Netherlands Cybersecurity Strategy 2022-2028

Ambitions and actions for a digitally secure society

Cover photo: Nowadays we are online more than ever. In 2021 there were no fewer than 17 million mobile connections in the Netherlands. Almost 96% of these connections was for a smartphone, 90% of which were also used to access the internet. Over 15 million people have one or more social media accounts.

The Netherlands Cybersecurity Strategy (NLCS) is the result of a broad partnership between public, private and civil society organisations, coordinated by the National Coordinator for Counterterrorism and Security (NCTV). The pillars and aims set out in the Strategy are based on the Cybersecurity Threat Assessment for the Netherlands (CSBN)

Foreword

The internet has changed our lives dramatically. We live and work online. In many respects this makes our lives easier, and the economic advantages are obvious. It's important that companies and the public can enjoy the full benefit of our digital society and economy, and for that, security is vital.

Security in the digital world, however, still lags far behind that in the physical world. Anyone buying a car knows that it meets all kinds of safety and quality requirements. And the buyer knows exactly what they are expected to do in order to drive the vehicle: hold a valid driving licence, refrain from drinking alcohol and undergo an annual vehicle test.

Things are very different in the digital world. In the design of many digital systems, security is still not the main priority. For decades, responsibility for that security has rested with end users, such as individual consumers and small businesses and organisations. But many of those end users are in practice completely unable to meet that responsibility. They do not know, for example, how to update a Wi-Fi router, and they struggle with system security, privacy requirements, and so on.

Meanwhile, the risks keep growing. As a highly developed society, the Netherlands is rapidly becoming more and more dependent on digital systems. But even in more mature organisations, tech companies and government organisations, system security depends on the actions of individuals. Whole systems may go down if one employee opens a phishing email or fails to install the right security.

The government believes that the one-sided focus on individual responsibility is a dead-end street, and has chosen to take a different route to a digitally secure ecosystem. On behalf of the government I am therefore presenting a new cybersecurity strategy which contains the following priorities:

1. **Understanding the threat.** The government will invest in people and systems that provide a clearer picture of the origin of threats and whom they are directed at.

2. **More cybersecurity specialists.** We will take various measures to bring more ICT specialists to the labour market.

3. **Government and sectors taking responsibility.** Responsibility for security will be transferred in part from end users to the government and specific sectors. The most mature and most key organisations will bear the greatest responsibilities. Robust government-wide statutory security requirements will be arranged, together with compliance monitoring.

4. **Better supervision and the necessary legislation.** Reorganising responsibilities requires an expansion of statutory rules and supervision. Security must become the basis on which new systems are founded. New rules will be introduced for central and subnational government authorities, critical providers and suppliers of digital products and services.

5. **Clear information via a national cyber authority.** A new central cyber authority will be established in the Netherlands: the national Cybersecurity Incident Response Team. This new organisation will collaborate with public and private partners to provide critical and non-critical organisations, government authorities and the public with information relating to cyber incidents (or potential incidents) to enable them to protect themselves.

This strategy sets out the government's ambitions for the next six years. In the first phase, we will be investing heavily in the General Intelligence and Security Service (AIVD) and the Defence Intelligence and Security Service (MIVD), in the National Cyber Security Centre (NCSC) and in reinforcing the Netherlands' nationwide network of cybersecurity partnerships (LDS) that provide organisations with security advice, and in strengthening the cyber resilience of specific sectors.

This is a shared responsibility of all parties in the cyber domain, and one that requires targeted public-private cooperation. I am therefore most grateful to all the public bodies, private parties and academic institutions – especially the members of the Cyber Security Council – that contributed to the development of this strategy. Keep up the good work as we move forward with implementation!

Dilan Yeşilgöz-Zegerius, Minister of Justice and Security

Table of contents

Increasing digitalisation provides the world of education with many opportunities, such as offering online lectures and unlocking vast reserves of knowledge. At the same time, this increased dependence on technology entails risks. In recent years, various universities have been the targets of ransomware attacks.

Introduction and context

In producing the Netherlands Cybersecurity Strategy (NLCS), the government's aim is to achieve a digitally secure Netherlands. That will enable us as a country to capitalise safely on the economic and social opportunities presented by digitalisation and, at the same time, to safeguard our security and public values. The Netherlands is one of the most digitally advanced countries in the world. Increasingly, we are working, shopping and meeting each other online. Digital systems now form the 'central nervous system' of our society. That presents society with countless opportunities, but it also poses risks.

Recent history has shown that cyber incidents, such as ransomware attacks, are now commonplace occurrences. As a result, cybersecurity is now largely perceived from the point of view of the threat, and thus in terms of risks. Which hackers need to be stopped? What vulnerabilities need to be patched? How can information about cyber threats be shared more quickly and more efficiently? How can organised cybercrime, such as ransomware attacks, be tackled effectively? How can potential victims be notified in time (provided the necessary information is available)? These are just some of the many relevant challenges which need to be overcome and which form part of this strategy.

We must not forget, however, that the ultimate objective is to safeguard our public values. We want to create an open, free, stable and secure digital world in which companies and individuals can participate as securely as in the physical world. Cybersecurity is an investment in our future and must not simply be regarded as an expense. To achieve this, we must realise that each element of the digital ecosystem, be it specific technology, an organisation, an information system, a digital product or a person, forms part of a globally interconnected network. The cybersecurity of all those individual elements contributes to the digital resilience of the system as a whole.

This is the great challenge for the coming years. The digital ecosystem is now so interconnected and complex that it is extremely difficult, if not impossible, for individual organisations and people to fathom it completely, while it is precisely this ecosystem that powers our modern way of life, our economy and society as a whole. Criminals and malicious states take advantage of this complexity by lurking in the shadows and exploiting digital vulnerabilities to attack our public values.

Against this backdrop, the government observes that the increased importance and complexity of the digital ecosystem are no longer commensurate with the autonomous way in which the cyber landscape has evolved in recent years. The ecosystem therefore needs to be adapted to the new reality. In the current system, a single phishing email or lost password can have a huge impact. This is because part of the responsibility for risk management for an entire ecosystem, including critical sectors and processes, lies with the least digitally mature participants: individuals, small businesses and local authorities. Many of the more mature organisations, tech companies and government organisations are working towards a more secure and stable internet, but at the same time implicitly assume that individuals are capable of deciding what security they should install and know how to use a password manager. It goes without saying that cyber hygiene is and will remain an essential issue for everyone, but from a systemic perspective this will not be enough to guarantee the continued resilience of our digital interests. The government has a duty to ensure that the ecosystem contributes to and serves our public values, and meets the cybersecurity requirements within it.

Many digital systems, services and processes were not designed on the basis of cybersecurity and risk management (i.e. on the basis of security by design and security by default). This means that end users are responsible for keeping our systems digitally secure. In other sectors, ecosystems have evolved over the years into a balanced composition of instruments, such as statutory security requirements, certifications, warranties and mandatory training. Similar structures will eventually be created for the cybersecurity of digital products and services too.

The government is therefore committed to strengthening and transforming the digital ecosystem so that no single organisation or individual can be the weakest link any more. This requires a reorganisation of the responsibilities of all players in the ecosystem, so that the relevant rights and obligations are allocated to the right parties. To achieve this, we need to deploy a well-balanced combination of instruments, from more intensive public-private partnerships to new legislation, designed to create an ecosystem in which businesses and the public can in principle purchase secure products and services.

In the context of the European digital single market and the pursuit of a level playing field and secure internet-of-things products and services, the government is concentrating its efforts on the development of European legislation. Various legal measures have now been taken and initiatives launched to make this happen.

We will eventually need to arrive at a situation in which every party involved in the digital ecosystem has a clear understanding of their contribution to the security and stability of the whole. This requires a system transformation. No single party can do this alone, not even the government. It will be a joint effort in which all parties contribute to the transformation. And that will require obligations and commitments. Cybersecurity will always be a responsibility shared among those who build our digital infrastructure, those who manage it and those who use it. This requires collaboration as well as robust coordination to achieve cohesion of effort and ensure that those efforts ultimately amount to more than the sum of their parts.

In this strategy, the government sets out its vision of a digitally secure Netherlands, where companies and the public can benefit fully from participation in the digital society, without having to worry about cyber risks. That is the ultimate goal. For some themes, achieving this vision will span multiple government terms or even remain an ongoing pursuit. The government will use the strategic aims and the action plan to set out how it will advance the achievement of this vision over the coming years. Phasing, prioritisation and decision-making will be necessary, as achieving a digitally secure Netherlands will take years. Not all ambitions will be realised in the short or medium term. In cases where additional resources are required, the government will opt at this stage for structural investment in the AIVD and the MIVD with a view to getting a better handle on the threat. Resources will also be made available to boost the Nationwide Network of Cybersecurity Partnerships, partly through the further development of the NCSC into a national CSIRT, and partly through the centralisation of government organisations in the chain wherever possible and in the public interest. Lastly, resources will be provided for ministries with major sectoral challenges to enable them to boost cyber resilience in the sectors concerned. Generally speaking, there is sufficient funding for the implementation of the actions set out in the action plan. If, however, there is a need for follow-up steps or supplementary processes, legislative or otherwise, as a result of the actions, additional resources will need to be found. The appendices contain a more detailed explanation of the financial basis for this strategy.

This strategy will also show what can be expected from the government in concrete terms, as well as what it is accountable for.

Cooperation in the cybersecurity domain

The strategy has been produced with the extensive involvement of many public, private and civil society organisations, and builds on previous government-wide cybersecurity strategies published in 2011, 2013 and 2018. All ministries are working together and with public and private partners to set out and implement the strategy. The Minister of Justice and Security is the coordinating minister for cybersecurity, is responsible for tackling cybercrime, and is in charge of implementing this strategy and monitoring the process. However, each party retains its own tasks and responsibilities for achieving the cybersecurity goals. Lastly, the strategy is closely aligned with the government's efforts in the area of digitalisation, which are led by the State Secretary for Kingdom Relations and Digitalisation, as set out in the framework letter of 8 March 2022 on this subject.[1]

Cybersecurity: the full spectrum of measures designed to reduce relevant cyber risks to an acceptable level. This also includes dealing with risks of damage to or failure of digital systems and the availability, integrity and confidentiality of data. Measures may focus on the prevention of cyber incidents and – if a cyber incident does occur – on detection, damage limitation and recovery. What constitutes an acceptable level of risk will be determined in a risk assessment.[2]

Cyber resilience: the ability to reduce relevant risks to an acceptable level by means of a set of measures to prevent cyber incidents and, if they do occur, to detect them, limit the damage and facilitate recovery. What constitutes an acceptable level of resilience is determined by a risk assessment. This can help with the selection of the right technical, procedural or organisational measures.[3]

Cybercrime prevention: efforts to prevent crime in which a computer system is attacked or misused for the purpose of criminal activity. Cybercrime prevention is an integral part of the cybersecurity approach.

The Port of Rotterdam has one of the Netherlands' most advanced ICT systems, comprising a dedicated infrastructure designed to connect terminals, depots and distribution centres. This makes it possible to see exactly where a container is located at any given time. But it also creates a great deal of interdependence. This became all too clear in 2019, when a hacker attack on shipping giant Maersk's systems completely paralysed all container transport.

