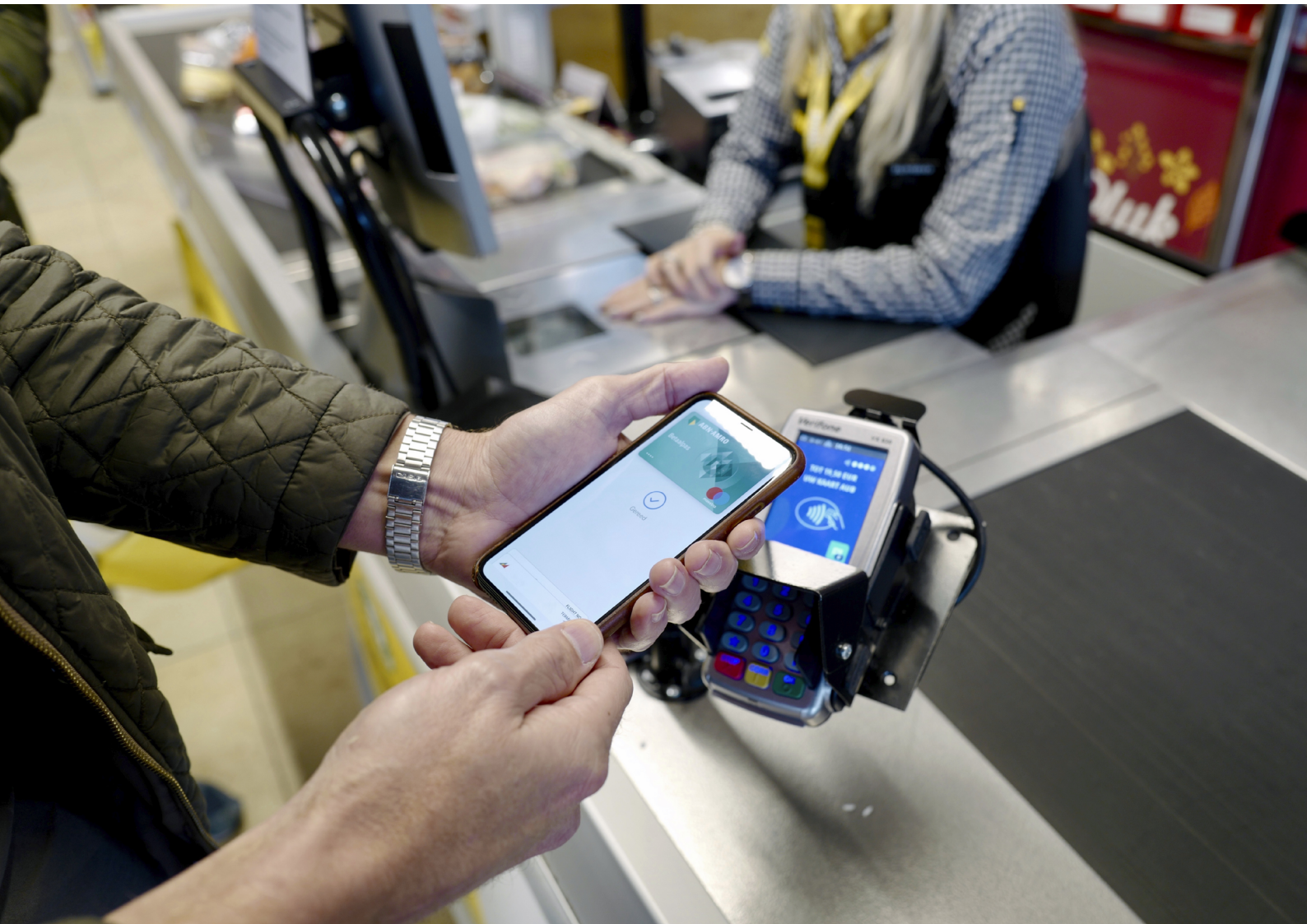
Action plan
Netherlands Cybersecurity Strategy 2022-2028

Ambitions and actions for a digitally secure society



Cover photo: We are using cash less and less frequently. These days, 81% of payments at the checkout are contactless. That makes it all the more important that our payment transactions remain secure.

The Netherlands Cybersecurity Strategy (NLCS) has been produced with the involvement of a wide range of public, private and civil society organisations, coordinated by the National Coordinator for Counterterrorism and Security (NCTV). The Cybersecurity Assessment for the Netherlands (CSBN) forms the basis for the pillars and aims of the NLCS.

Action plan
Netherlands Cybersecurity Strategy 2022-2028

Ambitions and actions for a digitally secure society

Table of contents

Pillar I

Digital Cyber resilience of the government, businesses and civil society organisations

Pillar II

Secure and innovative digital products and services

Pillar III

Countering threats posed by states and criminals

Pillar IV

Cybersecurity labour market, education and cyber resilience of the public

Digitalisation is an important step towards ensuring healthcare remains accessible for everyone and reducing pressure on healthcare professionals.

