; from the business community to public authorities and from individual citizens to cybersecurity professionals.

OBJECTIVES

- Public authorities and businesses are capable of responding appropriately to digital threats and attacks. To do this, they implement the necessary (preventative) measures and they have the basics in order.
- The Netherlands is prepared for large-scale cyber incidents which pose a threat to national security.
- Organisations of vital importance to national security have a better understanding of digital threats and attacks and are capable of detecting attacks that threaten themselves and national security.
- A nationwide network of cybersecurity partnerships will be created within which information about cybersecurity can be shared between public and private parties more widely, efficiently and effectively. The aim of this nationwide network is to strengthen the capabilities of public and private parties.
- The legal instruments for effective action in the digital domain remain in order and are kept up to date in light of the threat and technological developments.

MEASURES

o The incident response capabilities of, amongst others, the intelligence and security services, Defence Computer Emergency Response Team (CERT), the National Cyber Security Center (NCSC) and Rijkswaterstaat (Directorate-General for Public Works and Water Management) are being enhanced to be able to deal with ICT breaches that threaten national security. In addition, the creation of more private sector-wide computer crisis teams, such as Z-CERT (for the care sector) and I-CERT (for the insurance sector) is encouraged.

o The critical processes in our society demand extra protection and accelerated recovery in the event of failure or damage. It is therefore important that these organisations ensure that they have an appropriate response capacity or that they have agreement in place for this with a trusted third party. To this end, the development of a certification system for cybersecurity service providers, from whom secure services can be acquired, will be explored with private parties.[1]

o The Netherlands must be prepared for large-scale cyber incidents that threaten national security. The National Crisis Plan for ICT (*Nationaal Crisisplan ICT*) will be being updated. In addition, an integrated ICT emergency exercise policy will be formulated. It will include arrangements between government bodies and private organisations on a joint exercise agenda and the available capabilities of the parties involved for this.

o The capabilities of the intelligence and security services, DefCERT and the NCSC to gain insight into threats and digital attacks, to detect them, disrupt them and increase resilience will be improved structurally. To ensure this, the government has allocated additional funding in recent years and in the coalition agreement. The National Detection Network [*Nationaal Detectie Netwerk, NDN*] will be further enhanced to create a future proof network.

o Situational awareness at the national level will be enhanced by the creation of a cooperation platform[2] with the goal to offer more information and a swifter perspective for action with relevant organisations within the legal frameworks. When doing so, attention should also be paid to cybersecurity requirements. Recipients need to have a certain level of maturity to enable information sharing.

o Under NCTV coordination, round table discussions are organised in which the nationwide network of cybersecurity partnerships can be developed. This will build on the experiences from existing public and private cybersecurity partnerships.

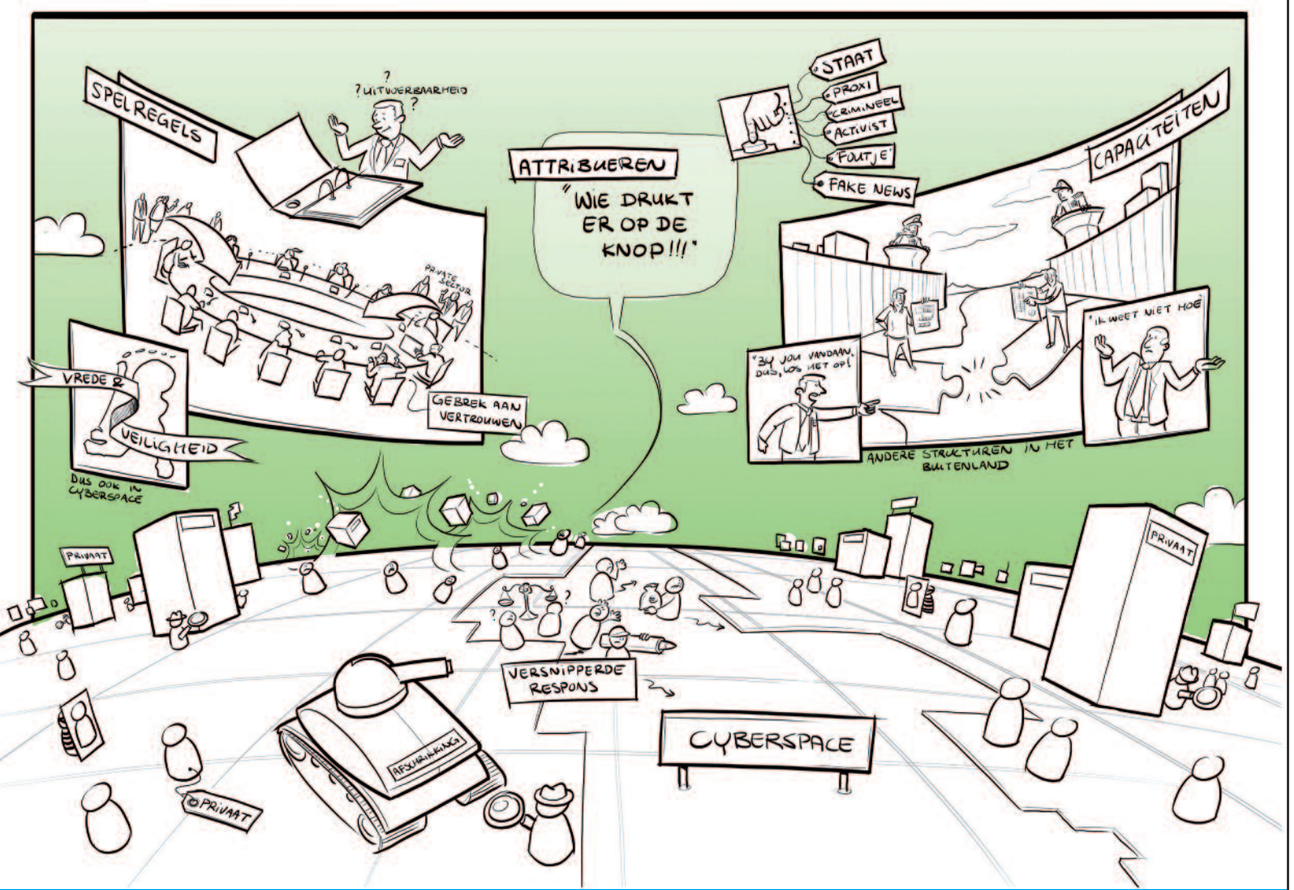
o The National Cyber Security Center (NCSC) and the Digital Trust Centre[3] (DTC) will encourage – and support where necessary – the creation and further development of cybersecurity partnerships for public authorities, the business community and civil society organisations. This will also include the creation of a set of basic security measures for the business community and civil society organisations.

o Legislation aimed at protecting national security will be reviewed to what extent it provides satisfactory possibilities to promote security in the digital domain, whilst retaining fundamental values and privacy.

