‘Building Digital Bridges’

International Cyber Strategy

Towards an integrated international cyber policy

1. Introduction

The Netherlands is committed to keeping cyberspace open, safe and free. Among other things, this means taking full advantage of the opportunities that digitalisation offers our economy and society, confronting threats, and protecting fundamental rights and values. Given the transnational nature of cyberspace, safeguarding these interests has an international dimension. Our foreign policy has a direct influence on the Netherlands' position as a model country, a partner and a place to do business.

In releasing this International Cyber Strategy the government is fulfilling the pledge it made in its response to advisory reports by the Advisory Council on International Affairs (AIV) ('The Internet: A Global Free Space with Limited State Control') and by the Scientific Council for Government Policy (WRR) ('The Public Core of the Internet'). The International Cyber Strategy is complementary to and in line with the National Cybersecurity Strategy (NCSS 2), the Digital Agenda 2016-17, the Human Rights Strategy 2, the Defence Cyber Strategy and the Netherlands' International Security Strategy.

Contents

Chapter 2 explores the international interests, threats and challenges at play in this area and presents the vision and principles underlying the Strategy. Chapter 3 explains the various types of international partnerships relating to cyber policy and reviews the prospects for the further development of policy. Chapter 4 sets out the policy priorities for further enhancing the Netherlands' already strong position in the digital domain.

2. Interests and vision

Cyberspace is a field where international interests, threats and challenges intersect. Against that backdrop, this chapter will first discuss, in succession, the interests, threats and challenges relevant to this field and then the Netherlands' overall vision and principles.

2.1 International interests

The government has identified a number of fundamental interests in the international arena with regard to cyberspace. As stated in NCSS 2 the government views these interests in terms of freedom, security and growth.

2.1.1 Social and economic growth

Interest: The Netherlands should be capable of seizing the social and economic opportunities offered by global digitalisation and taking further advantage of them.

The Netherlands is one of the most connected countries in the world, with a competitive market for data centres and web hosting services. This makes it perfectly positioned to profit from digitalisation. In the Netherlands, information and communication technology (ICT) is a significant contributor to economic growth, and it is increasingly used in all sectors of the economy and society. As a result, the Netherlands is evolving into a digital knowledge and information society.

Interest: The Netherlands benefits from an open, non-fragmented internet, in which information can circulate freely.

Open governance and 'permissionless innovation' are crucial to the development of the internet. Thanks in part to effective self-organisation and self-regulation, the internet has become a shared global infrastructure that is accessible to all. Internationally, the Netherlands is keen to continue safeguarding the development, openness, availability, reliability, security and integrity of the internet.

2.1.2 Fundamental rights and freedoms

Interest: The Netherlands benefits from the existence of global protections for human rights online.

Fundamental rights and freedoms are universally recognised, in both the real and digital world. They form the basis for an open, free and safe society. The Netherlands regards security and freedom as complementary, rather than conflicting, interests: a safe, secure society is a one where individuals' fundamental rights and freedoms are protected. Indeed, promoting a safe digital environment can protect the rights of individuals who may be vulnerable or threatened. It is important for everyone living in the Netherlands who uses the internet that these rights are well protected in the rest of the world and that relevant agreements are honoured.

2.1.3 Security

In the digital domain, security is a prerequisite not only for a well-functioning society, but also for confidence in our economy and the protection of rights online. The government has identified three security interests in this area:

Interest: Protecting the Dutch public and Dutch companies from cybercrime
Cybercrime is a transnational problem, and in the case of the Netherlands, the threat often originates abroad. Therefore, protecting businesses and the public in the Netherlands requires a highly coordinated international effort. To ensure that the rule of law is upheld in cyberspace, it is in the Netherlands' interests that international regulations are in place with regard to operational cooperation, law enforcement and prosecution.

Interest: International cooperation enhances the Netherlands' resilience to disruptions to, breakdowns in and misuse of ICT.
It is not possible to guarantee an open, free and stable digital domain without security. The Netherlands therefore works at national and international level to promote cybersecurity.

Interest: The Netherlands defends its national security interests together with its international allies, so as to guarantee peace, security and stability in cyberspace.
The three strategic interests set down in the International Security Strategy are equally applicable in cyberspace:

- defence of our own and our allies' territory;
- an effective international legal order;
- economic security.

All of these interests have a significant digital component and are consequently exposed to the types of risks associated with cyber threats.

2.2 International threats

Various malicious actors are making increasing use of the digital domain to pursue their interests, such as financial gain, the acquisition of information and political or military objectives. These trends and developments are discussed at length in the Netherlands' annual Cybersecurity Assessment (CSBN).

Threat: Both quantitatively and qualitatively, cybercrime originating abroad is a major threat to Dutch society.
The Dutch economy is harmed by cybercrime and economic cyber espionage. Cybercriminals are increasingly well-organised, a trend that magnifies the potential damage caused by their activities.