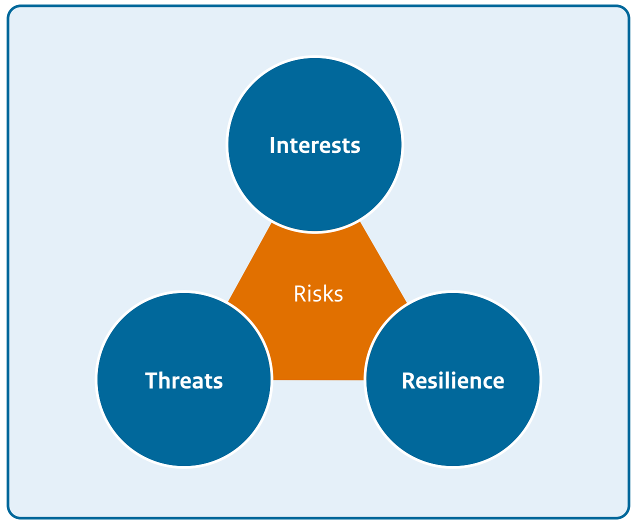
1. National cybersecurity task

This chapter gives an overview of current and future challenges in relation to cybersecurity, which form the basis for the pillars and aims of the Netherlands Cybersecurity Strategy. In order to produce a widely supported strategy, parties with a major cybersecurity role, both within and outside government, were involved at various stages.

Cyber risks have not diminished

Within the broad domain of digitalisation, the central goal is to achieve a secure, inclusive digital society with a wealth of opportunities for all Dutch people. The importance of digital processes is growing because of technological developments and far-reaching digitalisation. For that digital transformation to succeed, cybersecurity is an essential requirement.[4] Digital processes are the central nervous system of society and the economy: they cannot function properly without them. Digital security is thus inextricably linked to six national security interests: territorial security, physical security, economic security, ecological security, social and political stability and the international legal order.[5] An attack on critical processes, such as electricity or drinking water supplies, shipping or financial transactions, could bring society to a temporary or even enduring standstill.

Figure 1: Cyber risks are determined by the relationship between interests, threats to those interests and resilience in the face of such threats



The digital threat is here to stay and is more likely to increase than to diminish, with all the repercussions that entails. The threat could be posed either by a cyberattack or a digital system failure. Such a failure could be the result of natural or technical causes, or the result of human error. State actors and cybercriminals constitute the main threat in terms of malicious actions, and are not always distinguishable from each other because of their interwoven relations. State actors may hire, allow or pressurise cybercriminals to perpetrate cyberattacks on designated targets.[6] Cyberattacks by state actors are no longer unusual.

State actors can use a broad range of digital resources for this purpose: influencing and interference (including the dissemination of disinformation); espionage, including economic and political espionage; preparatory action for attacks and actual disruption and sabotage. According to the AIVD, the threat of offensive cyber programmes against the Netherlands and against Dutch interests remains high and will only increase in the future.[7] Cybercriminals are also still capable of inflicting serious damage on digital processes. They are motivated by money and are not intent on disrupting society, but their attacks can nonetheless have such an impact that they adversely affect national interests. The threat posed by hacktivists is relatively low, but could affect Dutch interests indirectly.

In recent years it has become clear that the level of cyber resilience in the Netherlands is insufficient.[8] Despite efforts to boost resilience, there is a disparity between the growing threat and the development of resilience. Complete imperviousness to cyber threats is impossible, but boosting resilience to system failures and misuse is the most important tool for managing cyber risks. Cyber resilience is not yet at the desired level across the board because basic measures have not been sufficiently implemented. There are major differences in resilience levels within and between sectors and supply chains.

Complications of risk management pose a threat to society

The 2022 Cybersecurity Assessment for the Netherlands (CSBN2022) includes strategic themes which have been identified in collaboration with partners and which are relevant for the Netherlands' digital security, now and in the future:

Risks are the downside of a digital society. Dutch society is highly digitised. That has a downside: reliance on digital processes has made us vulnerable to system failures and to the activities of those with malicious intent. Chain reactions can affect entire sectors or even society as a whole. The disruption of digital processes can also have physical consequences.

Cyberspace is an arena for regional and global dominance. Digital security is closely linked to geopolitics. States are using cyberspace constantly and intensively to promote their own geopolitical interests. Cyberattacks, such as those used to gather political and economic intelligence, are an important instrument in that respect; they are relatively inexpensive and scalable, and they have a significant, often long-term impact. Even the ultimate form of geopolitical conflict – war – involves cyberattacks. Attribution is also a difficult issue. Individuals, organisations, sectors and countries can do little to influence these geopolitical rivalries, even though they serve to heighten the risks.

Cybercrime is industrially scalable, while resilience – for now – is not. Serious, organised cybercrime has become highly scalable and has thus taken on industrial proportions in recent years in terms of victims, damage and criminal proceeds. Ransomware has proved to be a gamechanger in this regard. Serious cybercriminals and their service providers are primarily motivated by money and aim for maximum profit, happily exploiting the opportunities offered by cyberspace. Given the nature and growing scale of the cybercrime threat, the task of making and keeping the chain of resilience scalable will be a fundamental challenge in the years ahead.

Market dynamics complicate cyber risk management. Supply and demand for digital services, hardware (and components), software and networks converge on digital markets. These markets have a number of unique characteristics, such as the semi-monopolistic status of certain suppliers, the high level of interdependence and the focus on gathering as much data as possible. Moreover, incentives for digital security are not always the overriding concern in these markets. These factors complicate risk management for individuals, organisations, sectors and countries alike.

Coordinated and integrated risk management is still in its infancy. Coordinated and integrated risk management within and between the organisational, sectoral and national levels is still in its infancy. Cyber risks have not yet been given a definitive place in broader risk management within and between these levels. Risk management is not yet a given, even though a risk-based approach plays a big role in determining and achieving the desired level of resilience. Of course, many organisations do have the appropriate risk management in place, but in many cases it is not embedded in organisations' primary process.[9]

There is also an overarching theme that affects all the others: ***restrictions in digital autonomy also limit cyber resilience.***[10] European countries, including the Netherlands, are subject to restrictions in digital autonomy. That autonomy includes the Netherlands' ability and means to make independent choices about ongoing digitalisation, as well as the desired level of cyber resilience. This autonomy is restricted by various factors, which relate to the strategic themes referred to above; they limit the options for influencing and making decisions about the country's cyber resilience, and they reduce the country's control over that resilience. Despite their diverse nature, each of these themes, both separately and in association, illustrates the complications for strategic risk management.

Need for an integrated approach to cyber resilience

Over the past few years, various authoritative organisations have issued recommendations to the government on the subject of cybersecurity and on how to boost cyber resilience. These recommendations, in addition to the strategic themes listed above, were taken into account in the creation of this strategy. A wide-ranging group of stakeholders was also asked – by means of a questionnaire and in work sessions[11] – to identify further challenges.[12] This resulted in the following key additional insights which have been incorporated in this strategy.

- There is a growing 'cyber resilience gap' between organisations. Some organisations have their cybersecurity in order, but others do not.
- Demand for cybersecurity expertise is expected to continue rising, leading to a shortfall of qualified personnel.
- It has been observed that responsibilities in the Dutch cybersecurity system are not currently clearly allocated or clearly defined, which obstructs effective cooperation.
- In recent years, information-sharing has been found to be fragmented, and as a result threat information has not always reached all organisations in time to enable them to take the necessary measures.
- Organisations have limited oversight of the risks of and damage resulting from failure of digital systems and there is a lack of data on the scale of damage caused by technical faults or human error.
- The practice of learning from incidents in cyberspace is still in development.
- There is still too little scientific cybersecurity knowledge and innovation reaching the market.
- The development of international norms surrounding cybersecurity is challenging, and the formulation, adoption and implementation of international norms for state responsibility are proceeding slowly.

- Awareness among small organisations and the public of the need to protect themselves against cyber threats is still too limited.

An integrated approach to cybersecurity is required to overcome these challenges.

Looking back on enhancing cyber resilience under the National Cybersecurity Agenda (NCSA)

- The Network and Information Systems (Security) Act (WBNI) came into force in 2018. Among other things, it provides that operators of essential services and digital service providers are obliged to take appropriate and proportionate technical and organisational measures in relation to cybersecurity.

- The Digital Trust Centre (DTC) was also set up in 2018 so that non-critical companies too had a point of contact for cybersecurity issues. The DTC provides information and advice and encourages the establishment of cybersecurity partnerships.

- With the bill on promoting cybersecurity in the business sector and the establishment of an information service, the DTC made a start on receiving and sharing information about digital threats and risks with companies.

- The Civil Service Strategic Information Agenda 2019-2021 focused on strengthening the government-wide information-security pillar.

- Setting up and strengthening a nationwide system of cybersecurity partnerships (LDS) will allow information to be shared ever more widely, efficiently and effectively between organisations resulting in better provision of information to their target groups.

- In 2020 the Cyber Intel/Info Cell (CIIC) was established. This is a body in which the AIVD, the MIVD, the NCSC, the Public Prosecution Service and the National Police assemble threat information, and staff from these organisations evaluate the information jointly. This makes it possible to both form a picture of new threats and offer organisations potential courses of action more rapidly.

- The National Detection Network has been expanded in recent years, enabling steps to be taken in the detection and monitoring of threats within central government and critical infrastructure.

- The new dcypher platform was officially launched in 2021. Dcypher is the place where public, private and knowledge-based stakeholders, resources and expertise converge to ensure effective engagement in cybersecurity education, research, innovation and concrete applications.

The end of the Dutch public transport smart card is in sight. Soon it will be possible to check in with your debit or credit card or smartphone when boarding a train, bus or tram, which should make both travel and payments more convenient. An innovation of this scale is quite an undertaking: more than 60,000 entry gates and card readers need to be modified.

2. The vision: digital security is a given – for everyone

The vision underlying the strategy describes what a digitally secure Netherlands should look like in the future. That is our ultimate goal.

Vision

In the future, society will be fully digitised: our way of life is already closely interwoven with cyberspace. The risk of abuses, such as those perpetrated by state or criminal actors, or of process failures, form the downside of this digital society. Cyber resilience, including combating cybercrime, is essential for society and the economy to function. It is not simply a cost; it is a profitable investment. Cyber resilience offers competitive advantages and boosts the investment climate, innovation and employment.

By producing this strategy, the government is working towards a future in which the imbalance between the cyber threat and cyber resilience is kept to a minimum. In this vision of the future, cybersecurity is at a level commensurate with the threat and with the importance of ensuring the continuity, integrity and reliability of digital systems and processes. Cyber threats will also be identified and dealt with. Lastly, society will be resilient: there will be sufficient redundancy and recovery capability to absorb the repercussions of cyber threats, such as a system failure.

Underlying strategic choices

1. **In respect of the Nationwide Network of Cybersecurity Partnerships:**
   a. There will be a single national CSIRT, which will incorporate the NCSC, DTC and CSIRT-DSP. This will be the central cyber authority of the Netherlands.[13]
   b. The government will lead and coordinate this process. That means centralised where possible, decentralised/sectoral where necessary.
   c. More coordination of development of the nationwide network on the basis of added value and desired effect;
   d. The government will collaborate and operate decisively. Up-to-date knowledge and information about cyber threats, incidents, trends and vulnerabilities must be made available to partners in the nationwide network (LDS) to enable them to take action. The government will take the lead in this regard.
   e. Information-sharing will be based on possible courses of action. There will be differentiation in advice and information and information-sharing, appropriate to organisations' level of maturity and in comprehensible language.
   f. 'Large helps small': nationwide network partners are responsible for supplying and picking up information and thus can help boost resilience within their respective chains and sectors.
   g. There are clear points of contact within the nationwide network, and solutions for gaps relating to the points above will be sought with private parties.

2. **It should be possible to alert anyone in the Netherlands who is a (potential) victim or target of a cyberattack.**

3. **In respect of legislation:**
   a. European legislation where possible, supplementary national legislation where necessary.
   b. New legislation will form the framework in which the system can operate effectively and coherently.
   c. Regulate market failures in relation to security through legislation.
   d. Cybersecurity measures and requirements are proportionate and are differentiated according to the interest a company represents and its level of maturity. Life will be made as easy as possible for SMEs.
   e. Robust, government-wide statutory security requirements and compliance monitoring will be arranged.