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

Aim 1: Organisations have a clear picture of cyber incidents, threats and risks and know how to deal with them

Review of the cybersecurity ecosystem

Action summary	Timeline	Owner / Involved
The NCSC, DTC and CSIRT-DSP will be merged into a single national cybersecurity authority (CSIRT).	2022 - 2026	Owner: J&V, EZK Involved: NCSC, DTC, CSIRT-DSP
For government organisations in the cybersecurity information-sharing ecosystem, we will explore which tasks could be centralised (with the national cybersecurity authority) and which should be sector-based.	2022 - 2023	Owner: J&V, EZK Involved: VWS, BZK, DEF, OCW, I&W
A roadmap will be drawn up with the business sector for the implementation of a public-private platform for reciprocal cybersecurity information and knowledge sharing. The basis for this programme is the Cyclotron report.	2022 - 2023	Owner: J&V Involved: NCSC, DTC, AIVD, MIVD, police, Public Prosecution Service, private partners, local and regional authorities
The NCSC and its partners will explore the feasibility of a central national campus to promote cooperation, information sharing, knowledge development and research between public and private stakeholders.	2022 - 2023	Owner: J&V Involved: NCSC, DTC, AIVD, MIVD, police

Strengthen the Nationwide Network of Cybersecurity Partnerships (LDS)

Action summary
The legal framework will be modified to enable organisations in the LDS to share cybersecurity information with each other more widely, more efficiently and more effectively. Examples include the forth-coming amendment of the Network and Information Systems (Security) Act (WBNI), which will be debated in the House of Representatives this autumn and the parliamentary bill on promoting cyber resilience in the business sector.

Timeline
2022 - 2026

Owner
J&V, EZK

Involved
NCSC, DTC

Action summary
Requirements for joining the LDS will be drawn up at interministerial level. They will be binding for government organisations while providing guidance for private organisations. Private partners will be involved in developing these guidelines.

Timeline
2023 - 2024

Owner
J&V

Involved
EZK, VWS, I&W, DTC, NCSC

Action summary
The government will support organisations in the information security chains, which will enable them to secure sustainable funding.

Timeline
2023 - 2026

Owner
J&V

Involved
NCSC, DTC

Action summary
A LDS communications plan will be issued to guide organisations within the system. Part of this will involve establishing clear points of contact.

Timeline
2023 - 2025

Owner
J&V

Involved
BZK, EZK, NCSC, DTC

Expand organisations within the LDS

Action summary
An LDS building plan will be drawn up in collaboration with private partners to enable the government to work with the business sector to increase the coverage of the LDS. As part of this building plan, an overview of the current state of the LDS will generate insight into initiatives that have already been developed and the gaps that currently exist in the LDS.

Timeline
2022 - 2026

Owner
J&V

Involved
EZK, OCW, VWS, I&W, BZK, NCSC, DTC, subnational authorities and private partners

---

Action summary
With the aid of a financial contribution from the Ministry of the Interior and Kingdom Relations (BZK) and coordinated by the Association of Provincial Authorities (IPO), provinces will continue setting up an interprovincial information hub as a connectingorganisation within the LDS.

Timeline
2022 - 2023

Owner
BZK

Involved
IPO

Action summary
The Ministry of Education, Culture and Science (OCW) will set up a CERT for primary and secondary education.

Timeline
2022 - 2023

Owner
OCW

Involved
OCW and SURFcert

Action summary
The Ministry of Infrastructure and Water Management (I&W) will strengthen the CERT Water Management.

Timeline
2022 - 2023

Owner
I&W

Involved
RWS

National Detection Network (NDN)

Action summary	Timeline	Owner
All central government organisations not yet connected to the National Detection Network will be added.	2023	BZK Involved J&V, CIO-Rijk, NCSC

Action summary	Timeline	Owner
Collaboration and information-sharing between the partners in the NDN (AIVD, MIVD, NCSC) and service provision for affiliated organisations will be strengthened through enhanced knowledge-sharing.	2023 - 2026	J&V Involved AIVD, MIVD, NCSC, CIO-Rijk

Victim notification

Action summary	Timeline	Owner
Research will be conducted to determine how businesses and the public who are at risk of being targeted or who are victims of cyber incidents can best be informed. The NCTV and NCSC will look specifically at what form victim notification from a non-criminal-investigation source could take.	2022 - 2023	J&V Involved NCSC, AIVD, MIVD, private partners

Action summary	Timeline	Owner
The police and the Public Prosecution Service (OM) will explore how best to proceed with the notification of victims revealed by criminal investigations.	2022 - 2025	J&V Involved OM, Police, NCTV, NCSC

Aim 2: Organisations are properly protected against cybersecurity risks and are mindful of their own importance to the sector and other organisations in the chain