This trend is fuelled by the relatively low cost and limited risks associated with engaging in cybercrime or cyber espionage. The cost of mounting a robust defence is generally much higher than the cost of carrying out a cyberattack.

Threat: State actors are using digital resources to advance their geopolitical interests in a way that can threaten Dutch national security.
Increasingly, state actors are using digital resources for the purpose of exerting influence and engaging in sabotage and espionage, either as a general instrument of power or in specific conflict situations. This trend is inextricably linked to larger geopolitical developments. Russia's possible

involvement in hacking during the US elections is an example of this. Various conventional and 'hybrid' conflicts in the vicinity of Europe now have a significant digital component, including the wars in Ukraine and Syria. Active and latent conflicts are also spilling over into cyberspace. The Netherlands is systematically targeted by digital intelligence activities. Digital espionage attacks are continually being directed at the Dutch government and Dutch businesses. It is probable that such attacks against the Netherlands will increase in scope and severity at times of mounting geopolitical tensions, particularly when such tensions affect the Netherlands.

Threat: The increasing use of cyber operations for political objectives threatens the international legal order.
In cyberspace it is difficult to identify the perpetrators of international unlawful acts and to verify compliance with existing rules; consequently, cyber operations pose a threat to the international legal order. Cyber operations make it possible to create peremptory effects that remain below the traditional legal thresholds established by the UN Charter and Article 5 of the North Atlantic Treaty. In addition such operations often take place outside the public eye.

Threat: Cyberattacks on vital infrastructure carried out by international actors can pose a serious threat to national security by manipulating, damaging or denying systems.
Various agencies and levels of government work together to swiftly identify and combat cyberattacks on central government and vital infrastructure and to mitigate the repercussions of such attacks. This requires the close involvement of private partners, which are often interconnected with one another, both nationally and internationally. It is essential for all parties to be aware and resilient.

Threat: Digital economic espionage by foreign intelligence services puts pressure on the Netherlands' competitiveness.
The past year saw a large number of digital attacks targeting companies in the Netherlands for reasons of economic espionage. Economic espionage harms the Netherlands' competitiveness. The aim of these attacks was to obtain technology that may not yet have a proven market value. The technologies and trade secrets stolen in attacks like these could be of great value to ensuring a stable and growing economy that forms the basis for our prosperity. Two-thirds of the targeted companies were unaware that the attacks had occurred.

2.3 International challenges

In addition to the threats discussed above, there are a number of other developments that need to be taken into account. Although trends in the digital domain are difficult to predict, it is possible to identify several relevant international challenges:

- *Not only is the volume of data increasing, both nationally and internationally*, so too is international interest in obtaining data. More and more, the work of both the public and private sector is data driven and reliant on large files that are increasingly being stored in the cloud, thus often outside of national borders.
- *The internet of things ('everything is connected to the internet') and hyperconnectivity ('everything and everyone is interconnected')* stimulate innovation and make technology more user-friendly, but at the same time, these developments leave the door open to misuse on a global scale.
- *The issue of jurisdiction makes it more difficult to investigate cybercrime and prosecute cybercriminals and undermines public trust in the digital domain.* The government also has law enforcement responsibilities in cyberspace. However, it is difficult to reconcile the global nature of cyberspace with the territorial boundaries of traditional national jurisdictions. Criminal investigations are premised on territorial jurisdiction for law enforcement and use of investigative methods. The fact that customary notions of jurisdiction are not fully applicable to cyberspace can seriously impede investigations. Criminal are aware of this fact and take advantage of it. The traditional system of international legal assistance cannot keep pace with the methods used by criminals to avoid detection. As a result there is a danger that

cyberspace could become a haven for technologically-minded criminals to commit criminal acts.

- *Due to the non-centralised and anonymous nature of the internet, it is more difficult to monitor and enforce existing agreements.* There is no better place than the internet for maintaining anonymity and secrecy. The technology is easily obtainable and requires minimal investment. Moreover, attribution is often problematic. This poses a major challenge in devising effective international policy, given the difficulty of monitoring eventual agreements.
- *A sharp divide can be discerned in virtually all international discussions about cyberspace.* On the one hand, you have countries (like the Netherlands) that focus on a multi-stakeholder model and on international law and that champion the protection of the integrity of the internet and the applicability of international law. On the other hand, there are more state-oriented countries that argue for more government control and limitations on the applicability of international law. Between these two extremes there is a large group of countries ('swing states') which have not yet taken a clear position on the issue, due to their political, economic and social interests. The Netherlands is keen to convince them that a free, open and safe internet would serve those very interests.
- *Digital technologies are proliferating rapidly as standards of living rise and the need for connectivity grows.* Nevertheless, 60% of the world's population is not yet online and is unable to take part in the digital economy. As a result the digital gap is still large, and the advantages of the digital revolution cannot be widely shared. The digital gap affects developing countries in particular, depriving them of social and economic growth. A lack of infrastructure, political will and expertise ensures this gap remains entrenched and thus poses a threat to sustainable development.