4. **In respect of collaboration:**
   a. Public-private where possible, public where necessary.
   b. No more commitment-free partnerships. Collaboration is voluntary but not free of obligation.
   c. 'Large helps small' – the strongest/most mature organisations help the less strong/mature organisations (public-public, public-private and private-private).

5. **In respect of knowledge and innovation:**
   a. Through the collaboration platform dcypher and via thematic roadmaps and communities, the government will foster discussions between knowledge institutions and the business community regarding the high-end knowledge development needed to generate innovative knowledge and product development. Dcypher can play a facilitating and driving role in the quest for funding for that development.

6. **In respect of countering cyber threats posed by state actors and criminals:**
   a. The underlying strategic choice with regard to tackling cybercrime consists of two elements: efforts involving the investigation, prosecution and disruption of cybercriminals, and efforts involving the prevention of cybercrime.[14]

7. **Cyber risks for members of the public** will be minimised by largely removing responsibilities for the security of digital products and services from small and medium-sized enterprises (SMEs) and individuals, and placing them with government, manufacturers and service suppliers. Members of the public and SMEs will thus be relieved of this burden.

8. **The government** will use objective criteria to manage the distribution of scarce cybersecurity and ICT expertise in a crisis, as part of the National Crisis Plan for Digital Incidents.

Public values are key
In cyberspace, public values and fundamental rights need to be safeguarded at all times. This includes responsible use of data and responsible behaviour in the digital domain by government organisations. When exercising powers in the interests of national and international digital security, careful consideration must always be given to the balance between collective security on the one hand and individual fundamental rights and public values on the other. Statutory requirements, such as proportionality and subsidiarity, must take precedence when it comes to guaranteeing public values such as privacy, security and non-discrimination.

Role and responsibility of central government
People should be able to expect the same security in cyberspace as in the physical domain. Cyber risks for members of the public will be minimised by largely removing responsibilities for the security of digital products and services from individuals and placing them with suppliers and manufacturers.

People should also be able to count on reliable service provision by companies and public authorities in cyberspace. Central government is responsible for creating a system in which organisations can take appropriate measures to strengthen their cyber resilience and thus guarantee the continuity and reliability of their services. Central government does this by raising awareness, providing information and giving clear and consistent advice on risk management, implementing resilience measures, preparing for incidents and, if necessary, providing support. The level of intervention is determined by the risk to which organisations are exposed, by the organisation's level of maturity and by the impact such support would have. The assessment will be clear and transparent.

Central government also encourages and helps companies and other organisations to make the same assessment vis-à-vis their own target groups, including consumers. Partnerships, organisations and public authorities exchange information within the Nationwide Network of Cybersecurity Partnerships so that they can all provide customised services for their own target groups. To avoid fragmentation and save time, a single national CSIRT has been established, through which information can be channelled straight to vulnerable or at-risk organisations wherever possible. Operational expertise is pooled within central government and deployed jointly wherever possible. In the future, cybersecurity experts from government will work with the business community and ICT and cybersecurity service providers, in some cases at the same physical location. This will enable them to pool information, knowledge and expertise in order to safeguard cyber resilience and ensure a common strategy for – and response to – cyber incidents or threats.

Central government provides the framework in which the system can function effectively and coherently. To this end, it deploys a well-balanced combination of instruments, such as legislation (national and EU), financial support or incentives (tax advantages, subsidies), skills training, etc. It also serves as launching customer for secure-by-design innovations.

Digitally resilient companies, public authorities and organisations

In the government's vision, companies, public authorities and civil society organisations are in principle able to determine independently, in collaboration with each other or with the help of ICT or cybersecurity service providers, what risks they face in cyberspace and what measures they need to take to adequately manage those risks. Digital risk management has become a common good and is now expected from all organisations: by their clients and consumers, as well as by insurers and shareholders, for example.

Given the importance of critical infrastructure for our society to function, these responsible organisations have a high level of resilience. Partly because of European legislation, the government imposes additional requirements on these organisations. This means that measures are sometimes imposed to mitigate risks to national security even if they do not directly serve the commercial interests of an organisation or company.

A digitally secure and innovative economy

Clients and consumers can rest assured that all digital products and services will be properly protected throughout their specified life-cycle. Organisations negotiate resilience measures with suppliers. Manufacturers and suppliers have a duty of care in relation to cybersecurity measures for the entire life-cycle of their products and services, partly because of European legislation. It is also possible for clients and consumers to find out about the cyber resilience of companies from which they buy products or services, for example through certification or reports.

In the development and application of new technologies, security by design and security by default are always the guiding principles. Furthermore, in the purchasing and procurement of digital products and services, the risk of espionage, influencing or sabotage by state actors is assessed as standard.

The Netherlands has sufficient cybersecurity expertise, both in terms of resilience and in relation to cybercrime prevention, thanks to both a growing supply of experts on the labour market and the targeted stimulation of innovation.

Countering cyber threats

Together with the business community, the government has a clear understanding of the cyber threat emanating from within and beyond the Netherlands' borders and has its detection mechanisms in order. Most importantly, the Netherlands is capable of limiting cyberattacks by state and non-state actors, thanks to the use of broad-based attribution and response mechanisms, ideally in partnerships and coalitions with EU countries, NATO Allies and other like-minded nations. The government will intervene in identified attacks in order to minimise adverse effects for the Netherlands, repair any damage and address vulnerabilities.

Cybercrime will no longer pay to the same extent. The police and the Public Prosecution Service are targeting cybercriminals and their service providers with a broad, scalable and innovative approach which increases the likelihood of catching perpetrators and of effectively disrupting criminal activity, prevents criminal behaviour and eliminates criminal proceeds. Besides investigation and criminal prosecution, the Netherlands can also use other means of intervention, such as disruption capabilities, victim notification and/or damage limitation. Victims and/or targets can thus be given advance notification wherever possible.

The government is not tackling this threat alone but in a network of public and private cybersecurity and other organisations in which information is gathered, analysed and shared with clients. The provision of help and support to organisations is also a joint effort. Cybersecurity service providers are on hand to make their services available and are working with the government to foster the cyber resilience of organisations at home and abroad.

International cooperation

Cyber incidents do not stop at national borders, so the government actively exploits the opportunities offered by cooperation within and outside the European Union. The Netherlands is driving cooperation between EU member states and is thus contributing to a digitally secure and, where necessary, autonomous EU. This approach serves to tackle cross-border cyber risks and it allows a coordinated response to major cyber incidents and crises within and outside the EU. Constant efforts are being made through cyber-diplomatic means – including capacity building – to reinforce and expand the international coalition driving responsible state behaviour in cyberspace.

3. Aims

To make this vision a reality, aims have been formulated on the basis of four pillars. Those aims offer a response to the current and future challenges set out in Chapter 2.

Pillar I

Cyber resilience of the government, businesses and civil society organisations

This pillar concerns the cyber resilience of the government, businesses and civil society organisations, focusing on the ability to reduce risks to an acceptable level using a collection of measures to prevent cyber incidents and, if cyber incidents do occur, the ability to minimise damage and facilitate recovery.

Aims

- Organisations have a clear picture of cyber incidents, threats and risks and know how to deal with them.
- Organisations are properly protected against cybersecurity risks and are mindful of their own importance to the sector and other organisations in the chain.
- Organisations respond to and recover and learn from cyber incidents and crises swiftly and efficiently.

Pillar II

Secure and innovative digital products and services

This pillar focuses on the suppliers and consumers of digital products and services, and on boosting cybersecurity knowledge development and innovation. Working towards a secure and innovative digital economy contributes to the digital security and earning capacity of the Netherlands.

Aims

- Digital products and services are more secure.
- The Netherlands has a robust cybersecurity knowledge and innovation chain.

Pillar III

Countering cyber threats posed by states and criminals

This pillar focuses on the national and international approach to combating malicious actors that pose a threat, and on gaining a clearer picture of the cyber threat landscape, thus providing a basis for appropriate action. The government has a particular responsibility here and has a range of instruments with which to address the cyber threat.

Aims

- The Netherlands has a clear understanding of cyber threats posed by states and criminals.
- The Netherlands has a handle on the cyber threats posed by states and criminals.
- States adhere to the normative framework for responsible state behaviour in cyberspace.

Pillar IV

Cybersecurity labour market, education and cyber resilience of the public

This pillar focuses on the human being behind the technology and the cyber resilience of the public. Society as a whole has an important role to play in terms of developing digital skills, from basic knowledge and skills to high-level expertise and specialist cybersecurity skills.

Aims

- The public are properly protected against cyber risks.
- Members of the public respond to cyber incidents swiftly and efficiently.
- School pupils are taught digital skills, with an emphasis on security.
- The Dutch labour market can meet the growing demand for cybersecurity experts.

Pillar I: Cyber resilience of the government, businesses and civil society organisations

For our society to function safely and without disruption, digital security is crucial for all businesses, civil society organisations and government organisations. Consider the task of keeping the country's critical infrastructure permanently available, and the confidentiality and integrity of processes. Cybersecurity allows us to use information and communication technology successfully and to reap the benefits of innovation and computerisation. Organisations that have their cybersecurity in order will protect company profits, competitiveness, intellectual property and sensitive client data. Cyber incidents affecting businesses and public authorities could lead to a loss of consumer confidence or of public trust in the government.

The Dutch cybersecurity system, which is designed to help boost organisations' cyber resilience, has evolved autonomously over recent years into a system of wide-ranging partnerships in sectors, supply chains and regions. The positive effect is that cybersecurity knowledge is now spread widely and sectoral expertise has been accumulated. At the same time, this has also led to fragmentation of activities and responsibilities.[15] As a result, information about vulnerabilities or risks does not always reach the relevant organisation in time, if at all. This means that those organisations are not always able to take the necessary steps, and expertise is not deployed optimally. Legal and organisational obstacles have also hampered the effective exchange of information. Furthermore, it is not always clear to organisations within and outside government as to what support is available or where they can go with questions concerning digital security.

Organisations have a clear picture of cyber incidents, threats and risks, and know how to deal with them

To ensure that organisations have a good understanding of threats and risks and know how to deal with them, it is important that they have access to reliable information. Organisations must be confident that the government will provide up-to-date expertise and information about cyber threats, incidents, trends and vulnerabilities so that they can take the necessary action.

Government organisations must collaborate more closely in order to create the most up-to-date situational picture of the cyber risk landscape. This is essential so that the relevant parties can take preventive measures and organise appropriate incident response, including effective disruption, investigation and prosecution.[16] In order to reach as many organisations as possible with information (such as analyses, phenomenon analyses and courses of action) about impending cyber incidents and to organise an appropriate response, the government is working to achieve a detailed level of public-private information exchange which meets the needs of the target group as closely as possible. It will also take account of target groups in which organisations such as small and medium businesses, associations and foundations have limited capacity (time, expertise, resources, network) to apply this information in the right way.

General information about digital security and specific threat and risk information can be shared within the Nationwide Network of Cybersecurity Partnerships (LDS),[17] the development of which is coordinated by the government. The NCSC will evolve further to become the national Cybersecurity Incident Response Team (CSIRT). The NCSC, the DTC and the CSIRT for digital service providers will be merged to form a single organisation. Greater cohesion between existing organisations will also be created by stimulating integration wherever it is useful. For all existing sectoral CERTs and CSIRTs, central government is therefore exploring the extent to which greater cooperation, cohesion or amalgamation with the NCSC would add value. In principle, new CSIRTs are established only where they have added value.[18]

The range of the system is being extended to every corner of society in order to unlock as far as possible the current situational picture, threat information and victim information available to the government, businesses and civil society organisations. Specifically, the system is being further developed and expanded for the benefit of all layers of government, such as municipalities, provinces, water authorities, implementing organisations and safety regions.