Cyber resilience of critical infrastructure

Action summary	Timeline	Owner
The revised EU Network and Information Security Directive (NIS2) will be implemented in the Netherlands via the WBNI in 2024.	2022 - 2024	J&V Involved OCW, BZK, I&W, VWS, FIN, EZK, LNV, MIVD, AIVD and NCSC

Action summary	Timeline	Owner
To minimise the burden on businesses, the implementation of sectoral legislation, such as the DORA and the Network Code, and related legislation, such as the CER Directive, will be closely coordinated with the implementation of NIS2.	2022 - 2024	J&V Involved FIN, EZK, OCW, BZK, I&W, VWS and LNV

Action summary	Timeline	Owner
In 2023, the government will start extensive public information campaigns to inform organisations falling within the scope of the new legislation of their rights and obligations, and to actively guide them through the implementation process.	2023 - 2024	J&V Involved OCW, BZK, I&W, VWS, FIN, EZK and LNV

Action summary	Timeline	Owner
To ensure quality and consistency in the monitoring of the WBNI after the implementation of NIS2, the 'Coordinated inspection framework of cybersecurity of critical processes' and related governance will be developed further. This will ensure cohesion in and transparency about the information-driven and risk-based monitoring approach.	2022 - 2024	J&V Involved OCW, BZK, I&W, VWS, FIN, EZK and LNV

Action summary	Timeline	Owner
Explore the possibility of setting up a central hotline whereby NIS2 notifications can be made easily and simultaneously to the CSIRT and the supervisory authority. This exploration will also encompass notifications under related legislation (GDPR, DORA, Net-work Code).	2022 - 2024	J&V Involved OCW, BZK, I&W, VWS, FIN, EZK and LNV

Action summary	Timeline	Owner
Evaluate the current method used to determine thresholds for mandatory reporting of cyber incidents under the WBNI. These findings will in any event be taken into account when determining thresholds for newly designated suppliers.	2022 - 2024	J&V Involved OCW, BZK, I&W, VWS, FIN, EZK and LNV

Action summary	Timeline	Owner
Given the increase in the number of target group organisations, the NCSC will produce and implement scalable technologies for digital and automated information-sharing with and among target groups and partners.	2022 - 2024	J&V Involved NCSC

Action summary	Timeline	Owner
The NIS2 requirements intersect with the Government Information Security Baseline (BIO) and will be incorporated into it where applicable, so as to retain a recognisable connection with the security baseline for the government.	2022 - 2024	BZK Involved

Action summary	Timeline	Owner
A start will be made on exploring the steps necessary to boost the cyber resilience of critical infrastructure in the Caribbean Netherlands.	2022 - 2024	J&V Involved BZK

Action summary	Timeline	Owner
The government will launch an enhanced strategy to bolster the protection of the Netherlands' critical infrastructure. This will include a review of critical infrastructure policy and the related legislation, partly in the light of the CER and NIS2 directives. Critical suppliers will be consulted about the new system in early 2023. The enhanced strategy will also provide for structural partnerships with some of the critical sectors, an enhanced policy instrument to gain a better picture of sectoral risks and dependencies, and the further development of information-sharing on vulnerabilities and threats. Cybersecurity is an integral part of this.	2022 - 2024	J&V Involved OCW, BZK, I&W, VWS, FIN, EZK, LNV, NCSC, AIVD and MIVD

Cyber resilience of small and medium-sized enterprises (SMEs) and the wider business sector

Action summary	Timeline	Owner
NCSC and DTC will develop new products and services, focusing on issues such as the embedding of cybersecurity in the risk management process, crisis preparation, incident response and thematic advice. All these differentiated and data-driven information-and-knowledge products and services will be made easily accessible in a manner appropriate to an organisation's level of maturity.	2022 - 2024	J&V, EZK Involved NCSC, DTC

Action summary	Timeline	Owner
Produce first version of central registers for cybersecurity-related information (i.e. type of ransomware, vulnerabilities).	2023	J&V Involved NCSC

Action summary	Timeline	Owner
Encourage SMEs to use tools, such as risk scans, and products and security recommendations, including possible courses of action. This could be achieved via trade associations, for example through the public-private platform *Samen Digitaal Veilig (Digitally Safe Together)*.	2022 - 2024	J&V Involved DTC, NCSC, VNO-NCW, MKB-Nederland

Action summary	Timeline	Owner
The government will produce a single set of basic measures and promote it for use by organisations on a voluntary basis.	2023 - 2024	J&V Involved EZK, BZK, NCSC, DTC, AIVD, MIVD

Cyber resilience in education

Action summary	Timeline	Owner
A set of standards for information security and privacy will be implemented for primary and secondary education, to include periodic checks and benchmarks to monitor whether school boards are complying with the norm.	2022 - 2024	OCW

Action summary	Timeline	Owner
School boards in primary and secondary education are required to focus specifically on information security and privacy in their annual reports.	2022 - 2024	OCW