2.4 Vision and principles

On the basis of the above-mentioned international interests, threats and challenges, the government has drawn up the following vision statement:

> *Together with the private sector, the technology community, academia and non-government organisations (NGOs), the Dutch government is committed to ensuring a safe, free and open digital domain, in which we can confront threats, protect fundamental rights and values and take full advantage of the opportunities that digitalisation offers our society.*

Internationally, as in the Netherlands, the nexus between growth, security and freedom is a dynamic balance that must be achieved through an ongoing, open, pragmatic dialogue between all stakeholders. The government bases its policy on the following principles:

1. The purpose of cyber policy is to create favourable conditions for the activities of government authorities, companies and individuals. Due to the transnational nature of cyberspace these conditions can only be fully fleshed out once they have been agreed internationally.
2. The Netherlands aligns itself with existing international structures, instruments (including policy instruments) and partnerships and will enhance them where necessary.
3. As with national policy, international cyber policy will be developed and implemented in accordance with the multi-stakeholder consultation model and through public-private partnerships. In so doing the government will seek the input of the private sector, the technology community, academia and NGOs.
4. The economic and social advantages associated with the internet require the 'public core' of the internet to function in a reliable, predictable, stable and safe way. This core possesses elements of an international public good that transcends individual sovereign and private interests. The Netherlands recognises that, given the nature of cyberspace and our dependence on it, it is necessary to exercise restraint when engaging in activities that can affect that public core. To the greatest possible extent, the responsibility for maintaining and cultivating this public core should fall to the technology community, with the state playing a supporting role.
5. Ensuring consistency between domestic and foreign policy is key. The Netherlands' position on international matters should follow on from domestic practices, in line with the motto 'preach what you practice'. Conversely, domestic measures that deviate from the Netherlands'

international positions and treaty obligations undermine our credibility and effectiveness in our pursuit of international order in this area. With that in mind, 'practice what you preach', too, should serve as a point of departure for domestic policy. Obviously, the Netherlands is only obliged to abide by international rules once international consensus exists and the Netherlands has consented to assume the relevant obligations.

6. The internet's transnational nature means that any challenges and threats that may arise with regard to security must be dealt with in an international forum. Given that the international legal order is based on the principle of sovereignty, national governments can only address security challenges in cyberspace to a limited degree. This is an issue that requires international cooperation in accordance with an integrated approach.

3. Approach

The government takes an integrated approach to international cooperation on cyber policy. This extends to a variety of areas, which are discussed below. This section also looks at prospects for further policy development.

3.1 International cooperation, diplomacy and strengthening international legal frameworks

At both the domestic and international level, effective cooperation on cyber policy is a joint effort requiring the input of policymakers and the implementing bodies involved in the operational side of the equation. In keeping with this principle the Dutch government pursues its policy through a variety of channels (outlined below).

A. In order to promote the Netherlands' domestic and foreign interests, the government forges broad coalitions and partnerships, both bilaterally and multilaterally, in international organisations like the United Nations (UN), the European Union (EU), the North Atlantic Treaty Organization (NATO), the Council of Europe, the Organisation for Economic Co-operation and Development (OECD) and the Organization for Security and Co-operation in Europe (OSCE). The private sector, the technology community, academia and the non-governmental sector are involved by means of multi-stakeholder and public-private platforms such as the Internet Governance Forum (IGF), the Internet Corporation for Assigned Names and Numbers (ICANN), the Contractual Public-Private Partnership (cPPP) on cybersecurity, launched by the EU in July, and the European Information Sharing and Analysis Centres (ISACs).

B. A wide range of operational partnerships have been based on these bodies and coalitions, particularly in the realm of security. This is done through platforms like the Forum of Incident Response and Security Teams (FIRST), the Task Force on Computer Security Incident Response Teams (TF CSIRT), the Malware Information Sharing Platform (MISP) and the European CSIRT network, the last of which includes the participation of national bodies like the National Cybersecurity Centre (NCSC) and the Computer Emergency Response Team of the Ministry of Defence (DEFCERT).

   Throughout the whole cybersecurity system and within every element of the law enforcement process – from prevention to detection and from the initial response to investigation and prosecution – the Netherlands works with international partners. This includes providing mutual legal assistance in criminal cases. The majority of the organisations concerned have their own networks for that purpose. In the event of large-scale crises and incidents, the Netherlands can deploy its standard diplomatic instruments, complementary to regular and existing crisis structures, such as those associated with NATO and the EU Integrated Political Crisis Response (ICPR), in addition to the national handbook on decision-making in crises.

C. The Netherlands is committed to building and promoting an international legal and normative framework for cyberspace. Various ministries are focusing on this in international forums where international norms and standards are discussed. These norms and standards, which

relate to matters like internet governance, international peace and security, fighting cybercrime and protecting fundamental rights in cyberspace, can be technical or policy-related, and they can be voluntary or legally binding.