Further development of the Nationwide Network of Cybersecurity Partnerships (LDS)

The purpose of the LDS is to enable public and private organisations to boost their resilience level and thus their impact by sharing cybersecurity information widely, efficiently and effectively. It is essential that information-exchange via key organisations generates courses of action which can help organisations enhance their resilience.

Those functionalities include information-sharing, facilitating and boosting collaboration, general target group analysis and situational analysis.

CSIRTs and supervisory authorities will work more closely with national, as well as European and international partners. At European level, CSIRTs can benefit from collaboration on technological research into cybersecurity incidents, development of technological solutions and responses to large-scale cyber incidents. Supervisory authorities will increase collaboration at national level to ensure that scarce capacity is used effectively. In a European context, efforts will be made to step up cooperation and information exchange and, where possible, assistance on cross-border issues.

This leads to the following sub-aims:

- The government has a current and comprehensive picture of cyber incidents, threats and risks.
- There is an effective and efficient exchange of threat information and possible courses of action between the government and the business sector, appropriate to the knowledge and skills of the recipient.
- The LDS is well coordinated, with clear points of contact.
- Government organisations, such as CSIRTs and supervisory authorities, share information effectively, nationally and internationally.

Organisations are properly protected against cyber risks and are mindful of their own importance to the sector and other organisations in the chain

All organisations

Commitment from all companies and organisations is essential for the Netherlands' digital security, not only to ensure the continuity of their own service provision, but also in view of the potentially broader adverse effects for clients, suppliers or dependent third parties. Central government will encourage organisations to implement a basic level of measures in order to contribute to help boost cyber resilience.

The government is also working on more secure ICT products and services at European level with the aim of encouraging and enabling organisations to take responsibility for their own cybersecurity. To assist organisations, particularly SMEs, in safeguarding this basic level of security, the government has an important role to play by ensuring access to information (in comprehensible language) and possible courses of action with regard to cyber threats, for example via the LDS. There is also a role to be played by branch organisations and larger or more cybersecurity-mature organisations, given the potential risks emanating from chain-based and/or sectoral dependencies.

Cybersecurity requirements for a greater number of companies (NIS2)

Cyber incidents do not stop at national borders, so the EU is also working to boost digital security and resilience within the Union. As a result of the review of the Network and Information Systems Directive (NIS2), many more sectors and organisations within the EU will be subject to legal obligations for the security of their network and information systems. This applies to businesses as well as public authorities. It concerns sectors that are already regulated under the original NIS Directive (NIS1), such as energy, transport, drinking water and digital infrastructure. Under NIS2, more sectors will be added, such as waste water, central government, aerospace, food, manufacturing and postal and courier services. Public administration bodies at regional level, such as provinces and municipalities, can be included in the scope of NIS2 on the basis of a risk analysis. As part of the security requirements, these organisations need to meet a high level of cybersecurity. Incidents that have a significant impact will need to be reported without undue delay in order to minimise the adverse effects. Organisations such as the NCSC and the sectoral supervisory authorities will see a significant expansion of their tasks as a result of the implementation of this directive. In the revised directive, more organisations are designated than is currently the case under the Dutch Network and Information Systems (Security) Act (WBNI). When the system for the protection of critical infrastructure is reviewed, consistency in national terminology, NIS2 terminology and terminology from the EU Directive on the resilience of critical entities (CER Directive) will be improved. This strategy regards organisations that fall within the scope of the NIS2 and CER directives as part of the critical infrastructure.[19]

Critical infrastructure and the government

A high level of cybersecurity is expected from organisations within critical infrastructure and government, and requirements are imposed accordingly. The government believes it is important to adopt a risk-based approach in which companies and organisations take measures commensurate with the risk to the organisation. That starts with an understanding of the interests at stake, vulnerabilities, threats and risks. Setting up a sound risk management system is essential. Conscious decisions about this process need to be taken by a director or senior management board. Organisations are also expected to take account of risks stemming from (inter)sectoral dependencies, and of the importance of other parties' security (e.g. suppliers in the chain). Special attention must be paid to operational technology because of its vital importance for the continuity of our infrastructure, critical and otherwise.[20] Organisations are expected to take concrete measures to increase the cyber resilience of this technology. The NCSC and the responsible line ministries will help critical infrastructure organisations to boost their cyber resilience.

The government makes sure that its own systems are secure, that public services are adequately protected against cyber incidents and that personal data (sensitive or otherwise) is secure. Robust legislation covering the whole of government, together with compliance monitoring will be introduced. In the interest of its own security, central government encourages digital autonomy with regard to special products and services.[21] Furthermore, central government constantly monitors vulnerabilities in its own digital systems and processes. Subnational authorities, such as municipalities, provinces, water authorities and safety regions, are also expected to be sufficiently resilient; central government organisations and subnational authorities collaborate closely in this respect.

Some sectors are also subject to additional legislation that imposes sector-specific cybersecurity requirements at least as stringent as those set out in NIS2.[22] The line ministries are responsible for drawing up this sector-specific legislation. The Ministry of Justice and Security ensures that European and national legislation relating to cybersecurity is developed and implemented in a harmonised manner.

Insight, supervision and enforcement

Providing insight into and accountability for the cybersecurity measures that organisations take should be more of a common good. It should therefore be easier for stakeholders (e.g. clients, shareholders and insurers) to get an idea of an organisation's cybersecurity level. Such transparency would also allow stakeholders to properly assess the risk associated with the supplied product or service. Providing insight into cybersecurity measures would thus make organisations more commercially attractive, and it could be accomplished by including cybersecurity in their reports and contracts.[23]

Under legislation such as the forthcoming NIS2 and/or sectoral legislation, regulated organisations are currently obliged to account for their cybersecurity measures to supervisory authorities, which have various instruments to encourage organisations under their supervision to increase and maintain their resilience. They can assess what measures are proportionate and appropriate to the risk an organisation faces. Supervisory authorities also have good oversight of the actual resilience of organisations and sectors. At the same time, those authorities will be confronted by new developments and technological advances that occur in a particular sector or market and give rise to new cybersecurity issues.

This leads to the following sub-aims:

- Organisations know what basic cybersecurity measures are and apply them.
- Government and NIS2 organisations meet high security standards under new and existing legislation.
- Organisations are aware at all levels (including management level) of the importance of cybersecurity.
- Organisations also focus their risk management on cybersecurity risks, and increase transparency in this regard.
- Supervision of an organisation's cyber resilience is geared more to risks for the organisation itself, its sector and its significance for others.

Organisations respond to and recover and learn from cyber incidents and crises swiftly and efficiently

To prepare effectively for cyber incidents, organisations should develop incident, continuity and recovery plans in keeping with the organisation's risk profile. These plans need to be practised regularly, both within the organisation itself and with partners in the sector and chain so that employees know what to do in the event of an incident. Attention must also be paid to effects that may occur in the physical world.

Should an incident nonetheless occur, it is important that an organisation has arrangements in place for assistance. The NCSC also has a statutory obligation to provide support, with the main focus on national security and prevention of social disruption. The NCSC is responsible for operational coordination and management in times of national crises. The government also ensures coherent provision of public and private cybersecurity services in the event of an incident, for example in conjunction with trusted cybersecurity firms.[24] Central government thus provides a stimulus for greater and more effective collaboration between organisations, to ensure that cyber capabilities are deployed as effectively and efficiently as possible.

In order to prepare a response to a national cyber crisis, efficient cooperation must be in place between government organisations, the business sector, the research community and civil society organisations, even across local, regional and national borders. In the event of cross-border cyber incidents and crises, the government encourages fully integrated action on the basis of a national umbrella framework in the form of the National Crisis Plan for Digital Incidents.

Lastly, we must continue to learn from incidents and crises. To this end, organisations will need to be more proactive in sharing their experiences and lessons learned with each other, and in this regard trust is paramount. The information shared by government organisations will be more targeted, so as to ensure a clearer picture of the degree of resilience in organisations, sectors and chains, wherever possible in collaboration with, for example, the business sector or branch organisations. The government will use this insight to provide guidance wherever resilience levels are lagging behind the threat.

To make this possible, attention must be paid to the measurability of resilience and more insight must be gained into the costs and benefits of cybersecurity incidents and measures

This leads to the following sub-aims:

- Organisations are capable of swiftly responding to and recovering from a cyber incident and practise accordingly.
- The government offers coherent cybersecurity services with a recognised point of contact for organisations.
- The government, business sector and research community collaborate closely to ensure effective use of cybersecurity expertise.
- Organisations collaborate effectively in the event of (national) cybersecurity crises, in keeping with regional, supraregional, national and international crisis mechanisms.
- Organisations evaluate cyber incidents, learn from them and share these lessons with each other.

Actions and priorities for Pillar I

The following actions reflect the government's priorities for the current term of office which will be rolled out in pursuit of the objectives in this pillar. A detailed overview of actions is shown in the appendix. This action plan will be updated annually and will provide insight into underlying actions, expected duration and responsibilities.

A. Addressing fragmentation within the system

- The ability to receive timely information about threats and vulnerabilities in a way that is appropriate to the maturity level of the organisation is one of the most important elements for the Netherlands' cyber resilience. To achieve it, the available capacity and expertise need to be deployed as effectively as possible. Fragmentation within the cybersecurity information exchange system should be counteracted wherever possible. The NCSC, DTC and CSIRT-DSP will therefore be merged to form a single national cybersecurity authority. Working in collaboration with public and private partners, this new organisation will provide critical and non-critical organisations, public authorities and members of the public with security information and possible courses of action appropriate to their maturity level.
- The other organisations within the cybersecurity information-sharing system will be assessed in terms of which of their tasks (distributing security information, providing support, organising drills, etc) should be centralised (within the national cybersecurity authority) and which should be sector-based.
- Cybersecurity is an issue that must be addressed by means of a public-private approach. One key element in this respect is the joint collection and interpretation of threat information, so the government will start developing a public-private platform for information and knowledge sharing.

B. No more commitment-free partnerships

- The implementation of the NIS2 directive means that more than 5,000 companies in the Netherlands will be required to report cybersecurity incidents and to take specific steps to increase their cyber resilience. Compliance with these obligations will be monitored. At the moment, these requirements apply to only 200 organisations in the Netherlands, so this expansion will increase the cyber resilience of the designated organisations.
- The government is also taking various measures to boost the cyber resilience of specific sectors. There will, for instance, be additional norms for the healthcare and education sectors, and the government will provide various tools to help organisations to comply. Municipalities and provinces will be subject to tighter security requirements. Multiple support programmes are being offered by the Ministry of the Interior and Kingdom Relations to help them meet those requirements. Lastly, the government believes that it is not only the cyber resilience of IT systems that needs to be addressed, but also the resilience of operational technology. This is made up of complex digital systems that control the locks in our waterways or regulate production in factories, and the impact of system failure is considerable. The government will therefore work to increase knowledge and awareness of the risks in organisations that use these systems.

>>

C. Being prepared for cyber incidents and crises

- At the end of 2022, the government will present the National Crisis Plan for Digital Incidents. This plan will set out how public and private organisations in the Netherlands should prepare for cybersecurity incidents and what they should do if one occurs.
- The government will draw up an interministerial practice schedule on the basis of a government-wide risk analysis and the National Security Strategy. This schedule will incorporate the planning of national and international cyber and hybrid exercises.

Pillar II: Secure and innovative digital products and services

In order for our digitised society to be secure, we need digital products and services that are well protected throughout their lifecycle. This is difficult to achieve in today's market. Consumers cannot tell the difference between secure and insecure products or services, which is partly why suppliers and manufacturers are reluctant to invest sufficiently in the cybersecurity of the products and services they provide. In addition, more and more products and services are now digitalised, from smart televisions to connected cars and medical equipment. Every day, vulnerabilities are discovered in software and there are still too many devices and services on the market that can easily be misused for criminal activities, espionage or large-scale attacks.