Action summary	Timeline	Owner
Efforts will be made in primary and secondary education, secondary vocational and higher education to raise awareness of cyber risks and measures among students, staff and management by means of campaigns, crisis exercises and special working groups.	2022 - 2024	OCW

Action summary	Timeline	Owner
For their audits, institutions in secondary and higher education will use the Royal Netherlands Institute of Chartered Accountants (NBA) maturity model and SURF's derived Information Security Assessment Framework for Higher Education.	2022 - 2024	OCW Involved SURF

Cyber resilience of healthcare institutions

Action summary	Timeline	Owner
A revised version of NEN 7510[1] will be published. Implementation tools will also be developed to help improve the implementation rate of NEN 7510.	2025	VWS

Action summary	Timeline	Owner
The vulnerability analysis tool KAT has been made available as an open-source resource so that all healthcare organisations can use it to scan actively for vulnerabilities in their own systems. The Ministry of Health, Welfare and Sport (VWS) and Z-CERT are encouraging organisations to do this systematically. The tool will also be made more widely available.	2022 - 2023	VWS Involved Z-CERT

Action summary	Timeline	Owner
Incident support within the healthcare sector will be expanded by the phased incorporation of new subsectors in the scope of Z-CERT's services. Primary care sectors, such as general practitioners and pharmacies, will join before 2023. In the course of 2023 and 2024, the following sectors will be incorporated: disability care, nursing, social and home care, and rehabilitation care.	2023 - 2024	VWS Involved Z-CERT

Action summary	Timeline	Owner
The programme *Informatie veilig gedrag in de zorg* (information security behaviour in the healthcare sector) provides healthcare institutions with ways to promote the secure handling of information.	2022 - 2023	VWS Involved ECP, Z-CERT

1 An information-security standard for the healthcare sector in the Netherlands.
Under the Processing of Personal Data in Healthcare (Supplementary Provisions) Act, care providers must comply with NEN 7510.

Action summary	Timeline	Owner
In the context of prevention and detection, Z-CERT will organise exercise and test activities with affiliated healthcare institutions and develop best practices in relation to the care-sector-specific nformation-security standard NEN 7510.	2023	VWS Involved Z-CERT

Cyber resilience of the infrastructure and water management sectors

Action summary	Timeline	Owner
Strengthening the cyber resilience of sectors for which the Ministry of Infrastructure and Water Management (I&W) bears responsibility, such as drinking water, water quantity control and management, aviation, maritime, nuclear, railways and positioning and timing Global Navigation Satellite System (GNSS), by: • Organising administrative consultations with sectors to exchange knowledge and experience and to discuss how to collaborate in order to manage cyber risks; • Developing sectoral knowledge products, such as periodic cybersecurity threat assessments by sector, which contribute to integrated risk management; countering ransomware and under-standing supply chain risks; • Facilitating organisations in terms of education, testing, training and exercises so that they are better able to mount a swift response to and recover from cyber incidents, in accordance with sector requirements.	2022 - 2026	I&W Involved NCSC, AIVD, MIVD, Water Management CERT

Cyber resilience in central government

Action summary
The Ministry of the Interior and Kingdom Relations' ambition in this area is set out in the Central Government Information Strategy and the roadmaps presented to the House of Representatives on 15 July 2022.[2] Examples of concrete actions are as follows:

- A start will be made in 2022 on the triple-track red-teaming project approach: risk-based testing, knowledge-sharing (within central government) and follow-up on findings.
- There will be mandatory basic cyber resilience training for central government staff from 2024.
- With the help of CIO-Rijk, parallel efforts will be made to pursue policy for a number of activities: handbooks to accompany the government-wide cloud policy (which was revised in August 2022), tackling risks in quantum computing, government-wide provisions for highly classified information and reinforcing the Central Government system of Security Operation Centres (SOCs).
- Alongside dcypher, the government-wide Information Partnership programme will focus on cooperation between central government and higher education in ICT, including cybersecurity. One element of this is the *I-doctoraatsprogramma*, a course run at university and higher professional education level, which supplies knowledge workers and, through research and innovation, helps to strengthen central government's knowledge basis and tackle the cyber challenges it faces.

Timeline
2022- 2025

Owner
BZK

Involved
NCSC, Central Government CIOs, AIVD, MIVD

2 Letter to the House of Representatives on the Central Government Information Strategy 2022-2025 roadmaps | Parliamentary paper | Rijksoverheid.nl

Cyber resilience in the public sector

Action summary
An administrative agreement on cyber-security will be drawn up with the Association of Netherlands Municipalities (VNG) in which the joint approach by municipalities in the field of cybersecurity will be elaborated further.

Timeline
2022

Owner
BZK

Involved
VNG

Action summary
2023 will see the continued development and monitoring of the Government Information Security Baseline (BIO), including its legal embedding in the Digital Government Act.