The relevant ministries – foreign affairs, economic affairs, security & justice, the interior & kingdom relations, and defence – make an active contribution to these efforts. The Public Prosecution Service, the police, the intelligence and security services, Defence Cyber Command and the NCSC are closely involved.

At the 2015 Global Conference on CyberSpace (GCCS), a Cyber Task Force based at the foreign ministry was launched to oversee diplomatic efforts in the digital domain. There is also a special envoy for international cyber policy, who represents the Netherlands abroad in matters related to cybersecurity. Parallel to its integrated approach to transnational crises, the Netherlands also uses diplomacy to achieve a variety of ends, including the creation of a normative framework for regulating cyber operations between states. This is necessary over the long term in order to devise systematic solutions. However, the development of this normative framework is a gradual process, and there are limits in terms of implementation and compliance. Moreover, this will not address all the threats facing the Netherlands, particularly in the short term. In light of this, we also need to develop capabilities to defend our security.

3.2 Cyber Defence & Security

For the Netherlands, maintaining the security of its networks in the face of threats posed by internationally operating criminals and by state and non-state actors is paramount. To protect its national security from foreign threats, the Netherlands is developing robust capabilities based on the objectives of early detection, active defence and, if necessary, intervention. The Netherlands seeks to build up these capabilities in an international context as well, with due regard for Dutch interests. The Netherlands must retain sufficient scope to carry out lawful, necessary and proportional cyber operations. As with the deployment of other types of force, when it comes to the deployment of offensive cyber capabilities, the Netherlands believes in exercising extreme restraint and only taking action if there is an adequate basis for such action in national or international law. This is also in line with NATO policy. Within NATO the government focuses on boosting the alliance's deterrence and collective defence. Because military, intelligence, investigative and cybersecurity capabilities are, in the 21st century, inextricably linked to internal and external networks, the Netherlands works both independently and with allies to develop offensive and defensive operational capabilities for a growing, secure and reliable cyber ecosystem. The DCC, NCSC, the intelligence and security services and other agencies are responsible for these efforts.

3.3 Capacity building

The digital gap between technologically advanced and less advanced countries must be closed so that all countries can profit from the opportunities created by global digitalisation. Capacity building within cyberspace is therefore vital. In the conclusions on cyber diplomacy issued by the Council of the European Union in 2015, cyber capacity building in non-member countries is described as a strategic building block of the evolving cyber diplomacy efforts of the EU towards the promotion and protection of human rights, rule of law, security, growth and development. In a broader international context, too, such as the World Summit on the Information Society (WSIS) and the 2015 report by the UN Group of Governmental Experts (UNGGE), there is a growing focus on capacity building. In the light of these developments the Netherlands launched the Global Forum on Cyber Expertise (GFCE) during the 2015 GCCS in The Hague. The establishment of the GFCE galvanised capacity building in the areas of cybercrime-fighting, cybersecurity, data protection and e-governance. The GFCE is a pragmatic, strategic and flexible platform for policymakers, professionals and experts from various countries, companies and international organisations. A variety of parties work together within the GFCE: government ministries, researchers, NGOs and the technology community. The Netherlands not only encourages other

states to embrace the vision of a free, open and secure internet; it provides capabilities for implementing this vision.

Capacity building serves to further both short- and long-term objectives that are important to the Netherlands. The aim is to raise the level of knowledge and expertise in non-EU countries to the highest possible level in order to strengthen the currently weak links in the worldwide infrastructure of the internet. In the short term, capacity building helps boost partner countries' digital resilience and supports their ability to profit from the economic advantages of the digital economy. In the long term, Dutch investment in capacity building will help cement strategic alliances aimed at supporting a free, open and secure internet and associated Dutch policy objectives.

3.4 Prospects for the further development of policy

To optimally respond to the opportunities and challenges that technological developments offer us, it is necessary to adopt an integrated approach to cyberspace.
To this end the government will enhance existing international cooperation and diplomacy. For example, it will activate a network of cyber diplomats, who will be responsible for promoting Dutch cyber policy, starting at a number of key embassies. This network will fall under the existing budget for the Ministry of Foreign Affairs.

The cyber diplomats will work from embassies and other representations to promote an open, free and security digital domain. Among other duties, they will act as liaisons for other governments and international organisations, provide information about trends and developments and offer substantive support for strategic priorities. To this end they will work with attachés from a number of ministries (security & justice, economic affairs, and defence), the business community, academics and NGOs. In the months and years ahead the government will look into options for further activating the cyber diplomat network.

The government will also consider how to strengthen long-term cooperation within the EU, a key issue during the Netherlands' Presidency of the Council of the EU in 2016. Some of the most important avenues in this regard are the Global Strategy for the European Union's Foreign and Security Policy, the EU's Cyber Security Strategy: An Open, Safe and Secure Cyberspace, the Directive on security of network and information systems (NIS) and the European Commission's Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry.