Given the market dynamics that exist in an international competitive market where there is insufficient incentive for suppliers to make digital products more secure throughout their lifecycle, statutory measures are needed, in many cases at EU level. Such measures impose greater responsibility on suppliers for the security of their product or service, and offer consumers a basis for claiming compensation in the event of cybersecurity incidents.[25] The government is a major consumer and purchaser of digital products and services and will use its position to stimulate the development of secure products and services.

It is important to anticipate future opportunities and threats. Rapid developments in the digital and technological domain, as in the case of quantum technology or artificial intelligence (AI), require a permanent commitment to the expansion and application of expertise and innovation for the development of cybersecurity products and services. To enhance the Netherlands' competitive position on the EU and international markets, and to minimise undesirable dependence on foreign parties, collaboration within the Dutch innovation chain should be encouraged as much as possible.

Looking back: Roadmap for Digital Hard- and Software Security

The protection of digital products and services is a complex, global issue for which an assortment of measures exist. Under the NCSA, such measures were set out in the Roadmap for Digital Hard- and Software Security.[26] In recent years, for example, EU market entry requirements were introduced for wireless networking devices, a European system was developed for cybersecurity certification of ICT products, services and processes, and the Dutch system was set up, with supervision.[27] European consumers are now also entitled to updates for digital products, content and services and European cybersecurity requirements are being imposed on medical devices.[28] Cybersecurity requirements are also being imposed at global level for connected cars and vehicles.[29]

Digital products and services are more secure

Despite efforts to improve the security of digital products and services, there is still no comprehensive system of legislation (EU or otherwise) setting out the necessary standards for digital products, processes and services and geared to the individual responsibility of manufacturers and suppliers. EU legislation creates a level playing field and enhances the competitiveness of Dutch suppliers. And because EU frameworks have been established on the basis of European public norms and values, they also help to reinforce Europe's digital autonomy at global level, both in a geopolitical context and in respect of the 'tech giants'. In the coming period the Netherlands will be pressing at EU level for a coherent system of legislation, together with the associated standards. This will involve a combination of sectoral measures (such as those that apply to medical devices and energy-supply equipment) and more horizontal measures.[30] Efforts at EU and national level should ensure that consumers can be confident in demonstrably more secure products and services. Clarity about where responsibility for digital security lies and about the standards such security must meet will also ensure that potential compensation can be claimed more easily via regular liability law.

In the Netherlands, cybersecurity purchasing requirements have been developed for all government organisations. This stricter approach to government procurement and tendering also means that the government can use its role as a market player to greater effect when it comes to encouraging the development of secure ICT products and services. The government also has policy in place stipulating that national security interests must be considered during the procurement and tendering process for all products and services.

This leads to the following sub-aims:

- Under EU law manufacturers and suppliers have a duty of care for the cybersecurity of digital products and services throughout their entire lifecycle.
- There is a more coherent system of EU legislation for the cybersecurity of digital products and services.
- European security certificates are issued for different categories of digital products and services.
- European security requirements and standards are also used in non-EU countries.
- Organisations have contractual agreements with clients in respect of cybersecurity.
- The government has purchasing and other policy on the security of digital products and services, and is aware of the relevant requirements.

The Netherlands has a robust cybersecurity knowledge and innovation chain

To ensure measures against cyber threats can be taken both now and in the future, the development and application of Dutch knowledge and cybersecurity expertise need to be continually strengthened. A high-quality and autonomous Dutch knowledge and innovation chain in the field of cybersecurity will reduce undesirable dependence on companies, individuals and solutions in other countries, and will generate economic opportunities for Dutch businesses. Close cooperation between government, the business sector and knowledge institutions is essential in this respect.

Different parts of the chain – such as fundamental and applied research, businesses and public authorities – need to develop closer contacts and to collaborate on specific, long-term projects. By creating a healthy innovation ecosystem, we can ensure that valuable cybersecurity knowledge does not drain away to other countries but is converted into practical products and services. Only then can the Netherlands capitalise safely on the economic and social opportunities of the digital transformation.

A good innovation basis will reduce the Netherlands' dependence on cybersecurity expertise and solutions in other countries. This is vital in order for us to protect our national security and our most sensitive information, now and in the future. To achieve this, the Netherlands needs high-quality security products, including cryptographic products and services. Given that this rare knowledge and expertise is available in our country, the Netherlands is one of the few countries where cryptographic products and services are developed and manufactured. It is essential that we retain this expertise and develop it further, so that the Netherlands can properly protect its sensitive information.

Dcypher

The collaboration platform dcypher brings public and private parties and knowledge institutions together, as well as resources and expertise, to effectively engage in cybersecurity education, research, innovation and concrete applications. Dcypher's mission is to help build a safer, smarter, digitally autonomous and economically stronger Netherlands. The mission of dcypher's partners is to deepen and broaden the development and application of expertise in the field of cybersecurity in the Netherlands. The platform is designed to stimulate knowledge development in the cybersecurity domain, to give a major impetus to the cybersecurity industry and to support the government in its role as launching customer.

In order to foster a healthy cybersecurity innovation ecosystem, the government is working via the centralised public-private collaboration platform dcypher, which in recent years has laid the basis for substantive agenda-setting and programming of long-term research and innovation plans in respect of digital security together with government bodies, businesses and knowledge institutions. This approach covers the whole chain, from fundamental research, via applied research to innovative new cybersecurity products and services. This will generate more knowledge and innovation with a lasting impact on the cybersecurity ecosystem, helping us secure a leading position in Europe. It is also important to ensure a deeply-rooted connection between national and European initiatives and the associated instruments and EU resources. This will be done via the National Crisis Centre (NCC) which liaises between the national cybersecurity network and the European Cybersecurity Competence Centre (ECCC) and its associated network.

This leads to the following sub-aims:

- Dutch (and European) cybersecurity companies supply high-quality products and services that are essential for our digital security and our economy.
- The government, business sector and knowledge institutions collaborate closely on knowledge and innovation relating to cybersecurity.
- The Netherlands has joined European initiatives and funds to stimulate knowledge development and innovation in cybersecurity in the Netherlands.

Actions and priorities for Pillar II

The following actions reflect the government's priorities for the current term of office which will be rolled out in pursuit of the objectives in this pillar. A detailed overview of actions is shown in the appendix. This action plan will be updated annually and will provide insight into underlying actions, expected duration and responsibilities.

A. Security will be mandatory in digital product development

- One of the most important steps towards cyber resilient consumers and organisations is the availability of secure digital products. Security should be one of the main considerations in the development of digital products. The government will regulate this mainly via the EU Cyber Resilience Act. In the negotiations on this regulation, the Netherlands is pressing for the inclusion of a duty of care for manufacturers and suppliers of all ICT products, services and processes, to last through their entire life cycle, including the associated standards and supervision.
- Together with private parties, the government is also contributing to the development and adoption of European cybersecurity certification schemes for ICT products, services and processes, for example for cloud services, 5G technology and Common Criteria. The Ministry of Economic Affairs and Climate Policy is working to stimulate awareness and implementation of certification schemes under the EU Cybersecurity Act. Encouraging and facilitating the use of certification will enable consumers and organisations to make safe choices.

B. Government is stimulating the development of secure digital products via procurement

- The government must have its own cybersecurity in order and can, as a major consumer of ICT products, influence the market by imposing procurement requirements. Government procurement policy could thus contribute to the innovation and development of secure products and services.
- For example, General Security Requirements for Central Government (ABRO) are being drawn up and will be imposed on companies contracted to carry out sensitive and/or classified government assignments.
- The government cybersecurity procurement requirements (ICO) tool will be developed further, expanded and implemented, including the further development of government-wide sets of requirements. The tool will also be available to companies so that they too can apply the procurement requirements.
- The development of high-assurance products will be stimulated by means of enhanced and coordinated commissioning on the part of central government so that the Netherlands retains access to reliable cryptographic solutions.

C. Robust cybersecurity knowledge and innovation chain

- Development in the cryptographic domain will continue through the implementation of the National Crypto Strategy.
- New projects and work programmes are emerging from the interface in knowledge and innovation requirements between government and the business community. The public-private collaboration platform dcypher facilitates connection between government, businesses and knowledge institutions and provides agenda-setting and programming for cybersecurity knowledge and innovation projects and work programmes. Dcypher could play a facilitating and driving role in the quest for funding for high-end knowledge and product development.

Pillar III: Countering cyber threats posed by states and criminals

Cyberspace is fast becoming a place where tensions find expression: increasingly, state and non-state actors are conducting malicious cyber campaigns, often as part of a hybrid campaign, in pursuit of wide-ranging goals. In some cases, the capabilities of criminal groups are now comparable to those of states. And occasionally, states actually seek collaboration with criminal groups, or deliberately allow those groups to act without hindrance. This affects the Netherlands in many ways: theft undermines our earning capacity, sabotage constitutes a direct threat to our national security and cyber threats put pressure on our democracy and the rule of law. The relationship between cyberattacks and geopolitical dynamics could potentially put the allied cohesion of NATO and the EU under strain.

Cybersecurity (and thus also efforts to combat cybercrime) must therefore be regarded as a fixed element of national and international security policy. As this observation makes clear, neither central government nor the Netherlands as a whole can resolve this challenge alone.

If we are to keep pace with the countless malicious actors and the increasing vulnerability of cyberspace, we need a clearer picture of what we are dealing with. Although that picture on its own will not make the Netherlands any safer, it is nonetheless an essential step towards effective, scalable action.[31]

The Netherlands has a clear picture of cyber threats posed by states and criminals

Addressing this challenge is not merely a matter of better observing the actions of state and non-state actors in cyberspace. In addition, the political, diplomatic, military and economic behaviour of other countries provides insight into their views and intentions regarding the use of cyberspace as a means of gaining geopolitical influence. Deploying diplomatic resources is therefore essential in this respect, conducted by means of, say, targeted diplomatic reports, consultations, coalitions with like-minded partners and dialogue with parties who do not share our views. Much of this task falls under the unique responsibility of the government, with, for example, the police, the Public Prosecution Service and the AIVD and MIVD working in collaboration with stakeholders such as the NCSC and the DTC.[32] This enables the Netherlands to build and maintain a picture of the rapidly growing threat and some of the main players. We will also need to work more often, more closely and more actively with EU partners and NATO Allies so that we can identify threats and malicious actors at an earlier stage. To encourage a common understanding of the threat, the government will be more proactive when sharing cyber and other intelligence, thus enabling others to increase their resilience or to take action against cybercriminals.

The government also needs to step up cooperation with other parties and establish more partnerships in order to gather information from outside central government. Possibilities include the business sector, knowledge institutions and international organisations. On the basis of its own information and that of other parties, the government can form a clearer picture of the cyber threat targeting Dutch interests and those of our partners.

This leads to the following sub-aims:
- The government has the capabilities to gather, analyse and share information and intelligence relating to cyber threats posed by states and criminals.
- There is an effective exchange of cyber threat intelligence and information between the government and its international partners.

The Netherlands has a handle on the cybersecurity threats posed by states and criminals

Over the next few years, the government will work to improve information-sharing and to increase resilience, which will help to mitigate cyber threats.[33] The government will also, working within the legal parameters, make more use of the existing scope (both online and off) for detecting, tackling, disrupting and prosecuting malicious actors and their facilitators. To do so, the government can use the AIVD, the MIVD, the police, the Public Prosecution Service, the Ministry of Defence and the Ministry of Foreign Affairs.[34] Statutory and other frameworks will need to be taken into consideration, however.

The police and the Public Prosecution Service will employ a broad, scalable and effective strategy to tackle cybercrime, targeting both the perpetrators of cybercrime and their service providers. As well as pursuing criminal investigations, the police and the Public Prosecution Service will also focus on alternative interventions. Using this broad approach, criminal activities and networks will be disrupted, criminal behaviour prevented, criminal proceeds confiscated and criminal offences punished.