Timeline
2023

Owner
BZK

Action summary
The Centre for Information Security and Privacy (CIP) will extend and update the implementation of the BIO support programme for the government as a whole, thus providing assistance for organisations in the implementation and application of the BIO.

Timeline
2022 - 2027

Owner
BZK

Involved
CIP

Action summary
The CIP will extend and update the expansion and development of the Information Security and Privacy service. Public authorities will receive tailored advice from government experts about cybersecurity and privacy. Organisations with insufficient knowledge about information security will thus be assisted at the appropriate level by organisations with specific expertise.

Timeline
2022 - 2027

Owner
BZK

Involved
CIP

Action summary	Timeline	Owner
Further development of the ENSIA accountability system, the single information audit unified norm. By organising supervision horizontally and vertically with the BIO as a basis, municipalities are working towards better information security and facilitating democratic accountability in respect of information security.	2022 - 2025	BZK Involved VNG

Cyber resilience of sectors with operational technology and process automation systems

Action summary	Timeline	Owner
Efforts to increase the security of industrial automation and control systems (IACS) are being given a boost by means of a new coalition. Examples of actions taken within the coalition include: • Developing and implementing a significant and realistic IACS component in national exercises and training. • Strengthen knowledge creation and developing instruments such as handbooks and best practices to help public and private organisations implement the right measures for IACS and define and address the right risks. • Sharing these knowledge products and instruments via a collective IACS knowledge hub.	2022 - 2024	I&W Involved NCSC, EZK, (private) partners

Insight into cyber resilience of the public sector and business community

Action summary	Timeline	Owner
Pilots will be conducted to examine the added value of an IT report and an IT audit statement in the public sector. This will be similar to the usual annual financial report. The study will tie in with pilots conducted in the business sector.	2023	BZK Involved ADR

Action summary	Timeline	Owner
A system is being set up in collaboration with the wider cybersecurity field to monitor the Netherlands' cyber resilience. The first report is expected in 2024.	2024 - 2026	J&V Involved BZK, EZK, NCSC, DTC

Action summary	Timeline	Owner
The CIP will manage and develop the basisbeveiliging.nl website, where public sector organisations' security scores will be calculated on the basis of various indicators and displayed.	2023	BZK Involved CIP

Action summary	Timeline	Owner
In the context of the Corporate Governance Code, discussions will be held with the business sector on what sort of collaboration could be put in place to manage cybersecurity risks in listed companies.	2022	EZK

Action summary	Timeline	Owner
We will work with insurers to explore what role they could play in relation to consequential damages resulting from cyber incidents.	2022 - 2023	J&V Involved EZK, FIN

Aim 3: Organisations respond to, and recover and learn from, cyber incidents and crises swiftly and efficiently

Incident and crisis preparation

Action summary	Timeline	Owner
The updated National Crisis Plan for Digital Incidents (LCP-*Digitaal*) will be launched and put to use. This plan forms the basis for dealing with a cyber crisis.	2022	J&V Involved LCP partners

Action summary	Timeline	Owner
Individual ministries will ensure that their crisis plans are in line with the LCP-*Digitaal*, and can show that incident, continuity and recovery plans have been tested by means of, for example, a training exercise or an audit. Ministries will also follow up on training and other evaluations and findings.	2022 - 2024	J&V Involved Ministries

Action summary	Timeline	Owner
As a complement to LCP-*Digitaal*, consideration will be given to whether the current statutory crisis instruments (including emergency legislation) for dealing with national crises are sufficient for crises involving cyber elements. In this connection, we will consider introducing a ranking system.	2022 - 2024	J&V

Action summary	Timeline	Owner
Relevant regional crisis plans will be aligned with the LCP-*Digitaal*.	2022 - 2023	J&V Involved Safety regions

Action summary	Timeline	Owner
The Netherlands will take an active role in the ongoing development of international crisis networks.	2022 - 2026	J&V Involved DEF, BZ

Action summary	Timeline	Owner
Continue developing the National Response Network (NRN) into a national incident-response network, for instance by providing Defence cyber capabilities for military assistance and support. Enhance efforts through strategic secondment of cyber experts between central and subnational government organisations. Extend public-private partnerships. Identify existing response capability..	2022 - 2025	J&V, DEF Involved NRN partners

Action summary	Timeline	Owner
Develop knowledge products/services to advise organisations on their incident-response processes (factsheets, white papers, runbooks, etc.).	2022 - 2024	J&V Involved NCSC, DTC

Action summary	Timeline	Owner
Intelligence-based incident coordination by AIVD and MIVD to be further expanded, partly through collaboration in the Cyber Intel/Info Cell (CIIC).	2022 - 2026	BZK, DEF Involved NCSC, CIIC