Key priorities are to boost the resilience of the EU and its member states with regard to critical infrastructure and building a stronger framework for the management of cyber crises. Another obvious next step is to further integrate cyber policy into the Common Foreign and Security Policy and explore options for consolidating our partnerships with the US, Canada, NATO and the OSCE. Within the EU as elsewhere, preference should be given to public-private partnership and the multi-stakeholder approach, wherever applicable. The EEAS, the EU missions in third states and the relevant departments of the European Commission can contribute to an effective international EU cyber policy.

4. Policy priorities of an international cyber strategy

The vision for the international cyber strategy has been fleshed out into the following policy priorities:
- Economic growth and sustainable development of the internet
- Effective internet governance
- Further enhancement of cybersecurity
- Effective efforts to stop cybercrime
- International peace, security and stability

- Rights and online freedom.

These policy priorities are explained below.

4.1 Economic growth and sustainable development of the internet

Over a third of our economic growth comes from digital commercial activities. As the digital gateway to Europe, the Netherlands aims to further bolster its position as a safe place to do business. This position is dependent on prerequisites like robust cybersecurity and respect for rights and freedoms in cyberspace.

In order to combat online abuse and Distributed Denial of Service (DDoS) attacks, discussions are ongoing in a number of international multi-stakeholder and multilateral forums about internet governance, open source standards and private best practices. The Netherlands plays an active role in this. We also take part in discussions and decision-making processes within the EU on issues like ICT standardisation, boosting the cybersecurity industry, achieving a level playing field and product certification.

Using the multi-stakeholder consultative model, the government must also establish frameworks and norms where necessary. The relationship between the government and businesses is dynamic. Businesses are important partners in safeguarding public interests like privacy, security and freedom in cyberspace. On the other hand, businesses can also have a negative influence, for example on account of their globally dominant market position. Given their key role in the digital domain, it is important to involve these businesses in the debate.

The central question at national level is: how can we ensure that online standards keep pace with technological developments? Working as a team creates a greater sense of urgency and helps disseminate knowledge more widely. One example of this philosophy is the Internet Standards Platform, which includes parties like the Dutch Internet Domain Foundation (SIDN), Réseaux IP Européens Network Coordination Centre (RIPE NCC), Internet Society – Netherlands Chapter (ISOC) and the government.

With regard to sensitive issues, unambiguous and future-proof legislation is needed in order to provide investment security for the international business community and maintain an attractive business climate. Examples of such issues include cybersecurity, privacy, encryption, data protection and storage (in both the public and private sectors), use of open data, net neutrality, digital authentication and identification and accountability for products and services.

To protect the Netherlands' knowledge economy and innovation position, the government is also committed to combating digital economic espionage. At national level the General Intelligence and Security Service (AIVD) and the Defence Intelligence and Security Service (MIVD) are responsible for investigating the threat. Wherever possible, findings are shared with the victims and other interested parties. At international level, existing partnerships and diplomatic efforts will be strengthened.

4.2 Effective internet governance

Governance of the internet is unlike conventional governance. No single private party, organisation or government authority exercises sole control over the internet or has the ability to substantially influence the workings of the internet. It is the government's aim to preserve internet governance in this unique and effective form. The internet is kept up and running by various actors: research institutes, standardisation and technical organisations, the business community, civil society, users' organisations and government agencies.

This multi-stakeholder consultative model also underpins the large degree of self-regulation and self-organisation within the internet. The guiding principles in this regard are bottom-up participation, openness and non-discrimination. In order to safeguard the freedom, openness and

security of the internet, internet governance must continue to rest with the multi-stakeholder internet community. Governments play an active role in this, but they do not impede the process by intervening unilaterally or multilaterally.

The extension of the mandate of the global Internet Governance Forum (IGF) by 10 years through UN General Assembly Resolution 70/125 of 16 December 2015 was a major milestone, a universal reaffirmation of support for the multi-stakeholder consultative model for internet governance. At the same time, this resolution urges parties to expedite the implementation of the recommendations of the UN working group from 2012 to improve the IGF. A key point in this regard is to involve developing countries more in the IGF and also to make the results of this global consultative platform more tangible and visible. The Netherlands is actively working on both these fronts.

The recent transition with regard to the Internet Assigned Numbers Authority (IANA), supported by the Netherlands, whereby ICANN acquired full oversight over the management of the domain name system (DNS), was a big step forward for internet governance. The task before us in the years ahead is to enhance ICANN's transparency and accountability structure and ensure its further internationalisation. The government is therefore pushing for a more active role on the part of the committee of national governments within ICANN, the Governmental Advisory Committee (GAC), which will continue to act in an advisory capacity.