1 Please also see the objectives and measures on pages 27-28.

2 The possibilities for developing this cooperation platform, with which parties and the form it should take will be explored further.

3 Letter to Parliament 'Setting up the Digital Trust Centre', 23 September 2017.



The Netherlands contributes to international peace and security in the digital domain

2. International peace and security in the digital domain

More and more frequently, state actors employ digital resources for espionage, influencing and sabotage objectives as an integral part of their range of instruments to exert power, or in concrete conflict situations. There has also been an increase in the number of countries that are building offensive, military cyber capabilities. This threat has grown significantly in recent years and is a serious threat to international security.

At an international level, there are strong divisions between various countries in the approach to the cyber domain. There are differences of opinion on the application of international law, norms of behaviour in cyberspace and the dependence on and access to digital resources. Moreover, the decentralised nature of the internet and the opportunities the internet provides for anonymous action impede the enforcement and supervision of agreements that have been made. Due in part to the fact that attribution is difficult in the cyber domain, such cyber operations can pose a threat to international legal order. The Netherlands should also have its own capabilities and instruments to be able to resolutely avert digital attacks on our national interests and – in extremis – to retaliate proportionately.

OBJECTIVES

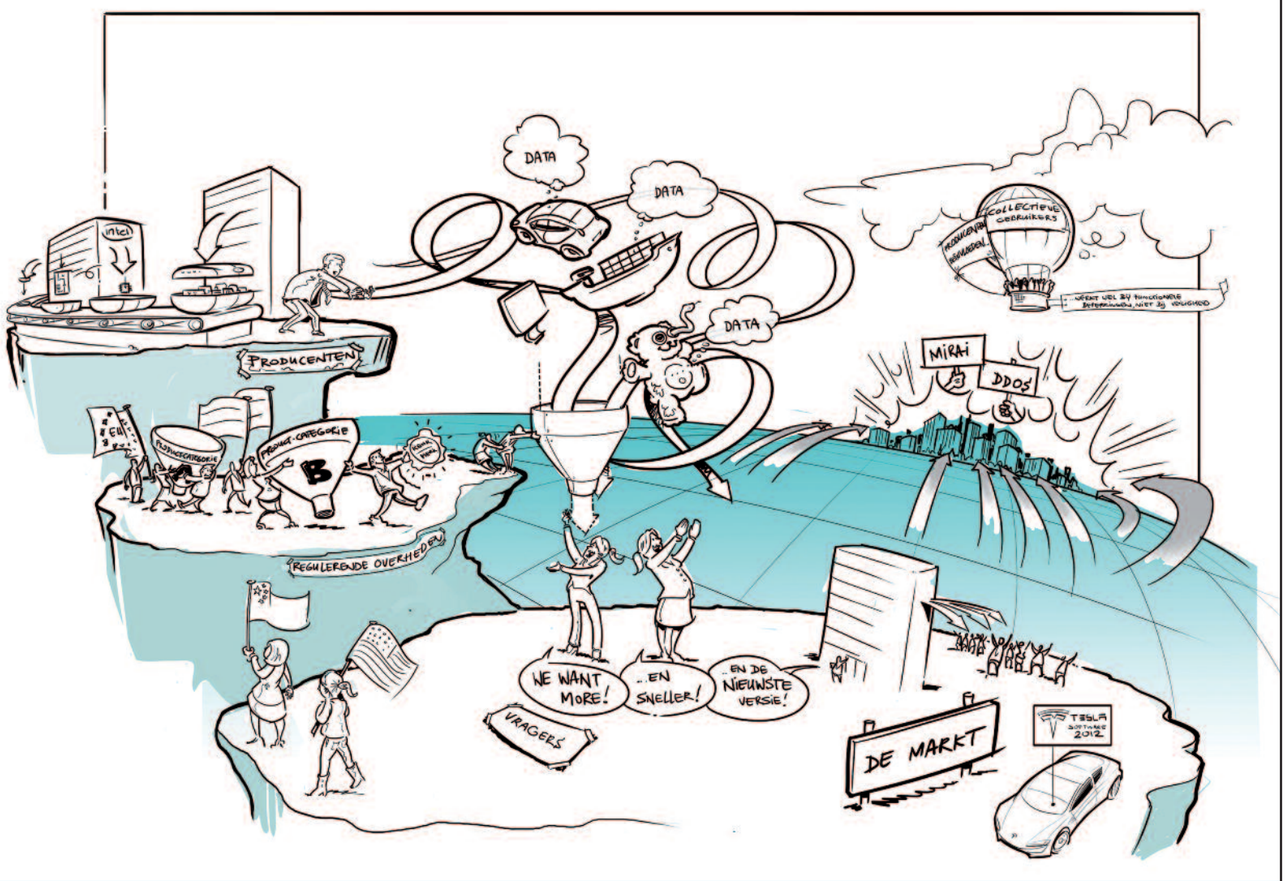
- The Netherlands promotes the international legal order in the digital domain, including safeguarding human rights.
- The Netherlands is able to respond immediately and appropriately, alone or as part of a coalition, to digital attacks by state actors and has offensive capabilities that contribute to deterrence.
- The Netherlands contributes to the mitigation of cyber threats from criminals and state actors, by investing in the development of capabilities of the global cybersecurity chain.