In various international forums, including the EU, the Council of Europe and the UN, the Netherlands contributes actively to the ongoing development of legal instruments designed to strengthen international cooperation against cybercrime, while safeguarding human rights and fundamental freedoms. State-sponsored cyber operations will be disrupted more effectively by the AIVD and the MIVD. The Ministry of Defence will deploy the its constitutional powers more often and more systematically in the national domain, and must be ready to act when needed: not just as a last resort, but also as an offensive digital force.[35]

Given the geopolitical dimension of digital threats, our efforts in cyberspace are an integral part of our broader foreign policy. Together with partners at home and abroad, the Ministry of Foreign Affairs will deploy diplomatic means more effectively in response to cyberattacks and incidents. The Government-wide State Threat Response Framework, which is currently in development, will also be applied in cyberspace wherever possible. The interministerial cyber incident response framework, coordinated by the Ministry of Foreign Affairs, will be used for this purpose. This framework has been applied successfully since 2018 and will be developed further in the coming years.

Where legal parameters restrict operational effectiveness to such an extent that the aim cannot be achieved, consideration will be given to extending those parameters, based on our public values and keeping in mind the normative framework for responsible state behaviour, including fundamental rights and international law (for example, human rights law and international humanitarian law).

This leads to the following sub-aims:

- The government has an effective, internationally aligned attribution and response framework with clear powers and responsibilities.
- The government has offensive and defensive cyber capabilities that are effective in both peacetime and wartime.
- The government ensures the well-coordinated national and international deployment of instruments against cyber threats posed by states and criminals.
- The government can use criminal and non-criminal interventions against cyber criminals and their service providers (e.g. ransomware attacks).

States adhere to the normative framework for responsible state behaviour in cyberspace

Given the geopolitical tensions in the world, cyber threats and cyberattacks are only likely to increase in future. The best way to nip the source of the threat in the bud is to turn the geopolitical arena more to our advantage by promoting the international legal order in cyberspace.

The Netherlands will be an integral part of robust coalitions pressing for responsible state behaviour in cyberspace and will contribute to the further development of a uniform and widely supported normative framework in order to reduce geopolitical tensions. To this end we will use cyber diplomacy to promote democratic norms and values governed by the rule of law, including human rights. Central government complies with this normative framework and actively promotes it, on the basis of our norms and values, and our vision of a free, open and safe internet.

Normative framework for responsible state behaviour in cyberspace

International agreements are needed to deal with the threat of destabilising cyberattacks. UN negotiations on the rules that apply in cyberspace have been ongoing since 1998.[36] The process has now expanded into multiple consultation and negotiation mechanisms focused on cyberspace, to which the Netherlands either actively contributes or has done so in the past: the Group of Governmental Experts (GGE), the Open-Ended Working Group (OEWG) and the Programme of Action (PoA).

The need for stability gave rise to the establishment of a normative framework for responsible state behaviour in cyberspace, which was reaffirmed by consensus by the UN member states in 2021.[37] This framework helps foster stability, as non-compliant countries can be called to account for their behaviour. The guiding principle is that existing international law is applicable in cyberspace.

This means, for example, that the interstate prohibition on the use of force and the non-intervention principle in international law also apply in cyberspace, and that an actual or imminent cyberattack can in certain circumstances be regarded as an armed attack against which a state can invoke the right of individual or collective self-defence. It is also acknowledged that human rights apply online as well as offline and that states must fulfil their human rights obligations in cyberspace, as well as those pertaining to international humanitarian law. In addition, agreement has been reached on 11 non-binding norms of conduct, which provide for agreements, safeguarding and protection below the threshold of armed conflict.

The government endorses the multistakeholder model of internet governance. This model entails open collaboration between stakeholder authorities, civil society organisations, the business sector, research community and the internet technical community within organisations such as the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Engineering Task Force (IETF) and the Institute of Electrical and Electronics Engineers (IEEE). They must take the lead in adjusting the standards, protocols and procedures for the internet's core functionality , without inappropriate interference by state or private actors. The Netherlands is committed to preventing a situation in which national and regional legislation creates barriers that ultimately lead to the fragmentation of the internet.

This leads to the following sub-aims:

- States have a common understanding of the importance of norms of conduct and international law in cyberspace, and act accordingly.
- The Netherlands forms part of a broad coalition which promotes compliance with international law in cyberspace.
- The multistakeholder model continues to be the guiding principle for worldwide governance of the internet.

Actions and priorities for Pillar III

The following actions reflect the government's priorities for the current term of office which will be rolled out in pursuit of the objectives in this pillar. A detailed overview of actions is shown in the appendix. This action plan will be updated annually and will provide insight into underlying actions, expected duration and responsibilities.

A. Understanding the cyber threat

- Knowing and understanding the threat is the first step towards a cyber resilient Netherlands, so the government is investing heavily in the research capability of the intelligence and security services for the purpose of intelligence-oriented in-depth research. This will provide a broader view of current and potential cyber threats. Unique intelligence will thus be translated into specific courses of action so that clients are better able to protect themselves.

B. Increase research and investigative capacity in respect of cybercriminals

- As well as understanding the threat, being able to investigate perpetrators is extremely important. This goes beyond criminal-law interventions alone. The police and the Public Prosecution Service will therefore work with public and private partners to develop other interventions to tackle cybercrime (including ransomware attacks).
- Over the coming years, the Public Prosecution Service will expand its knowledge and expertise in this area and explore the scope for expediting cases by means of a fast-track system.
- The police will make it possible to report more cybercrime phenomena online from 2023.
- In addition, the police will start building a security overview in relation to cybercrime and digitalised criminality, giving society at large

an idea of the main criminal phenomena, operating methods and risk levels. This overview will guide the police and the Public Prosecution Service in their choice of where they focus and which investigations are prioritised.

C. Expand the diplomatic response and defensive cyber capability

- The government is investing in the cyber diplomacy network, and its tasks will be expanded to ensure the availability of better information on cyber threats and developments. The government will also work in a coalition setting to boost compliance with international standards of behaviour and the application of international law in cyberspace. Furthermore, the government will work to promote an open, free and secure internet through stronger commitment to internet governance and by engaging with the multistakeholder community in the Netherlands.
- Together with international partners, the government will develop new, more effective options for a diplomatic response to cyber threats. Existing frameworks, such as the national diplomatic cyber response framework, the EU Cyber Diplomacy Toolbox and the NATO Guide are being developed further. The government will build further on the Government-wide State Threat Response Framework, which brings together all possible response options within central government, and includes an escalation ladder and assessment framework.
- The Ministry of Defence is investing in its overall cyber capability chain and in increasing staff readiness via training and exercises. It is expanding support structures to provide assistance to other organisations in major incidents, for example via the National Response Network (NRN).

Pillar IV: Cybersecurity labour market, education and public cyber resilience

Society's ability to function without disruption depends increasingly on the secure use of digital resources. Pillar II describes the European approach to safeguarding the security of digital products and services. The public's level of cyber resilience is also an important requirement.[38] For many Dutch people, however, achieving and maintaining a sufficient level of cybersecurity is still too big a task. The most vulnerable groups run the greatest risk[39] and many people fall victim to cybercriminals.[40] Putting the necessary cybersecurity measures in place can significantly help reduce the number of cybercrime victims.[41]

Because of the digitalisation of our society, children of ever younger ages are coming into contact with digital products and services. It is imperative that they have the necessary skills to deal with cyber risks and to take cybersecurity measures. This is not yet being adequately addressed in a systematic way by primary or secondary education, even though it is vital that young people learn the skills they need to be safe in our digital world.

The Cybersecurity Council has pointed out the need for sufficient qualified professionals in order to boost our society's long-term cyber resilience.[42] There is a general shortage of expertise on the cybersecurity market.[43] Ensuring organisations' security and resilience requires specialists at secondary vocational, higher professional and university education level who can make and keep digital systems and processes secure.

The public are properly protected against cyber risks

Members of the public need to be as self-reliant as possible and to have the necessary basic knowledge and skills to be able to take effective preventive measures against cyber threats and risks, and they need to actually take those measures in practice. To achieve this, ongoing efforts are needed to make the public more tech-savvy. Awareness-raising campaigns should be run to alert them to what measures they can take to enhance their cybersecurity. In this way, our society will become more cyber resilient.

The aim is that the public take basic cybersecurity measures, such as the use of strong passwords, multi-factor authentication, making backups, installing updates and responding appropriately to phishing attacks. So it is important that they have the knowledge and tools to apply such measures. They should therefore have easy access to information and advice, provided in familiar and trusted surroundings, to enhance their cybersecurity skills.

This leads to the following sub-aims:
- The public are aware of cyber risks, threats and measures, and know where they can obtain help.
- People apply basic cybersecurity measures when they use digital products and services.
- People can get easy access, in a range of settings, to cybersecurity information and advice appropriate to their knowledge and skill level.

Members of the public respond to cyber incidents swiftly and efficiently

It is important to enable people to respond swiftly and efficiently to cyber threats, attacks and disruptions. This can be achieved by ensuring that people are informed at an early stage about current threats that could affect them and about what they can do to stay safe. Over the next few years, efforts need to be made to improve the speed and quality of public information. People need to know where they can find this information and what action they can take. They also need an accessible and straightforward process for reporting or lodging a criminal complaint regarding cyber incidents, such as phishing.

This leads to the following sub-aims:
- People receive sufficient information quickly about urgent cyber incidents and how to respond to them.
- It is easy for people to report cyber incidents or to lodge a criminal complaint about them.

Schoolchildren are taught digital skills with an emphasis on security

It is vital that children learn at a young age how to deal with the digital world and to recognise the risks involved. Pupils need to learn about safe online behaviour. Digital skills, including awareness of cyber risks and security, are not currently part of the national curriculum for primary or secondary education. To equip pupils with digital skills, teachers must also possess those skills themselves and be able to teach them proficiently. It is important that schools receive appropriate support in this respect.

This leads to the following sub-aims:
- Digital skills with an emphasis on security are part of the national curriculum in primary and secondary education.
- Teachers in primary and secondary education are capable (with support) of providing effective instruction in digital skills with an emphasis on security.

The Dutch labour market can meet the growing demand for cybersecurity experts

In order to meet the growing demand for cybersecurity expertise, efforts must be made to make sure there are sufficient specialists on the labour market. Public-private partnerships are essential in this respect. To ensure a better supply, it must be clear precisely where the shortfall is and what is needed to cover it. For example, what mechanisms are available to promote and effectively deploy cybersecurity expertise on the labour market? It may, for instance, be possible to link up with the action plan for technology, focusing on such aspects as the digital transition.[44]

This leads to the following sub-aims:
- There is a clear overview of shortfalls on the cybersecurity labour market and the options for addressing them.
- There are more secondary vocational, higher professional and university education places in cybersecurity that are properly aligned with the labour market, partly through the involvement of companies and knowledge institutions.
- Organisations offer upskilling and reskilling programmes for cybersecurity expertise.

Actions and priorities for Pillar IV

The following actions reflect the government's priorities for the current term of office which will be rolled out in pursuit of the objectives in this pillar. A detailed overview of actions is shown in the appendix. This action plan will be updated annually and will provide insight into underlying actions, expected duration and responsibilities.

A. Increase awareness of cyber risks among members of the public

- The risks posed by digital vulnerabilities and threats must be borne as far as possible by the developers and suppliers of digital products and services. However, there will almost always be a residual risk, which means that the individual user or SME will also need to take their own measures. To do so, the public and SMEs must first of all be aware of the risks and the measures they need to take. To this end, the government will use various public-information-campaign programmes focused on basic cybersecurity measures for specific target groups.
- In addition, the government is bolstering its Digital Government Information Units. These will be able to answer people's questions about cybersecurity and refer them where necessary to support centres, information helpdesks and local support initiatives by private partners.