The Netherlands has staked out its position within the internet governance debate by endorsing the outcome document of the 2014 NETmundial Conference, along with over 100 other countries, the business community, the technical internet community and the leading internet governance organisations. This document sets out the principles for internet governance, including internet freedom, respect for human rights and the further entrenchment of the multi-stakeholder consultative model.

Given the global public interests associated with the internet, the government is also working to ensure the recognition of the core of the internet as an international public good. The Netherlands recognises that, given the nature and dependence of cyberspace, it is necessary to exercise restraint when engaging in activities that can affect that public core. The Netherlands is working on developing and promoting the acceptance of international norms and rules of conduct, and to that end it has submitted a proposal to the United Nations Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security.

4.3 Further enhancement of cybersecurity

Security, freedom and social growth exist in a dynamic balance. It is not possible to guarantee an open and free digital domain without security. With that in mind the government is actively working to promote and enhance cybersecurity – bilaterally, regionally and multilaterally. In this way, both the Netherlands and the digital domain can be kept safe and secure.

As the CSBN has noted in its annual reports, the cyber threat posed by states, criminals and non-state actors to the Netherlands' political, economic and social interests is real and growing. The government has therefore been working for some time on enhancing security in cyberspace, as stated in the strategic objectives laid down in NCSS 2. These objectives, which also apply internationally, include boosting resilience to cyberattacks and protecting vital interests in cyberspace; public-private partnership; detection, response and awareness-raising; and education. The Netherlands also endeavours to lend its guidance to relevant initiatives at international level, given that cyberspace has no borders and security can only be achieved through joint efforts to address the weakest links.

4.3.1 Enhancing digital security in Europe

At international level, the government pursues an integrated approach to cybersecurity. It does so through a combination of developing domestic cybersecurity strategies, working towards technologically neutral European legislation and promoting public-private partnership. Particular attention is paid to vital sectors and infrastructure and to the promotion of a level playing field. These efforts mainly take place within the EU, but the focus is also increasingly widening to include other bilateral and multilateral spheres. The entry into force of the NIS Directive is a major step forward, and the Netherlands has been one of its chief advocates.

The 'Cooperation Group' was set up in order to support and facilitate strategic cooperation and information-sharing between EU member states, to foster trust and to create a high joint level of security for network and information systems in the Union. It is the government's aim to use its involvement in this group to oversee, at strategic level, the enhancement of digital security for Europe. The Commission's recent Communication on the enhancement of cybersecurity systems and the cybersecurity sector is a major milestone for European cooperation. At both strategic and political level the Netherlands actively works to raise awareness, cultivate mutual understanding and assign responsibility.

4.3.2 Operational activities and cooperation on cybersecurity

At international level, the Netherlands works closely with its partners on the operational front. Collaborating on operational issues contributes to a robust exchange of information and knowledge, incident management, resilience and recovery capabilities. This cooperation mainly takes place through established networks, such as the Computer Security Incident Response Teams (CSIRTs) or CERTs. The Dutch intelligence and security services also have a part to play on this front, in both bilateral and multilateral settings. The Netherlands is a prominent actor in this international arena. Operational collaboration also benefits security, freedom and social growth in both the private and public domain. To promote trust and operational collaboration between CSIRTs within the EU, a CSIRT network was established with the entry into force of the NIS Directive. The Netherlands is making a particular effort to help put this network into operation and make it a success.

4.3.3 Stimulating research on cybersecurity

The National Cyber Security Research Agenda (NCSRA) serves as the basis for short- and long-term research, both domestically and internationally. The issues in question dovetail with NCSS 2; both possess the overarching goal of expanding cybersecurity knowledge and know-how and investing in ICT innovation to achieve our cybersecurity objectives.

In this connection, collaborative cybersecurity research is also undertaken by the Netherlands Organisation for Scientific Research (NWO) and the US Department of Homeland Security (DHS).

4.4 Effective efforts to stop cybercrime

Cybercriminals are employing ever more advanced methods and becoming more organised. As a result, the amount of damage caused by their actions is growing. These developments are magnified by the relatively low cost and risk of committing acts of crime and espionage in cyberspace. The costs and risks associated with conventional – physical – forms of crime are often higher and the proceeds lower.

The government has a duty to uphold the rule of law, in both the real and virtual worlds. The customary system of international legal assistance is very slow, however, in comparison to the methods used by criminals to avoid detection (e.g. re-routing their activities through different countries and rapidly moving their data from one country to the next). Moreover, criminals will often make a point of choosing to operate from countries where legislation and/or capabilities are insufficient to tackle cybercrime. As a result there is a danger that cyberspace could become a haven for 'tech savvy' criminals. To promote international investigative efforts in cyberspace, the Netherlands is working to step up international cooperation and strengthen international legal frameworks. The Netherlands put these matters on the agenda of the 2015 GCCS and raised them

again during its EU Presidency. Building capacity and strengthening legal frameworks in other countries is also a key issue. Such efforts will be supported with capacity-building projects conducted as part of the Convention on Cybercrime under the aegis of the Council of Europe.