MEASURES

o The Netherlands will bolster the application of international law in cyberspace, promote additional norms and build trust between states and other parties. The Netherlands continues to build and broaden the international coalition which subscribes to the vision of an open, free and secure internet. The Netherlands will do this by promoting the further interpretation and application of international law in the digital domain, for instance in the field of human rights, humanitarian law and the framework for combating cybercrime, and for the protection telecommunications and critical infrastructure. In addition, confidence building measures between states and the further development of norms will be encouraged. The Global Commission on the Stability of Cyberspace has already made an important contribution to this.

o The Netherlands will develop a broad strategic framework for responding to digital attacks. It will include all available instruments, including (public) attribution, deterrence, use of offensive capabilities and a broader response in the cyber domain. To this end, the Netherlands will strengthen the diplomatic and political response to disruptive or destructive cyber operations by state actors. The framework will be followed with a suitable range of instruments for a diplomatic response. This ties in with the cyber diplomacy network and the toolbox for diplomatic action in the event of cyber incidents developed by the European Union. The Netherlands played a leading role in this.

- To deter (potential) adversaries, the Netherlands will further enhance the offensive cyber capabilities of its armed forces. In doing so, we contribute to the development and operationalisation of the capability to act in the digital domain at EU and NATO level. This will also serve to support military missions and operations in the physical domain.
- The Netherlands makes a significant contribution to a free, open and secure internet and promotes adequate protection of human rights online, for instance through the development of norms. This will, in part, be shaped by the further development of the Freedom Online Coalition.
- The Netherlands strengthens the global cybersecurity chain by improving the security level of third countries and by reducing the digital divide between technologically advanced countries and those less advanced. Strategic capacity building projects are facilitated through the Global Forum on Cyber Expertise (GFCE) and the international multi-stakeholder coalition for an open, free and secure internet will be expanded.



The Netherlands is at the forefront of digitally secure hardware and software

3. Digitally secure hardware and software

As a result of the introduction and continuous development of the Internet of Things, more and more devices are connected to the internet. Some 20.4 billion devices are expected to be connected in 2020. At least 63% of them will be consumer devices.[4] The remaining 37% are devices used by businesses and for which the impact in case of disruption or misuse (on businesses' own processes, but also further along the chain) is potentially much greater than in case of private use.

It is important that everyone is able to use these products with confidence in a digitally secure manner, not only for their own digital security, but for that of society as a whole. Malicious parties can easily gain access through vulnerabilities in hardware and software in a device, and through this device to the network it is part of.

Users and providers of digital products often do not or barely consider the potential harmful effects of their actions on others. This can have serious consequences, such as the misuse of the device for DDoS attacks, manipulation of the device or the theft of stored information.

Digital security of hardware and software is not ensured by default. Hardware and software providers do not always resolve the security risks that are associated with their processes and production. Users have hardly any means of making a reliable assessment of the digital security level of a device that is connected to the internet - and even if they do have the knowledge, it is still difficult to make an assessment. For instance, it is difficult for users to assess the long-term impact of their decisions. Very often, specialist knowledge is needed to fully understand the digital security of a device. Users therefore need to be empowered. This is done by providing instruments, aimed at the behaviour of users, to make an estimation of the digital security of hardware and software. Research into the effectiveness of information campaigns on secure user behaviour plays an important role in this regard.

OBJECTIVES

A cohesive set of measures is needed to encourage and enhance the digital security of hardware and software in a balanced way, and for which various parties have a responsibility. This why the Netherlands will implement and further develop the Roadmap for Digitally Secure Hardware and Software (Roadmap Digitaal Veilige Hard- en Software).[5] The following objectives apply here:

- The Netherlands will encourage standardisation and certification initiatives and by strengthening supervision and enforcement, in order to prevent digital security risks in hardware and software.
- The Netherlands will work to improve the detection of digital security risks by testing digital products and making the digital security risks clear.
- The Netherlands will work on mitigating of digital security risks through a liability regime, and by increasing awareness and by offering a perspective for action for citizens and businesses.
- The Netherlands will strive to for the realisation of a set of basic principles to foster the digital security of hardware and software.

MEASURES

- Standards and certification make an important contribution to the digital security of hardware and software.
- In the negotiations in Brussels, the Netherlands will advocate the quick adoption of the Cyber Security Act (CSA), and the expeditious development of a European framework for security certification for ICT

4 https://www.gartner.com/newsroom/id/3598917.

5 Roadmap Digitaal Veilige Hard- en Software [Roadmap for Digitally Secure Hardware and Software Roadmap], Ministry of Economic Affairs and Climate Policy, 2018.

products and services. In the short term, the government will advocate the adoption of mandatory certification for specific product groups. That is, for products where the risk is greatest or products that have many problems in practice. In the long term, there must be a gradual expansion of mandatory certification or compliance with a CE mark for all internet-connected products should be implemented.

- In addition, the Netherlands will encourage the adoption of international standards, partnerships and frameworks. The Netherlands wants to proactively join relevant European and global standardisation and certification initiatives through the NEN standardisation platform. The Netherlands is also going pursue multilateral cooperation on standardisation for the Internet of Things, amongst others through the Global Forum on Cyber Expertise (GFCE).
- Together with public and private parties, the government will develop a monitoring system with information about the digital security of digital products, with specific attention to Internet of Things devices. The government will include international experiences in this.
- The government will enter into discussions with internet access providers about how they will contribute to combating insecure Internet of Things devices – analogues to the successful approach to botnets. Product testing is crucial to gain assurances on the digital security of devices. Based on use cases from various sectors, a pilot will be launched to gain knowledge and understanding on what a shared testing platform can offer.
- The development and commercialisation of innovative solutions can make an important contribution to making hardware and software digitally secure. Through the National Cyber Security Research Agenda III (NCSRA III), which is due to be published in 2018, the Netherlands will pursue the development of cybersecurity research aimed at the development and commercialisation of innovative solutions. In addition, various research tenders that contribute to new, innovative, digitally secure hardware and software are ongoing as a result of application of the Small Business Innovation Research (SBIR)[6]. Furthermore, the government encourages open-source encryption by making additional resources available for this within the framework of NCSRA III. Finally, the government will organise dialogue sessions on innovative solutions to keep hardware and software secure or whether some solutions should be discontinued. This also refers to objectives under Ambition 5.
- Liability is an important financial incentive for suppliers to make and keep their hardware and software secure. The government is discussing focus areas, areas of improvement and potential solutions for liability with regard to digitally insecure hardware and software with stakeholders and academics. In addition, the Netherlands is actively participating in the liability and new technologies experts group and involves the contribution of Dutch stakeholders in this process. Furthermore, in the negotiations on the Proposal for a Directive on Digital Content and Digital Services, the Netherlands proposes to include an obligation to make security updates mandatory in all cases involving software supplied to a consumer.
- Setting minimum security requirements can keep insecure products off the market. The government will investigate which minimum requirements could be set for devices through the European Radio Equipment Directive.[7]
- The government will investigate what additional measures are needed and desirable for the digital security of hardware and software when procured by central government.
- Supervision and enforcement encourages suppliers to comply with laws and regulations. The government will organise a national dialogue session for supervisory bodies to see what role they can play in the near future to promote the digital security of hardware and software, to create synergy between the various activities of the supervisory bodies and to examine how cooperation between supervisory bodies can be improved.
- Awareness and empowerment make an important contribution to the digital security of hardware and software because, among other things, as a result providers can take digital vulnerabilities into account and users are aware of the possible risks. As part of the cybersecurity awareness campaigns by veiliginternetten.nl, the government will launch one or more policy-supporting public campaigns for digitally secure hardware and software.

