The Netherlands Cybersecurity Strategy at a glance

People and businesses should be able to benefit fully from participation in the digital society. Security is an essential part of this. Our economy, democracy and society depend on the security and reliability of digital products and connections. This dependency is only going to increase in future, so investment in cybersecurity is an investment in our future. In producing the Netherlands Cybersecurity Strategy 2022-2028, the government is working towards a future in which our cyber resilience can always keep pace with any cyber threats we face. To achieve that vision, we have formulated a series of aims on the basis of four pillars.

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 of 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.

The government is therefore investing in strengthening and transforming the digital ecosystem so that no single organisation or individual can be the weakest link any more. The government's efforts will be based on the following five priorities:

1. Be more aware of cyber threats so that we know and understand them.

In order to determine how and where our cyber resilience needs strengthening, it is essential to have a clearer picture of the origin of threats and of the specific interests being threatened.

- Invest in intelligence and security services, and in defence organisation

2. Ensure sufficient cyber expertise is available on the labour market so that we can meet the challenges we face.

There is currently a major shortage of such expertise, which is being felt by our businesses, knowledge institutions and government organisations. Specific measures are needed to bring more ICT specialists to the labour market.

- Incorporate digital security in the national curriculum for primary and secondary education
- Invest in higher education courses, and in refresher/retraining programmes

3. Be aware of and understand risks and threats.

The risks associated with digital vulnerabilities and cyber threats must, as much as possible, be borne by the developers and suppliers of digital products and services. However, there will almost always be residual risks, making it necessary for consumers or SMEs to take their own precautions. In order to be able to take such precautions, they must first be aware of the risks, and of the measures they need to take.

- Organise awareness-raising campaigns and education
- Organise clear points of contact where the public and businesses can obtain information
- Notify victims and/or targets promptly

4. Legislation to ensure that frameworks are clear and verifiable.

At present, many of the cybersecurity measures taken by businesses are based on voluntary guidelines and frameworks. For certain organisations, the risks to business continuity are such that we cannot run the risk of failing to prioritise digital security. Voluntary guidelines are no longer enough: legal frameworks are needed for these organisations. In addition, security needs to be made a prerequisite in the development and provision of digital products and services.

- Expand statutory rules and supervision of national and subnational public authorities and critical entities and sectors (NIS2, Digital Government Act, etc.).
- Use European legislation (Cyber Resilience Act) to ensure the security of hardware and software.
- Strengthen supervision and step up political-administrative oversight of measurable effects and results.

5. Review of national cybersecurity system to ensure effective and efficient use of cyber capabilities.

A key element of the Netherlands' cyber resilience is the timely sharing of information on cyber threats and vulnerabilities in a way that matches an organisation's level of maturity, so that the organisation in question can take appropriate measures. To achieve this, the available capabilities and expertise must be used as effectively as possible.

- Merge the NCSC, DTC and CSIRT-DSP to form a single national cybersecurity authority.
- Assess the other organisations within the cybersecurity information-sharing system in terms of which of their tasks should be centralised (within the national cybersecurity authority) and which should be sector-based.
- Introduce legislative changes to promote information sharing within the system.
- The government will therefore start developing a public-private platform for sharing knowledge and information.