4.4.1 International cooperation on investigations related to cyberspace

Fighting cybercrime places new demands on the police, the criminal justice authorities and private parties, especially in terms of their ability to take swift action and share information. In June 2016 the Justice and Home Affairs (JHA) Council adopted Conclusions about creating a European network of public prosecutors, with the support of Eurojust, and on options for a shared EU platform for sharing information on electronic evidence. Council Conclusions have also been adopted on jurisdiction in cyberspace, which also entail enhancing legal assistance procedures. In addition, the Standing Committee on Operational Cooperation on Internal Security (COSI) has adopted recommendations for enhancing operational collaboration, on the basis of actual experiences. The Netherlands has also contributed to the development of the European Cybercrime Centre at Europol, and it supports the INTERPOL Global Complex for Innovation (IGCI) in Singapore. One of the reasons the IGCI was established is to enhance support for global international cooperation in cybercrime cases.

4.4.2 Fortifying options for conducting investigations in cyberspace

Trends in the digital domain demand a reconsideration of international legal frameworks. Particularly in situations where data related to criminal offences is being rapidly moved or where the physical location of data cannot be determined by reasonable means, the traditional instruments used in international investigations are inadequate. During the Netherlands' EU Presidency, the JHA Council adopted Conclusions requesting the European Commission to develop proposals to enhance cooperation with private partners in other countries. The Conclusions also asked the Commission to explore different premises other than territoriality that could underlie enforcement jurisdiction and whether certain investigative powers could be used irrespective of territorial borders.

The Netherlands also promotes the importance of the wider ratification of the Council of Europe's Convention on Cybercrime. Finally, the Netherlands is in favour of developing an Additional Protocol to the Convention which would usher in new possibilities for the international investigation of cybercrime.

4.5 International peace, security and stability

In cyberspace we appear to be witnessing a growth in distrust and a danger of escalation and miscalculation. Defensive measures taken by one state can be interpreted by other states as a threat. This can lead to international instability, with the attendant risk of a possible arms race. In order to keep this situation manageable, defend identified international security interests and address the threat posed by state actors, the 3D approach (defence, diplomacy and development), which had already been noted in NCSS 2, will be developed further. The guiding principle in this regard is that cyber operations by state actors are ultimately merely a means to achieve broader geopolitical and economic objectives. Therefore, influencing the conduct of state actors is also a key element of this policy priority, alongside boosting national and international digital resilience.

4.5.1 Military capabilities

Because military capabilities are, in the 21st century, inextricably linked to networks, the Netherlands works with trusted partners to develop offensive and defensive operational capabilities for a growing, secure and reliable cyber ecosystem. For the Dutch government, maintaining the security of its networks from internationally operating state and non-state actors is paramount. With due regard for national law and international agreements, the government seeks to build resilient national networks and foster the development of internationally credible intervention capabilities. These measures are intended to serve as a deterrent to any hostile or criminal actors.

Within its borders the Netherlands attaches importance to a culture and ecosystem in which public and private parties jointly pursue a secure digital domain. Key elements of this outlook are the ability to provide an adequate response and a timely recovery of the system's integrity, availability and confidentiality. In the international arena the Netherlands pursues robust and credible capabilities, on its own and in collaboration with allies, based on the principle of early detection, active defence and – if necessary – intervention.

To protect its domestic and international security interests, the Netherlands also plays a leading role in bolstering NATO's strong collective defence in cyberspace. At the 2016 Warsaw summit, NATO recognised cyberspace as a separate domain, so that cyber aspects could henceforth be factored into the entire operational process. Not only is a secure operational process important; it should also be remembered that the alliance's cyber defence is only as strong as its weakest link. By taking the Cyber Defence Pledge, all allies have made a political statement committing themselves to further enhancing the domestic cyber defence of national networks and infrastructure.

4.5.2 International justice, standards of conduct and confidence-building measures

Over the medium term the government will seek to establish an international normative framework for the regulation of cyber operations between states. The framework will largely take its cue from existing international law. Clarifying the applicability of international law to cyber operations is the Netherlands' most important priority in this area. As a small country the Netherlands benefits from a well-functioning international legal order that provides a measure of predictability, stability and conflict prevention. By means of the Hague Process and on the basis of the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, the Netherlands supports a more inclusive and detailed debate on the application of international law to cyber operations. The government is also pushing for international agreements on non-binding, voluntary standards of conduct for states and for confidence-building measures. In this way the Netherlands contributes to the development of an international security architecture for cyberspace, which will make the security dilemma more manageable. This security architecture will lead to increased stability and reduces the risk of escalation, miscommunication and miscalculation. To this end the Netherlands will launch a Global Commission on the Stability of Cyberspace, a multi-stakeholder platform which will facilitate a global discussion on new voluntary standards of conduct in cyberspace.