6 SBIR benut de creativiteit van ondernemers om maatschappelijke problemen op te lossen en daagt ondernemers uit om nieuwe producten te ontwikkelen en op de markt te brengen, zie https://www.rvo.nl/subsidies-regelingen/sbir.

7 Kamerstuk 26643, nr. 467 en Kamerstuk 24095, nr. 415.



The Netherlands has resilient digital processes and a robust infrastructure

4. Resilient digital processes and a robust infrastructure

ICT is becoming increasingly interwoven with Dutch society. One of the consequence of this is that the operations of businesses and public authorities are becoming increasingly data-driven through intelligent applications. Organisations are often no longer capable of carrying out all of the tasks themselves. They operate in chains. They depend on other organisations for, among other things, supplying the data or for carrying out or supporting their data processing. This is not without risk. Business processes can be disrupted if data is not exchanged with other organisations in a secure and reliable manner. When this occurs in the chains of providers of critical processes, it can lead to major system failure, damage to physical security and societal disruption. Problems could arise with the physical infrastructure or with the protocols and the software for data exchange. Finally, the parties that provide data processing services may cease to exist or fall short.

Due to the importance of the availability (or continuity) of data communications networks, specific requirements are set for the providers of such networks, amongst others through the Telecommunications Act [Telecommunicatiewet] and the proposed legislation for the Cybersecurity Act [*Cybersecuritywet, CSW*].[8] Their objective is that such providers make their systems resilient to various threats and incidents, including those that could lead to failure of the physical infrastructure. The CSA also creates the obligation to implement suitable technical and organisational measures for all providers of an essential service and digital service providers. Implementation of this will be overseen by the sectoral supervisory bodies. This will further increase the security level of providers and create the possibility to take firm action against vulnerable (not appropriately protected) information systems. The CSW replaces and adds to the Dutch Data Processing and Cybersecurity Notification Obligation Act [Wet gegevensverwerking en meldplicht cybersecurity, WGMC] already in effect, which among other things stipulates that the NCSC is tasked with providing advice on cybersecurity to central government and providers of critical services. This Act also provides the opportunity to inform a relevant Minister in those cases where a government body or provider of critical services does not deal with the recommendations from the NCSC adequately. The Dutch government expects all organisations to be able to respond appropriately when the continuity of their services is at risk. It is also important that outdated software and hardware is replaced in good time (legacy issues).

To ensure effective and unhindered data exchange, the software and protocols for worldwide exchange of data also require attention and maintenance. This often involves what is known as open source software which is usually developed by communities of volunteers. As a result, they often lack the capabilities or resources for maintenance and/or professional review of the quality of the software. Other software developers also use open source software as building blocks for their work, further increasing the dependence on this software.
The quality of paid software and the security of hardware components is equally important to the effective and unhindered exchange of data. This is addressed in

8 The Cybersecurity Act stems from the EU Directive on Security of Network and Information Systems (NIS Directive) and was submitted to the House of Representatives in February 2018.

Ambition 3. Some popular protocols for data exchange via the internet are decades old and are no longer resistant to contemporary attacks. Improved versions of old internet standards (such as IPv6, or HTTPS) are being adopted very slowly and as a result the drawbacks of the old versions (IPv4 and HTTP) will continue to be an issue for some time.

Businesses and public authorities depend on other organisations for their data processing, including cloud providers and their customers, public authorities who make open data available and certificate providers who guarantee the integrity of data exchange. The Dutch government aims to make important (chain) interdependencies between organisations transparent but realises that it is not feasible to have a full grasp of these at all times. The Dutch government is therefore calling for all organisations to be able to respond appropriately when the continuity of their services is at risk. The Digital Trust Center, currently in development, aims to help parties in this regard by raising awareness and offering perspectives for action. The center will do this in consultation with the NCSC and various other parties, including small and medium businesses. Where organisations want to use the services of cybersecurity service providers, it is important that also they deal with computer networks and sensitive information in a professional manner and with integrity. Many Dutch organisation are dependent on a limited number of foreign digital infrastructure service providers, which means that the impact of disruption is severe.