B. Cyber resilience will be part of the curriculum

- Children need to learn from an early age how to deal with digital products and services. The Curriculum Development Foundation Netherlands (SLO) has been given the task of working with the teaching profession to develop concrete core objectives for basic skills, including cybersecurity skills, for both primary and secondary education. These detailed core objectives for primary and secondary education will be submitted to the House of Representatives in a parliamentary bill.
- A 'basic skills master plan' will be produced to ensure that teachers are properly equipped to provide the best education in language, arithmetic/mathematics, citizenship and computer literacy.

C. Addressing cybersecurity in the labour market

- The government is working with educational institutions to roll out upskilling and reskilling programmes to enhance employees' cybersecurity expertise. They are also working alongside the business community and other relevant parties. Any obstacles and limitations in that collaboration that stem from legislation will be identified and examined to see how they can be resolved.
- The government is investing in higher professional education in the sciences, which includes cybersecurity. Resources are being allocated to (1) higher intake, (2) lower dropout and switch rates, (3) higher lateral intake, and (4) induction/hot transfer to the labour market.

Work has long ceased to be 'tethered' to the office. Thanks to laptops, hotspots and Wi-Fi in the train, it's now possible to send email and attend meetings from any location we choose. But what does this mean for data protection?

4. Governance, evaluation and monitoring

Governance, coordination and cooperation

Digital security is so important that it should be addressed at the highest possible level of an organisation. Leadership, coordination and ownership are crucial in this respect. The relevant government ministers are working closely with each other under the responsibility of the Minister of Justice and Security, the coordinating minister for cybersecurity. Cybersecurity is a standing theme in the Cabinet Committee on Defence and International, National and Economic Security (RDINEV), which manages the overall implementation of this strategy and the associated action plan.

Rigorous coordination will help to synchronise and link national initiatives and investments. A key guiding principle is that coordination by the Minister of Justice and Security should above all facilitate, support and stimulate the process, and should focus on the effectiveness, coherence and strength of government policy on cybersecurity.

The Netherlands Cybersecurity Strategy (NLCS) can only be implemented successfully with close collaboration between representatives of the business sector, the research community and decentralised, regional and national authorities and implementing organisations. An integrated management model will be set up at the beginning of 2023. This will be linked to existing governance structures and will be based on the positive experience gained in the past few years with public-private partnerships. In this model, the joint efforts of public and private stakeholders will be focused on subsidiary topics and intensified with a view to achieving the objectives. With regard to the objectives aimed at strengthening the labour market, for example, efforts will be made to step up innovation or to enhance the efficiency and effectiveness of the cybersecurity system.

It is the task of the Cybersecurity Council (CSR) to advise the government in respect of the implementation and effect of the NLCS. The CSR will be asked to advise periodically on the developments that need to be considered when reviewing the action plan.

The NLCS is a clearly defined framework used to ensure that cybersecurity policy evolves in a coherent and structured manner at all levels. Line ministries will translate this general framework into sector-specific frameworks and regulations for the organisations and processes for which they bear system responsibility. When formulating supplementary policy or legislation in respect of cybersecurity, the government observes the following guiding principles.

Guiding principles from central government for the development of cybersecurity policy and legislation

- Cybersecurity must be an integral part of the Netherlands' digitalisation process.
- Digital security and resilience should be a common good. Cyber risks are an integral part of a broader risk assessment and, on that basis, organisations must take measures that are proportionate, realistic and, where necessary, sector-specific.
- Organisations, public authorities and companies all have a responsibility to bring and keep their own cyber resilience up to date; the government's role is to inform, stimulate, facilitate and assist on the basis of risk assessment. It will set legal and other frameworks and will intervene where necessary, taking account of organisational maturity levels and the interests that organisations represent.
- It must be clear to organisations and the public how and when they can seek information, expertise and assistance.
- Central government and subnational authorities should set the right example and have a level of resilience appropriate to the risks. That is necessary to protect our public interests.
- Capacity within government must be used effectively and efficiently, through efficient organisation, prompt action and maximum collaboration. The NLCS will serve as the general framework that prevents fragmentation of effort in the cybersecurity domain; it provides the basic premise. In addition, there is scope for specific interpretation, for example by means of sectoral policy frameworks, strategies, agendas, roadmaps for subsidiary topics or additional sets of norms.
- Public-private partnership – the pooling of resources – is and will remain the foundation of the strategy. Public-private partnerships must be designed to achieve tangible and measurable results.
- Digital security transcends national borders, so international cooperation at EU/NATO level and beyond is vital. The Netherlands is taking a pioneering role in this respect. Wherever possible, solutions will be sought in an international and European context to strengthen cybersecurity and digital autonomy.

Evaluation and monitoring

The Netherlands' digital security is inextricably linked to technological and social developments. Cybersecurity measures that are effective today might be obsolete by tomorrow, and that is why the government has opted for an adaptive approach to this strategy and the associated action plan. In order to respond to trends, current threats and risks, we need to be able to develop, adjust or intensify the measures arising from the Netherlands Cybersecurity Strategy over time.

In this regard it is important to look at what measures work and what do not, so that the government and other partners can be as effective as possible in their policy and other interventions, and ensure the maximum benefit to society. However, as the Cybersecurity Council has pointed out, measuring the effects of cybersecurity policy is no simple matter.[45] First, this strategy consists of different aims designed to enable the Netherlands to capitalise on the economic and social opportunities of digitalisation and at the same time safeguard our security. The successful achievement of the aims in this strategy will thus involve a combination of different factors. Second, security interventions are designed to prevent incidents. Naturally it is difficult to measure the number and nature of incidents that have been prevented. Third, cybersecurity also depends on external factors. It hard to know how much of the improvement in cybersecurity can be attributed to cybersecurity policy itself. This must therefore be factored into the evaluation approach for this strategy.

Nevertheless, it is important to continue working to improve our insight into the effects of cybersecurity policy so we can ensure an effective cybersecurity approach in the future too. To this end, a monitoring and evaluation programme has been formulated as part of the NLCS, based on what *can* be measured.

Approach

The Netherlands Cybersecurity Strategy is the country's fourth integrated cybersecurity strategy.

The methodology from the Strategic Evaluation Agenda (SEA)[46] was used to compile the monitoring and evaluation programme. This method is designed to plan monitoring and evaluation activities in a more structured way so that relevant insights can be gained at the right moments, with a view to learning and accountability.

Evaluation programme

Pre-implementation phase

Under the previous government, the Netherlands Cybersecurity Agenda (NCSA) was evaluated for the first time.[47] Based on the experience gained with the NCSA, the compilers of this strategy decided to make a sharper distinction between the strategy and the action plan, resulting in a more future-oriented and longer-term strategy, accompanied by an adaptive action plan that could be adjusted or intensified in the event of changes in the interests at stake, the threat, resilience levels or other political/administrative requirements. Completed actions could also generate follow-up actions, for example after a survey or study has been conducted.

Further focal points arising from this evaluation (or incorporated in the formulation of the action plans) were the explicit allocation of ownership and responsibilities, and a more definitive description of intended actions and effects. Lastly, greater attention needs to be paid to the measurability of the intended results and effects of the strategy and interim evaluation.

The NCSA evaluation proposes a methodology to enable a logical structure for a strategy. This is followed by the formulation of key aims that define the desired situation or effects to be achieved in the future, and a series of sub-aims which will help to achieve them. The aims will be fleshed out into an action plan describing the government measures that will further the attainment of the goals. The activities or measures will be clearly linked to the intended effect set out in the key and sub-aims.
The actions in the plan will be financed in part from the additional funds set aside for cybersecurity in the coalition agreement. A more detailed breakdown can be found in the Financial Overview in the Appendix to the NLCS.

Implementation phase

The House of Representatives will be informed annually about the progress of the Netherlands Cybersecurity Strategy. It will also be possible to supplement or adapt actions in the progress report on the basis of emerging insights and developments, for example in the light of the new CSBN.
In order to track the progress of the measures over time, the Research and Documentation Centre (WODC) of the Ministry of Justice and Security will commission a baseline measurement to be taken, so as to gain a clear picture of the situation before the measures are introduced.

Post implementation phase

In principle the NLCS will cover a period of six years. There will in any event be an evaluation in 2025, halfway through the term covered by the strategy, with the aim of producing lessons learned that can be incorporated in future policymaking.

In order to effectively meet current knowledge needs, a decision will be made at a later stage with regard to the specific focus of the evaluation. Given the breadth of this strategy and the wide variety of actions, an evaluation of all aims and measures is not likely to produce many firm recommendations. For this reason it may make sense to focus on one or more relevant sub-topics, e.g. one about which little is known in terms of the theory of change, or one whose significance will increase in the future.

A subsequent government can ultimately decide about the eventual duration and any final evaluation of the Netherlands Cybersecurity Strategy.

Online shopping is still enjoying explosive growth. Owing to the COVID-19 measures, in 2020 the number of parcels delivered rose by 100%. Digital systems are essential for ordering and delivering all these products.

Appendices

Financial overview

Like the previous government, this government has made available structural resources specifically earmarked for increasing cyber resilience. The previous government made a structural investment of €95 million to boost cyber resilience,[48] and this government is investing a further €111 million in cybersecurity. A breakdown by ministry is shown below. These resources are part of a broader structural investment of €300 million which is being used, for instance, to strengthen the AIVD and the MIVD and to invest in economic security and critical infrastructure.

The structural investment of €111 million will contribute to the implementation of the ministries' various actions in pursuit of the strategy's aims.[49] In addition, cyber resilience forms part of the government's further investment in digitalisation more broadly, in enhancing its own ICT infrastructure or in specific policy areas. Examples include improvements to the mission network, (which is home to cyber diplomats, for instance), and strengthening the Defence organisation, with some of the investment going to cyber capabilities. In cases where no additional investment is possible but there is still a requirement, there will need to be a reprioritisation within individual budgets. Lastly, the government is exploring the scope for financing additional activities through EU digitalisation funds. Generic national funds, such as the National Growth Fund, could also be used to enhance digital resilience. Besides funding, there are other critical requirements that need to be met in order for the actions to be realised. Sufficient capacity in the labour market requires particular attention in this regard.

Ministry	2022	2023	2024	2025	2026	2027 onwards
Economic Affairs and Climate Policy	2,1	6,6	13,5	13,5	13,5	16,1
Infrastructure and Water Management	0,5	1,1	2,3	2,3	2,3	2,8
Justice and Security	8,7	14,8	29,5	29,5	29,5	35,5
of which NCSC	6,6	13,7	27,5	27,5	27,5	33
Interior and Kingdom Relations	5,9	13,5	27,2	27,2	27,2	32,6
of which NCSC	3,8	7,9	15,9	15,9	15,9	19,1
Foreign Affairs	0,5	0,5	0,5	0,5	0,5	0,7
Defence	3,4	7,1	14,2	14,2	14,2	17
of which NCSC	3,4	7,1	14,2	14,2	14,2	17
Education, Culture and Science	0,5	1,3	2,7	2,7	2,7	3,2
Health, Welfare and Sport	0,5	1,3	2,7	2,7	2,7	3,2
TOTAAL	**22,1**	**46,2**	**92,6**	**92,6**	**92,6**	**111**

Abbreviations

AI	Artificial Intelligence
AIVD	General Intelligence and Security Service
CERT	Computer Emergency Response Team
CDINEV	Senior Civil Service Committee on Defence and International, National and Economic Security
CSBN	Cybersecurity Assessment for the Netherlands
CSIRT	Computer Security and Incident Response Team
CSIRT-DSP	Cybersecurity Incident Response Team for Digital Service Providers
CSR	Cybersecurity Council
DOCS	director-level management meeting on cybersecurity
DTC	Digital Trust Centre
ECCC	European Cybersecurity Competence Centre
EU	European Union
FIOD	Fiscal Information and Investigation Service
GGE	Group of Governmental Experts
ICAAN	Internet Corporation for Assigned Names and Numbers
ICT	Information and communications technology
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IOCS	Interministerial Committee on Cybersecurity
MIVD	Defence Intelligence and Security Service
NCC	National Crisis Centre
NCSA	Netherlands Cybersecurity Agenda
NCSC	National Cyber Security Centre
NCTV	National Coordinator for Counterterrorism and Security
NIS2	Revised Directive on Security of Network and Information Systems
NLCS	Netherlands Cybersecurity Strategy
OEWG	Open-Ended Working Group
PoA	Programme of Action
RDINEV	Cabinet Committee on Defence and International, National and Economic Security
SEA	Strategic Evaluation Agenda
UN	United Nations
WBNI	Network and Information Systems (Security) Act

Glossary

Based on the CSBN, the main terms are defined as follows:

Attack: see 'cyberattack'.