4.5.3 Transparency regarding offensive military cyber capabilities

The government is transparent about the Netherlands' aim to develop military cyber capabilities. Internationally, the Netherlands is also pushing for greater transparency on the part of other countries in this area – not in terms of the nature of the capabilities, but rather with regard to the goals the capabilities are meant to achieve, the legal framework that governs their use, and the political control and democratic oversight that applies to their deployment. Transparency on this front serves as a confidence-building measure that can help prevent misunderstandings and reduce distrust. This, in turn, can help promote international stability, prevent the start of an arms race and eliminate distrust and the danger of escalation and miscalculation.

4.5.4 Export controls and the EU Dual-Use Regulation

In order to safeguard international security and human rights, the government will push for either a ban on or a mandatory export licence for specific hardware, software and technology. These items are set down in the lists of controlled goods agreed within the Wassenaar Arrangement. These lists are fully incorporated into the relevant piece of European legislation, the Dual-Use Regulation, which deals with monitoring trade in goods that have both civilian and military applications. An example of this is 'intrusion software', which can be used by authoritarian regimes to restrict civil rights.

The government is in favour of expanding existing controls on devices for smart surveillance for reasons relating to human rights. On the other hand the government is highly critical of the

proposal by the European Commission to amend the Dual-Use Regulation by adding a new category of goods to the control list. This approach can lead to overlapping or even contradictory regulations. What is more, it disrupts the level playing field at global level, to the disadvantage of European industry, since the autonomous control list only applies to the EU.

4.5.5 Capacity building

To address existing threats and take full advantage of the opportunities that digitisation offers our international community and economy, the government is committed to capacity building. The aim of capacity building is to promote a basic level of cybersecurity around the world and in Europe in particular. To this end the Netherlands shares knowledge, best practices and training in the field of cybersecurity. For example, we stress the importance of Coordinated Vulnerability Disclosure (CVD) in European and international platforms, including the EU and GFCE. The government is also keen to promote CSIRT capabilities ('CSIRT maturity'). The Netherlands also contributes to capacity building for the benefit of actors in the field of security and human rights online. It contributes to digitalisation processes and applications at country level, and in terms of society the Netherlands supports projects that use digital technologies as a catalyst for sustainable development. Over the long term such efforts help cement strategic alliances aimed at fostering a free, open and secure digital domain.

4.6 Rights and internet freedom

4.6.1 Fundamental rights and freedoms online

To maintain and advocate fundamental rights and freedoms internationally, the government pursues a policy on human rights that includes an international cyber component. Respect for human rights is the basis for an open, free and secure society. The protection of personal data and privacy, freedom of expression, the right to seek information, freedom of association and assembly, and the prohibition on discrimination are under increasing pressure from some governments, which use national security as a pretext for disproportional intrusions. The Netherlands regards security and freedom as complementary, rather than conflicting, interests: a safe, secure society is a society in which the fundamental rights and freedoms of the individual are protected. The government champions this human-rights-inclusive vision abroad in order to further the dialogue on it.

In international forums and multi-stakeholder platforms, the Netherlands works to achieve greater recognition and safeguards for fundamental rights online. This recognition is vital to offset negative trends that are putting pressure on internet freedom in a growing number of countries. In order to reverse such trends, all interested parties around the world need to work together. Countries need to learn from and share each other's best practices.

Better diplomatic coordination is vital to keeping the internet open and free at a time when more and more states are seeking to create a 'national' internet. The Netherlands seeks to encourage the involvement of companies, NGOs, the technology community and academia.

4.6.2 The right to personal data protection and the right to privacy

To ensure the protection and recognition of the right to personal data protection and the right to privacy, the government is supporting relevant initiatives in various multilateral forums. It is vital that the right to the protection of personal data and respect for privacy are also protected and recognised in a digital context. The Netherlands will therefore continue to form coalitions with like-minded countries on this matter.

In early 2016 the government presented its position on the issue of encryption. It is the task of the government to safeguard the Netherlands' security and investigate criminal offences. In this connection the government underscores the need for lawful access to data and communication. Moreover, public authorities, businesses and individuals benefit from having the most secure possible digital systems. The government endorses the importance of strong encryption for online security as a way of protecting individual privacy, enabling confidential communication on the part

of the public and private sectors, and helping the Dutch economy. At the same time security considerations also play a key role. The government believes that at the present time it is not advisable to enact restrictive statutory measures with regard to the development, availability and use of encryption within the Netherlands. In its official position on this issue, the government stresses that the Netherlands will promote this conclusion and the considerations underlying it in an international context.

To guarantee trust in data and privacy protection, the government is committed to international standardisation and legal certainty vis-à-vis the transfer of data. International legal frameworks are necessary when data is exchanged with countries that have less rigorous standards than the EU. International standardisation helps create a level playing field for companies, but we should not let the lowest common denominator be our point of departure. Ultimately, good data protection is in the interests of individuals, the government and the business community.