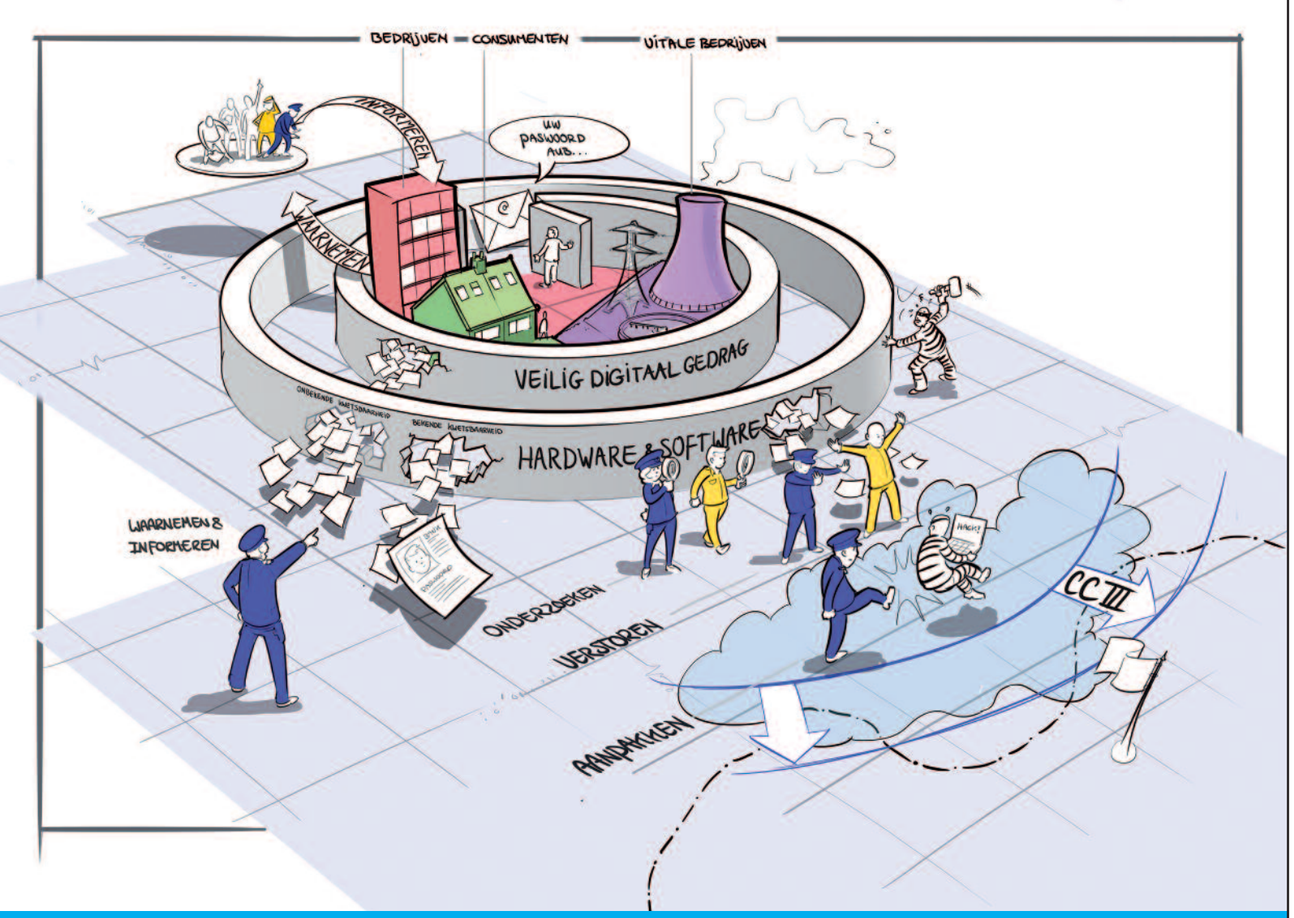
Example: *Heartbleed*
Heartbleed was a vulnerability in the OpenSSL programming library, which was discovered in 2014. At the time, the vulnerability had already been present in this commonly used software for two years. Many web servers, VPN servers, mail servers and other applications use OpenSSL to establish secure connections. Other devices can also use OpenSSL. Examples include *appliances*, routers, WiFi *access points* and some applications on *client* systems. By exploiting Heartbleed, attackers could read the internal memory of systems remotely. This example underlines the fact that a vulnerability in open source software can have major consequences for the cybersecurity of the business community, public authorities and citizens.

OBJECTIVES

- All relevant parties will be involved in ensuring the continuity and digital resilience of critical processes which increases the resilience of the entire chain.
- The Netherlands aims to improve the quality of open source software and the accelerated adoption of modern internet protocols and internet standards.
- The Dutch government promotes an innovative cybersecurity climate in which secure ICT products and services are developed and adopted.

MEASURES

- In addition to existing obligations for telecommunications providers under the Telecommunications Act, the proposal for the Cybersecurity Act greatly increases the number of providers of critical services subject to duty of care requirements and an obligation for notification. Sectoral supervisory bodies will supervise cybersecurity in sectors in critical infrastructure, which was not done up to now, and they will be given the instruments to do so.
- In addition to the above, these supervisory bodies, together with the responsible ministries, will develop a method for identifying dependency relationships of providers of critical services for their own data-driven operating processes.
- Research will be conducted into whether additional (European or international) measures are needed to mitigate the impact of disruption of the services of a limited number of foreign providers of digital infrastructure upon which many Dutch organisations depend.
- Open source software fulfils a central role in the exchange of data between organisations. The Ministry of Economic Affairs and Climate Policy, in close cooperation with the NCSC, will review how the communities that develop and maintain open source software can be supported to improve the quality of the software.
- The government ensures that suppliers incorporate modern internet protocols and internet standards in their products and services, in part through agenda-setting in Europe.
- The government, as a *launching customer*, uses cybersecurity requirements when procuring ICT products and services and strongly advices providers of critical services on this matter.
- Together with private parties the development of a certification system for cybersecurity providers will be explored so that public authorities and private parties know who they can acquire secure services from.



The Netherlands has successful barriers against cybercrime

5. Successful barriers against cybercrime

EXAMINATION OF THE PROBLEM

Criminals pursue their activities on a large scale via the Internet: one in nine people were victim of cybercrime in 2017. The term cybercrime covers a broad range of criminal actions, from classic crime in digital form to new crime. This involves, for instance, hacking computers to transfer money to criminal bank accounts or turning on cameras and microphones undetected to be able to spy on people in their own surroundings. Professional criminals primarily target private organisations and citizens to steal data which can then be sold-on or published.

Threats to national security within the framework of cybersecurity are often criminal acts targeting digital infrastructure and the devices connected to it. The approach to these crimes primarily focuses on new crime, or cybercrime in a strict sense. The approach to cybercrime focuses on the prevention and combating of crimes and on limiting the number of victims, perpetrators and recidivism rates. This concerns both hightech crime and common crime. Digital investigation is also important in more classical crimes in which the internet is a tool, such as the drugs trade and fraud. These types of crime are outside the scope of this strategy.

The efforts to strengthen cybersecurity and tackle cybercrime are implemented in conjunction with each other, and nowhere more explicitly so than in the field of preventive measures.