Cyberattack: Malicious act aimed at using digital resources to disrupt one or more digital processes.

Cyber incident: Combination of events or activities that could result in disruption of one or more digital processes. This includes both a cyberattack (malicious action by an actor intent on disrupting one or more digital processes by digital means) and a system failure resulting from natural or technical causes or human error.

Cybersecurity: The full spectrum of measures designed to reduce relevant risks to an acceptable level. Measures may focus on the prevention of cyber incidents and, if a cyber incident does occur, on detection, damage limitation and recovery. What constitutes an acceptable level of risk is determined by a risk assessment.

Digital domain or **cyberspace**: a complex environment resulting from the interaction of digital processes, supported by globally distributed physical information and communication technology (ICT) devices and connected networks. The digital domain is approached from three different angles or levels: 1) digital processes implemented (or initiated) by humans; 2) the technology (IT and OT) that enables the digital processes; 3) risk management and/or governance that guides the other two levels.

Digital process: a process carried out entirely or partly through the complex and interrelated interaction between people and numerous components of hardware, software and/or networks. Fully automated processes, such as process control systems, are also defined as digital processes.

Digital security: the undisrupted functioning of information and process control systems, the data processed and stored within them and the services and processes that depend on them.

Disruption: adverse effect on the availability, integrity of confidentiality of information or the processing of information; in other words, a disruption of the technological level of the digital domain.

Interests: Values, social gains and tangible and intangible assets that may be damaged if a cyber incident occurs, and the importance that society or a party attaches to protecting them. The CSBN focuses on national security interests.

Resilience: the ability to reduce relevant risks to an acceptable level by means of a set of measures to prevent cyber incidents and, if they do occur, to detect them, limit the damage and facilitate recovery. What constitutes an acceptable level of resilience is determined by a risk assessment. The risk assessment can help with the selection of the right technical, procedural or organisational measures.

Risk: the chance that a threat could lead to a cyber incident and the impact on the interests concerned. Both are viewed in relation to the current level of cyber resilience.

System failure: a situation in which one or more digital processes are disrupted due to natural or technological causes or as a result of human error.

Threat: a cyber incident that could occur or a combination of simultaneous or successive cyber incidents.

Other terms

Central government: central government comprises 12 ministries, many implementing agencies and services, various inspectorates and the High Councils of State.

Civil society organisations: civil society organisations operate in a field of activity between government, market and community. As a rule, they are non-profit-making organisations with a social purpose. This strategy uses the term to refer to foundations and partnerships which help to boost cybersecurity in the Netherlands and other countries.

Combating cybercrime: efforts to combat crime in which a computer system is attacked or misused for the purpose of criminal activity. Combating cybercrime is an integral part of the cybersecurity approach.

Government: the government as a whole consists of central government, provinces, municipalities and water authorities.

Multi-factor authentication: method used to determine whether a user or digital system is actually who or what they claim/it claims to be. This can be done in various ways. One example is a password and a code that the user receives via SMS. Another is a combination of a fingerprint and a password.

Organisations: the totality of government bodies, companies, knowledge institutions and civil society organisations.

Phishing: attack in which the perpetrator tricks someone into revealing important information, such as login data or credit card details. Phishing is usually done via emails, but perpetrators also do it by phone, text message or in-app messages.

Public values: a reflection of what society regards as key values, such as security, democracy, self-determination, non-discrimination, participation, privacy and inclusion.

Safety region: an area in which different authorities and services collaborate on tasks relating to fire services, disaster control, crisis management, medical assistance, law enforcement and public order. The Netherlands has 25 safety regions.

Security by default: this means that the configuration is based on the highest protection.

Security by design: this means that security is factored in at the design phase.

Sub-national authorities: these consist of provinces, municipalities and water authorities.

For more definitions of cybersecurity terms (in Dutch), please refer to the Cybersecurity Alliantie's Cybersecurity Dictionary.

Notes

1 Digitalisation policy framework (Parliamentary Papers, House of Representatives, 2021-22, 26 643, no. 842 reprint).
2 NCTV, 'Cybersecurity Assessment for the Netherlands' 2022 and Glossary NIST Computer Security Resource Centre.
3 NCTV, 'Cybersecurity Assessment for the Netherlands' 2022.
4 Digitalisation policy framework (Parliamentary Papers, House of Representatives, 2021-22, 26 643, no. 842 reprint).
5 The six national security interests, as set out in the National Security Strategy, can all be affected from cyberspace.
6 NCTV, 'Cybersecurity Assessment for the Netherlands', 2021
7 AIVD, 'House of Representatives informed about AIVD priorities and focus for 2022', 2021.
8 NCTV, Cybersecurity Assessment for the Netherlands', 2018-2022; Dutch Safety Board (OVV), 'Vulnerable through software – Lessons resulting from security breaches relating to Citrix software', 2021. Cybersecurity Council (CSR), 'Integrated approach to cyber resilience', 2021.
9 Risk management often proves to be organisationally complex. Thorny issues include the identification of information flows, maintaining hardware and software inventories, keeping pace with developments and consistent updating of risks.
10 For the government, EU digital autonomy means the EU's ability, as a global player, in collaboration with its international partners and on the basis of its own insights and choices, to safeguard its public interests in the digital domain and be digitally resilient in an interconnected world (Parliamentary Papers, House of Representatives, 2021-22, 26 643, no. 842).
11 These work sessions and the meetings intended to formulate specific goals together with various parties were facilitated by De Argumentenfabriek (www.argumentenfabriek.nl).
12 The outcome of the questionnaire and sessions with stakeholders can be found at www.nctv.nl (in Dutch).
13 The term CSIRT is used in this strategy to refer to a CSIRT as defined in NIS1 and NIS2.
14 For further details of these two tracks, see the letter regarding the integrated approach to cybercrime that will be sent to the House of Representatives in November 2022.
15 Cybersecurity Council, 'Integrated approach to cyber resilience', 2021.
16 See also the aims in Pillar III.
17 For more information about network organisations, see https://www.ncsc.nl/onderwerpen/samenwerkingspartnerworden/aansluiting-op-het-landelijk-dekkend-stelsel-lds and partnerships https://www.digitaltrustcenter.nl/samenwerkingsverbanden (in Dutch).
18 The term CSIRT is used in this strategy to refer to a CSIRT as defined in NIS1 and NIS2.
19 Proposal for Directive from the European Parliament and the Council on measures for a high common level of cybersecurity across the Union and the withdrawal of Directive (EU) 2016/1148; Proposal for Directive from the European Parliament and the Council on the resilience of critical entities (CER Directive).
20 Other commonly used terms for operational technology include Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) and Industrial Automation & Control Systems (IACS).
21 See also the aims in Pillar II.
22 For example, the General Security Requirements relating to Defence Orders 2019 (ABDO); proposal for a revised Network Code for cybersecurity aspects of cross-border electricity flows as an elaboration of the Regulation of the European Parliament and of the Council on the internal market for electricity; proposal for a regulation of the European Parliament and of the Council on digital operational resilience for the financial sector.
23 Dutch Safety Board (OVV), 'Vulnerable through software – Lessons resulting from security breaches relating to Citrix software', 2021.
24 See also the aims in Pillar II.
25 This refers to a claim for damages by the client to the supplier as a result of non-compliance with specified security requirements for the safety of their product or service.
26 See also the Evaluation Report Roadmap for Digital Hardware and Software Security (Parliamentary Papers, House of Representatives, 2021, 26643, no. 867.
27 On the basis of a delegated act under the EU Radio Equipment Directive, 2014/53/EU; the EU Cybersecurity Act, 2019/881; the Cybersecurity Regulation (Implementation) Act.
28 Sale of Goods and Supply of Digital Content (Implementation of EU Directives) Act; on the basis of the EU Medical Devices Regulation, 2017/745.
29 UN Regulation No. 155 – Uniform provisions concerning the approval of vehicles with regards to cybersecurity and cybersecurity management system.
30 Horizontal measures refer to non-sector-specific measures.
31 The emphasis in this pillar lies on tackling state actors and criminals as they pose the main threat to Dutch interests. This does not detract from the fact that other malicious actors, such as hacktivists, also pose a potential threat. Where relevant, activities that help to achieve the aims in this pillar could also be useful in tackling other malicious actors.
32 See also the aims in Pillar I.
33 See also the aims in Pillar I.
34 Besides the specified organisations, there are also other investigation services which could, in specific cases, play a part in detecting, tackling and disrupting malicious actors. These services include Customs, the Fiscal Information and Investigation Service (FIOD) and the Royal Military and Border Police.
35 As a last resort, the Ministry of Defence can provide additional sustainment capability in support of the civil authorities, in both normal and exceptional circumstances.
36 United Nations General Assembly resolution (A/RES/53/79) concerning 'Developments in the field of information and telecommunications in the context of international security', 1998.
37 United Nations, 'Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security', 2021; United Nations, 'Open-ended working group on developments in the field of information and telecommunications in the context of international security: final substantive report', 2021.
38 NCTV, 'Cybersecurity Assessment for the Netherlands', 2022
39 Behavioural Insights Network Netherlands, 'Gedragsadviezen: Gedragswetenschappelijk perspectief op vijf grote maatschappelijke vraagstukken: klimaat, digitalisering, kansengelijkheid, wonen en niet-gebruik van voorzieningen' Behavioural recommendations (Behavioural science approach to five major issues facing society: climate, digitalisation, equal opportunities, housing and non-use of services) (in Dutch), 2022.
40 Statistics Netherlands (CBS), 'De Veiligheidsmonitor 2022' (Safety Monitor 2022) (in Dutch).
41 This pillar is closely related to combating cybercrime, as also discussed in Pillar IV.
42 Cybersecurity Council, 'Integrated approach to cyber resilience', 2021.
43 Dutch Safety Board, 'Vulnerable through software - Lessons resulting from security breaches relating to Citrix software', 2021.
44 In line with the motion submitted by Mustafa Amhaouch et al about an analysis of the effectiveness of initiatives to resolve personnel shortfalls in the technology sector (Parliamentary Papers, House of Representatives, 2021-2022, 35925 XIII, no. 38)).
45 Cybersecurity Council, 'CSR Recommendation Letter concerning focus of and approach to the evaluation of the NCSA', 2020.
46 https://www.toolboxbeleidsevaluaties.nl.
47 Parliamentary Papers, House of Representatives, 2020-2021, 26643, no. 763.
48 For allocation by ministry, see the budgetary overview in the coalition agreement 'Confidence in the Future', 2017.
49 Some actions are based on the implementation of European law, such as NIS2, CER and CRA, for which negotiations are still ongoing. The exact amounts needed for investments in these programmes cannot yet be calculated.

October 2022

This is a publication of the National Coordinator for Counterterrorism and Security (NCTV) on behalf of the Dutch government.
info@nctv.minjenv.nl