Action summary	Timeline	Owner
The Ministry of Defence is investing in personnel and technical capacity throughout the chain to enable information to be shared faster and more securely, and to improve the response time for vulnerabilities and incidents. For further details, see Annex 2 of the 2022 Defence White Paper.	2023 - 2026	DEF

Exercises

Action summary	Timeline	Owner / Involved
After the publication of the Government-wide Risk Analysis and the Government-wide Security Strategy, an interministerial exercise schedule will be drawn up, which will include the planning of cyber and hybrid exercises.	2023 - 2024	Owner: J&V Involved: All ministries
The national cyber exercise ISIDOOR will be held again. In the run-up, participants are being encouraged to ensure that their organisations have their own plans and procedures in place and that their staff have received the necessary training.	2023	Owner: J&V Involved: NCSC, police, AIVD, MIVD and private partners
In addition to ISIDOOR, various sectoral and local exercises will be organised. Examples include the symposium (with a crisis simulation) that the Ministry of Health, Welfare and Sport is arranging for around 200 participants from all tiers of the health-care sector; the annual government-wide cyber programme which includes exercises; and local exercises such as 'Hack the Hague'.	2022 - 2026	Owner: J&V Involved: Ministries, public authorities, operational partners and private partners
Yearly exercises will be held by public authorities (central government, provinces, municipalities and water authorities) using a simulated hacking attack. In addition, webinars will be held throughout the year, allowing organisations within and outside government to share knowledge.	2022 - 2026	Owner: BZK Involved: Subnational authorities
The Ministry of Defence will organise more frequent cyber exercises, and in doing so will seek to link up with national and international partners.	2022 - 2026	Owner: DEF
The Netherlands takes part in international NATO and EU exercises, including PACE, CMX and Blue OLEx, and will strive towards more intensive annual participation.	2022 - 2026	Owner: J&V, DEF Involved: AIVD, MIVD, NCSC

The end of the public transport smart card is approaching. It will soon be possible to check in on public transport with a debit card or a smartphone. This should make travel and payment easier. A change like this is a huge operation. More than 60,000 ticket barriers and card readers will need to be converted.

Pillar II
Secure and innovative digital products and services

Aim 1: Digital products and services are more secure

European legislation for digital products and services

Action summary	Timeline	Owner
In the negotiations on the EU Cyber Resilience Act (CRA), the government is pressing for the inclusion of a duty of care for manufacturers and suppliers of all ICT products, services and processes, including related standards and supervision. This duty of care should apply throughout the entire life cycle.	2022 - 2024	EZK Involved J&V, BZK, private partners

Action summary	Timeline	Owner
The government will promote cohesion in legislation on products and services by, for example, working to ensure that the CRA ties in with sector-specific cybersecurity requirements in EU regulations (such as those that apply to medical devices and cars) and general legislation such as the General Product Safety Directive and the Product Liability Directive.	2022 - 2024	EZK Involved J&V, VWS, I&W, private partners

Action summary	Timeline	Owner
Together with private parties, the government is contributing, via the Royal Netherlands Standardization Institute (NEN), to the creation of European harmonised standards for cybersecurity requirements in accordance with the Radio Equipment Directive.	2022 - 2024	EZK Involved NEN, private partners

Supervision and enforcement in respect of digital products and service

Action summary	Timeline	Owner / Involved
Consumers and businesses will be informed about the Sales of Goods Directive and the Digital Content Directive, on the basis of which consumers are entitled to (security) updates for as long as they may reasonably expect them.	2022 - 2026	Owner: EZK Involved: ACM
The Radiocommunications Agency Netherlands (AT) is tightening its supervision of cybersecurity market entry requirements for wireless networking devices under the Radio Equipment Directive, for example through research via the Internet of Things test lab and boosting capacity.	2022 - 2024	Owner: EZK Involved: AT
As the Netherlands' national cybersecurity certifying authority, the AT supervises certification schemes in the Netherlands and authorises the issue of certificates with a 'high' certification level. It also works with the AIVD's National Communications Security Agency.	2022 - 2026	Owner: EZK Involved: AT, AIVD
The Authority for Consumers and Markets (ACM) monitors the product suppliers who are required to inform consumers as to how long security and other updates will be available.	2022 - 2024	Owner: EZK Involved: ACM

Action summary	Timeline	Owner / Involved
The Radiocommunications Agency and the Authority for Consumers and Markets will collaborate more closely to improve monitoring and enforcement in relation to secure products and services, for instance by drawing up a joint exercise schedule.	2022 - 2024	Owner: EZK Involved: AT, ACM

Certification and standards

Action summary	Timeline	Owner / Involved
In partnership with private stakeholders, the government will contribute to the development and adoption of European cybersecurity certification schemes for ICT products, services and processes, such as those for cloud services, 5G technology and Common Criteria.	2023	Owner: EZK Involved: BZK, J&V, private stakeholders
The government is committed to the development of European certification schemes for secure software and cybersecurity services.	2022 - 2026	Owner: EZK Involved: J&V, BZK, private stakeholders
The Ministry of Economic Affairs and Climate Policy(EZK) is raising awareness and stimulating the implementation of certification schemes under the EU Cybersecurity Act.	2022 - 2026	Owner: EZK Involved: AT