Secure hardware and software is an important barrier in the prevention of digital threats. When this hardware and software is exploited because of vulnerabilities, it encourages cybercrime. Security of this software and hardware is extremely important and this will have to be developed together with the providers of hardware and software. This is set out in greater detail in Ambition 3 of the NCSA. This applies in equal measure to the secure use of hardware and software by citizens and businesses. This is also set out in Ambition 6.

In addition to this, the National High Tech Crime Unit (Dutch National Police) and the Public Prosecution Service's National Unit have gained considerable experience in countering advanced threats to national security in recent years. The knowledge and expertise they have gained will be used in the approach to cybercrime. Cybercriminals keep on developing their methods. The powers of the Police and the Ministry of Justice must keep in step.

OBJECTIVES

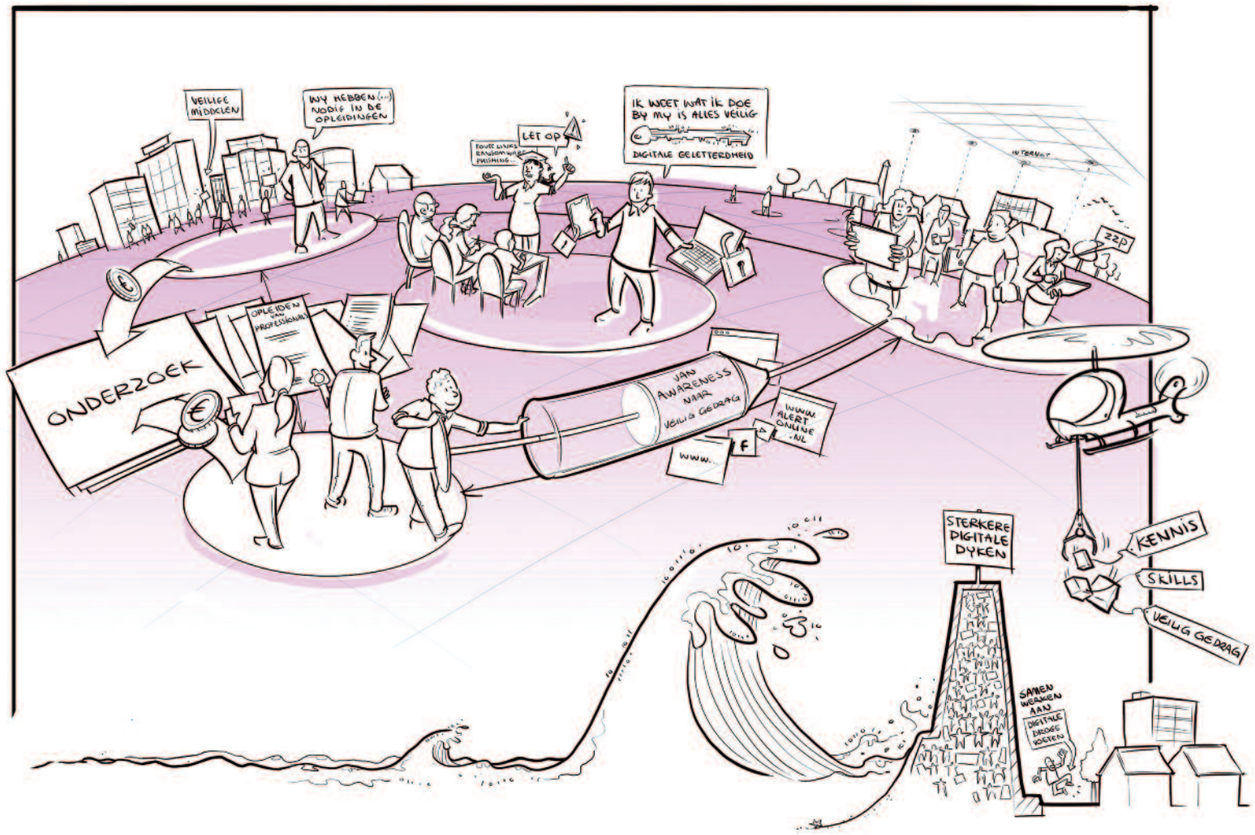
- There are effective barriers that resist cybercriminals.
- The efforts to strengthen cybersecurity and tackle cybercrime are implemented in conjunction with each other. Cooperation between public authorities and the business community, citizens and civil society organisations is extremely important in this respect.
- For cybersecurity, it is important that investigative powers keep step with the developments in the working methods of cybercriminals so that threats to national security can be addressed.

MEASURES

o Following acceptance by the Dutch Senate, Computer Crime Act III will be implemented expeditiously. This will strengthen the Police and the Ministry of Justice's capabilities to investigate digital attacks by criminals, on critical sectors for instance. The Act will be evaluated two years after coming into effect.

- Proposals will be developed to make citizens and businesses more digitally skilled so that there are fewer opportunities for cybercrime. Please also see the objectives and measures in Ambition 6.
- The use of secure hardware and software is encouraged to prevent *cybercrime*. Please also see the objectives and measures in Ambition 3.

Integrale aanpak *cybercrime*
Investigating cybercriminals and disrupting their revenue model contributes to cybersecurity. The current approach to *cybercrime* focuses on investigating, prosecuting and disrupting crimes, prevention, and strengthening laws and regulations. This approach will be continued and intensified. In addition, new elements are being added, such as preventative measures for potential perpetrators and victims, a possibly different form of support for victims, an approach to perpetrators to prevent recidivism and knowledge development for policy-making in the longer term.



The Netherlands leads the way in the field of cybersecurity knowledge development

6. Cybersecurity knowledge development

Knowledge is an extremely important asset in the Netherlands. Dutch society, and digital security in particular, depends on the development and use of knowledge, which is why ambitions in the field of knowledge development are essential in the NCSA.

There is an urgent need to maintain and deepen high-quality cybersecurity knowledge development in the Netherlands. Intensifying sufficient and high-quality development of both fundamental and applied cybersecurity research is crucial in this regard. Cybersecurity knowledge development is needed to be able to implement measures to avert existing and new digital threats. Moreover, high-quality autonomous knowledge helps to avoid over-reliance on cybersecurity expertise and cybersecurity solutions from other countries. Cybersecurity knowledge development does not only apply to natural sciences, but to arts and humanities and social sciences as well. It concerns both monodisciplinary and interdisciplinary research into short and long term solutions. When doing so, it is extremely important for such research to cover the entire knowledge chain.

Cybersecurity research in the Netherlands is of a high standard. Numerous parties, such as universities, universities of applied sciences, the Netherlands Organisation for Scientific Research [*Nederlands Organisatie voor Wetenschappelijk Onderzoek, NWO*], businesses and central government, are investing in this research. Successive editions of the National Cyber Security Research Agenda (NCSRA) have formed an important framework for cybersecurity in recent years. As a result of investments in cybersecurity research in neighbouring countries, a multi-year boost for cybersecurity research is needed in the Netherlands to maintain talent, and thereby our own knowledge position in the area of cybersecurity.

In addition, there is a growing demand from the business community and public authorities for innovative solutions to cybersecurity issues and well-trained personnel. This shortage on the labour market leads to scarce cybersecurity knowledge in organisations, which makes them insufficiently resilient to digital threats.

It is equally important that citizens and businesses also continue to develop their knowledge to protect themselves against digital threats. In addition to its task in the field of cybersecurity research, Dcypher[9] (set up by the Ministry of Justice and Security, Ministry of Education, Culture and Science, and the Netherlands Organisation for Scientific Research [*Nederlands Organisatie voor Wetenschappelijk Onderzoek, NWO*] in 2016) was also given a task in the field of cybersecurity higher education. It has charted the field of higher education in the Netherlands, which has facilitated mutual comparisons of degree programmes and the assessment of the skills of recent graduates who are entering the labour market. A next essential step, is an analysis of the differences between the curricula (supply) and the requirements for well-trained personnel (demand). European cooperation in this field is being pursued. Sufficient teaching capacity (in all disciplines concerned) requires further attention.

Digital literacy is now part of the curriculum for primary and secondary education but given the risks to (young)

9 Dcypher is the platform that unites researchers, lecturers, producers, users and policy-makers in the Netherlands to improve knowledge about and expertise in cybersecurity.

children there is a need for the educational field to continuously renew and anticipate developments. The agreed revision of the curriculum (where digital literacy is one of the themes) is being pushed forward together with teachers, pupils and parents, educational institutions and the professional field. This revision of the curriculum will become law from 2019 onward.

There is still a need for current generations to catch up. Research[10] has revealed that citizens and businesses are still not sufficiently aware of the dangers of digital activities and the measures that they can implement to avoid becoming a victim in the digital domain. In recent years the business community and the government have already invested heavily in the awareness of the general public and smaller businesses to digital threats and perspectives for action have been offered, amongst others through veiliginternetten.nl and Alert Online but also through campaigns such as maakhetzeniettemakkelijk.nl (*'boefproof'*) [don't make it easy for them ('crook proof'] or *veiligbankieren.nl* (*'hang op, klik weg'*) [safebanking.nl. (hang up, click away]. The effects of these various efforts can be improved by more public-private cooperation and by introducing cohesion into communications campaigns in the public domain. This also applies to the efforts by employers to make their employees digitally skilled and keep them up-to-date. When doing so, there is a need to develop a guide containing basic security measures for both citizens and smaller businesses. This set of security measures does not protect against all conceivable digital threats but is an important step that citizens and small businesses can take to further develop their digital skills.

OBJECTIVES

- The Netherlands conducts high-quality cybersecurity research.
- The Netherlands has a long-term knowledge development programme under which the academic community develops and improves high-quality knowledge, and there are sufficient academics available to acquire an independent knowledge position in the area of cybersecurity.
- Citizens and businesses are able to see the importance of addressing digital threats and become more resilient to *cybercrime*.

MEASURES

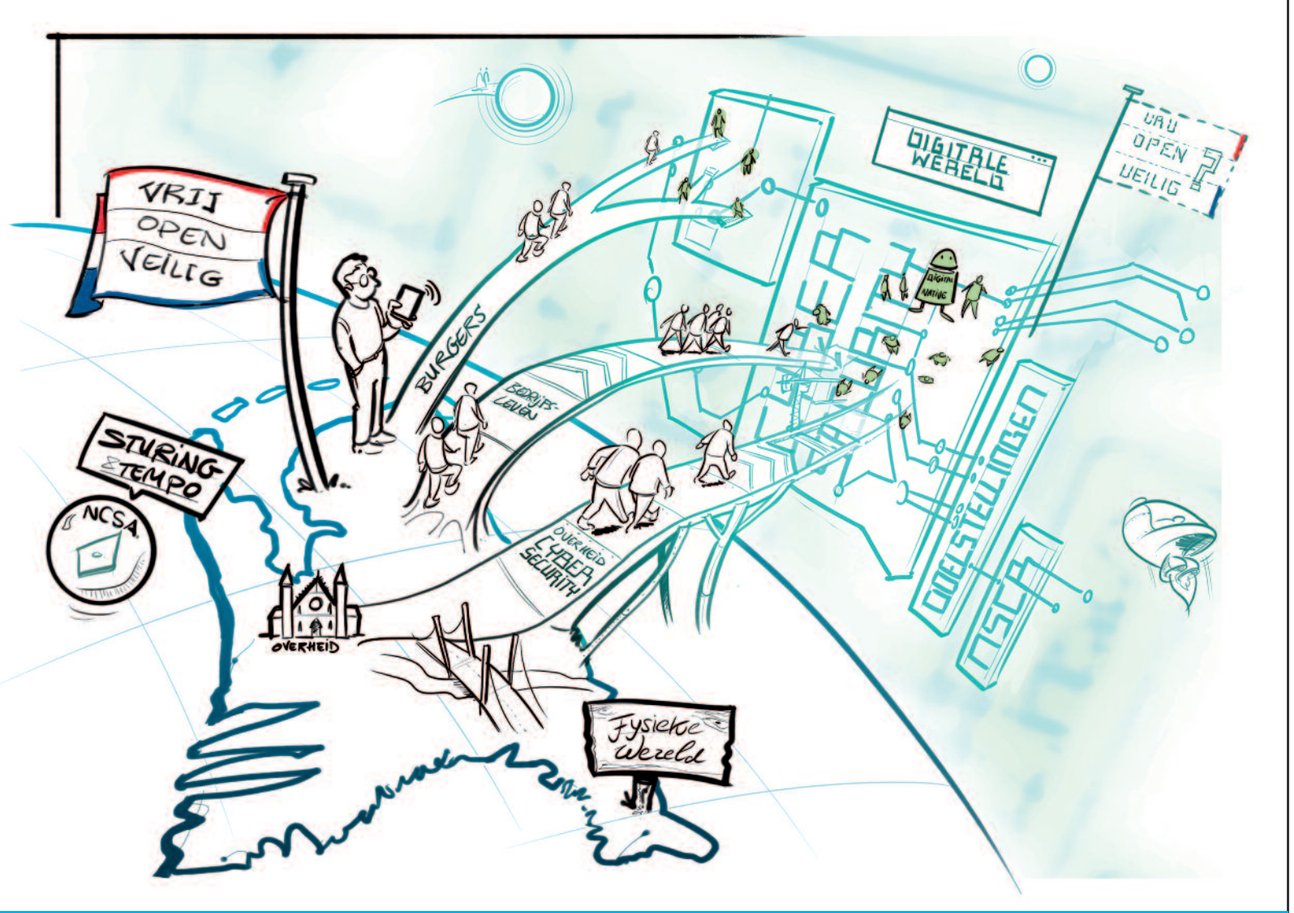
o The Netherlands will invest structurally in fundamental and applied cybersecurity research. This will take the form of a multi-year public-private approach, as a boost for high quality cybersecurity knowledge development. The way in which various initiatives, programmes and instruments relating to cybersecurity research can be better aligned with each other will be investigated to this end. The Verhoeven/Rutte[11] motion will be included in this. In anticipation of this investigation, a financial incentive for cybersecurity research will be organised first.