Action summary	Timeline	Owner
The Baseline Security Product Assessment will be developed further, so that it corresponds to similar European evaluation standards to promote the exchangeability of secure European products. The AIVD is also working with the Radiocommunications Agency on the transition from the national scheme NSCIB, based on Common Criteria, to the European scheme, as soon as the Cybersecurity Act comes into force.	2022 - 2023	BZK Involved AIVD, EZK

Action summary	Timeline	Owner
The government is stimulating contacts with like-minded third countries about aligning international standards with European ones, as well as the development of similar legislation and standards in those countries.	2022 - 2026	EZK Involved J&V, BZ, private stakeholders

Action summary	Timeline	Owner
The government will explore how organisations can be better enabled to make clear agreements with their clients about cybersecurity. To this end, it will examine contract law practices and best practices in business-to- business relationships between suppliers of ICT products and services and clients.	2023	EZK Involved DTC, private stakeholders

General Security Requirements for Central Government (ABRO) and government procurement policy

Action summary	Timeline	Owner
General Security Requirements for Central Government (ABRO) will be drawn up on the basis of the development of the existing General Security Requirements relating to Defence Orders (ABDO), which must be met by companies fulfilling sensitive and/or classified government contracts.	2022 - 2023	BZK Involved DEF, J&V AIVD, MIVD

Action summary	Timeline	Owner
The cybersecurity procurement requirements (ICO) tool will be developed further, expanded and implemented. This will include the further development of government-wide sets of requirements. This will have a positive indirect effect on the market since it will encourage the supply of secure products and services.	2022 - 2023	BZK Involved CIP, EZK, subnational authorities

Action summary	Timeline	Owner
Together with the Association of Netherlands Municipalities (VNG), the Ministry of the Interior and Kingdom Relations will examine what is necessary to raise supplier management for subnational authorities to a higher level, with a focus on integrating service provision into procurement support and organising effective supervision of suppliers.	2022 - 2023	BZK Involved CIP, EZK, subnational authorities

Action summary	Timeline	Owner
The Centre for Information Security and Privacy is developing a package of cyber-security requirements and a tool that will support public sector organisations in the procurement of ICT products and services. This tool will be developed further and the public sector will be encouraged to use it. In addition, legislation will ensure that use of the sets of norms for secure purchasing is made mandatory for the public sector.	2022 - 2026	EZK, BZK Involved Subnational authorities

Aim 2: The Netherlands has a robust cybersecurity knowledge-and-innovation chain

Secure cryptography

Action summary	Timeline	Owner
The development of high-assurance products will be stimulated by enhanced and coordinated commissioning from central government, so that the Netherlands always has reliable cryptographic solutions at its disposal. This will be done in close collaboration with the Dutch cryptographic industry.	2022 - 2026	BZK Involved AIVD, J&V, DEF, EZK, OCW, I&W, private stakeholders, knowledge institutions

Action summary	Timeline	Owner
Together with the business sector and research institutions, studies will be conducted on the development of modern, high-quality security products.	2022 - 2026	BZK Involved AIVD, J&V, DEF, EZK, OCW, I&W, private stakeholders, knowledge institutions

Action summary	Timeline	Owner
The government is compiling long-term thematic roadmaps on the basis of which research will be conducted or outsourced by the dcypher platform. These include roadmaps on cryptocommunications and automated vulnerability scanning.	2022 - 2026	EZK Involved J&V, BZK, DEF, OCW, I&W, private stakeholders, knowledge institutions

Nationwide knowledge and innovation research collaboration

Action summary	Timeline	Owner
Interministerial cybersecurity knowledge and innovation requirements will be identified and listed on an annual basis. Needs will be prioritised where necessary.	2022 - 2026	EZK Involved BZK, J&V, OCW, DEF, I&W

Action summary	Timeline	Owner
The Ministry of Defence is reinforcing the Cyber Innovation Hub (CIH) in order to expand the innovation portfolio and strengthen the Netherlands' position in cybersecurity knowledge and innovation networks.	2022 - 2024	DEF

Action summary	Timeline	Owner
In accordance with a multiannual agenda and in partnership with a number of knowledge and other institutions, NCSC is conducting research activities in various domains on the role of NCSC and its target group(s).	2022 - 2026	J&V Involved NCSC

Action summary	Timeline	Owner
The cybersecurity knowledge and innovation requirements of the business sector and knowledge institutions will become part of the Dutch Top Sectors Programme.	2022 - 2026	EZK Involved Private stakeholders