o Digital skills, including media-literacy and cybersecurity are explicit focus areas in the integral review of the primary and secondary education curriculum. Proposals for this will be developed in 2018 and will be evolved into laws and regulations from 2019 onwards. Schools will be supported by Knowledge Net [Kennisnet] (which is funded by the Ministry of Education, Culture and Science) in anticipation of this.

o The government encourages the business community and civil society organisations to further develop the digital skills of employees and citizens and ensures the continuity and cohesion between various awareness campaigns to increase their effect. When doing so, the latest insight in behavioural sciences wil be taken into account.

10 National Cybersecurity Awareness study 2017 [Nationaal cybersecurity bewustzijnsonderzoek 2017], Alert Online and HM Government et. al. A call to action: The Cyber Aware perception gap, 2018.

11 The Verhoeven/Rutte motion asks the government to explore the possibility of setting up an institute for research in the field of cybersecurity (Parliamentary Papers II, 2017/18, 34 775 VI, No. 68).



The Netherlands has an integrated and strong public-private approach to cybersecurity

7. Public-private approach to cybersecurity

In recent years, the public, private and public-private sectors have taken various initiatives to improve cybersecurity in the Netherlands. The course and speed of the approach needs to be coordinated to safeguard that direction. Coordination can and must be stronger and that, of course, is up to the government. As the coordinator, the NCTV takes the lead in promoting and ensuring the improvement of cybersecurity in a cohesive manner, in conjunction with all the parties involved (public authorities, business community, science, civil society). However, the government cannot do this on its own. All parties may and must be expected to accept their responsibilities and contribute to make and keep the Netherlands digitally secure as part of a concerted effort. The approach can only be successful if it is designed, further developed and evaluated in close public-private cooperation. The increasing complexity and breadth of the cyber domain require continuous clarification of the roles and responsibilities of the various parties involved. This should also help to identify successful market initiatives and link them to this Agenda. For instance, cybersecurity is included in the *Corporate Governance Code* and as such is a topic during audits and reviews. And on the private side, there is also a need for more cohesive efforts in the integrated Dutch approach to cybersecurity.

The importance of information security and cybersecurity to public authorities is growing, because citizens and businesses are increasingly using their services from public authorities digitally. Failure, sabotage to or disruption of digital services will therefore directly lead to damage to critical service provision processes. To optimise the digital services provided to citizens and businesses by the government and to be able to guarantee high-quality services, it is essential for public authorities to keep investing in information security and cybersecurity and to prioritise the availability and continuity of services. In addition to services, digitalisation also has an impact on public values and human rights and ensuring them in the information society. In addition to the secure provision of services to citizens and businesses, the government also needs to have and keep its own information security in order and be resilient to digital attacks. The Broad Agenda for Digital Government (Ministry of the Interior and Kingdom Relations, BZK) discusses these topics in greater detail, as well as the measures the government will take, at an inter-governmental level, to step up its efforts on information security and cybersecurity.

OBJECTIVES

- The coordinating role of the government in the integrated approach to cybersecurity will be strengthened.
- Dutch businesses, citizens and government organisations implement their responsibilities, rights and obligations with regard to cybersecurity.
- For the information security of the digital government, there is a coherent package of measures to enhance the information security for the digital basic infrastructure, to further standardise and harmonise frameworks of norms on information security, including the creation and implementation of a Government Information Security Baseline [*Baseline Informatiebeveiliging Overheid*]. In this regard, attention will be paid to reducing administrative burdens on municipalities for information security and to bundling audits and assessments in a single

chain of accountability. Amongst other measures, information security and cybersecurity will be embedded in the Digital Government Act [*Wet Digitale Overheid*].

MEASURES

- The strengthened coordination of the integrated approach is the responsibility of the NCTV.
- A cybersecurity alliance will be formed which commits public and private parties to implement the measures from the NCSA.
- Progress of the approach to cybersecurity will be monitored under the coordination of the NCTV and in cooperation with all parties involved, and where necessary will be recalibrated based on technological and social developments. There will be an integral evaluation of the Agenda in 2021.
- Cooperation between public authorities and the business community will be reinforced by creating a nationwide network of cybersecurity partnerships. The principle of big businesses helping small businesses will be part of the framework. There is scope for different modalities in public-private cooperation.
- A coherent package of measures for information security and cybersecurity in public administration will be addressed in the Broad Agenda for Digital Government. These measures will be coordinated from the Government-wide Digital Government Policy Forum [*Overheidsbrede Beleidsoverleg Digitale Overheid, OBDO*].

This publication was issued by the NCTV on behalf of central government.

info@nctv.minvenj.nl