European research collaboration and funding

Action summary	Timeline	Owner
A National Coordination Centre (NCC-NL) will be set up at the Netherlands Enterprise Agency (RVO) as part of the European Cybersecurity Competence Centre and Network (ECCCN).	2022 - 2026	EZK Involved BZK, DEF, J&V, OCW, I&W

Action summary	Timeline	Owner
Organisations in the dcypher network will be supported via the National Coordination Centre in preparing and implementing projects stemming from European initiatives and funds, such as Digital Europe and Horizon 2020.	2022 - 2026	EZK

Action summary	Timeline	Owner
Active measures will be taken to incorporate the research requirements of Dutch organisations in new work programmes by, for instance, Digital Europe and Horizon 2020, making use of Dutch cybersecurity expertise and innovative capacity.	2022 - 2026	EZK Involved OCW, J&V, BZK, DEF, I&W

Airports are no longer trying to stand out from the crowd with just the services and facilities they offer. Digitalisation and data are also areas in which they are advancing rapidly. For both passengers and cargo, this also means greater dependence on technology and greater potential vulnerability.

Pillar III
Countering threats posed by states and criminals

Aim 1: The Netherlands has a clear understanding of cyber threats posed by states and criminals

Understanding of threats posed by state actors

Action summary	Timeline	Owner / Involved
Research capacity will be expanded to allow in-depth intelligence-based investigation, which will provide a broader understanding of current and potential cyber threats.	2022 - 2026	Owner: BZK, DEF Involved: AIVD, MIVD

Action summary	Timeline	Owner / Involved
Unique intelligence will be translated nto specific courses of action that will enable clients to protect themselves more effectively.	2022 - 2026	Owner: BZK, DEF Involved: AIVD, MIVD

Action summary	Timeline	Owner / Involved
The scope for effective deployment of special investigative powers in respect of countries with an offensive cyber programme will be increased. A bill to this effect will be submitted to the House of Representatives.	2022 - 2026	Owner: BZK, DEF Involved: AIVD, MIVD

Cybercriminal research and investigative capacity

Action summary	Timeline	Owner / Involved
Together with local authorities and private partners, the police and the Public Prosecution Service (OM) will work to develop non-criminal-law interventions as well as criminal-law interventions to fight cybercrime, including ransomware attacks.	2023 - 2026	Owner: J&V Involved: Police, OM, BZK, subnational authorities, BZ
Efforts will be made to enhance cyber-security knowledge and expertise within the Public Prosecution Service.	2022 - 2026	Owner: J&V Involved: OM
The Royal Netherlands Marechaussee (KMAR) and the police will explore scope for further collaboration in tackling (cross-border) cybercrime.	2022 - 2024	Owner: J&V, DEF Involved: KMAR
The Public Prosecution Service will investigate the possibility of expediting cybercrime cases by means of a fast-track procedure.	2022 - 2026	Owner: J&V Involved: OM
The police will compile an annual security assessment on cybercrime and digitalised criminality. This will help build a picture of the main criminal phenomena, operating methods and risk levels facing society. These assessments will guide the police and the Public Prosecution Service in deciding where to focus and which investigations should be prioritised.	2022 - 2026	Owner: J&V Involved: Police, OM

Strengthening the diplomatic network

Action summary	Timeline	Owner / Involved
The number of cyber diplomats and their tasks will be increased in order to enhance the level of information we possess about digital threats and developments. This will be done by means of proactive reporting based on diplomatic contacts in third countries.	2022 - 2026	Owner: BZ Involved: DEF, BZK, J&V
Increase cyber competence and knowledge within the mission network to ensure that cybersecurity is better integrated in regular diplomatic contacts and related policy areas.	2022 - 2026	Owner: BZ Involved: DEF, BZK, J&V
The Ministry of Foreign Affairs (BZ) will press for better international information-sharing and joint analysis in the EU and NATO and, where necessary, will initiate smaller coalitions to improve the situational cyber-threat picture.	2022 - 2026	Owner: BZ Involved: DEF, BZK, J&V, NCSC
The NCSC will begin implementing the capacity-building programme internation-ally, including through the design of training activities.	2022 - 2026	Owner: J&V Involved: BZ, NCSC
The Ministry of Defence will participate in cyber initiatives, e.g. within the European Defence Fund and via PESCO projects, and will take a leading role within the EU and NATO. Participation in international exercises will become the norm.	2022 - 2026	Owner: DEF Involved: BZ

Aim 2: The Netherlands has a handle on the cyber threats posed by states and criminals

Attribution and response

Action summary	Timeline	Owner
Together with international partners, the government will develop new, more effective options for a diplomatic response to cyber threats. Existing frameworks and tools, such as the interministerial diplomatic cyber-incident response framework, the EU's Cyber Diplomacy Toolbox and the NATO Guide will be developed further and in alignment with the Government-wide State Threat Response Framework.	2022 - 2026	BZ Involved DEF, BZK, J&V, AIVD, MIVD, NCSC

Action summary	Timeline	Owner
The Netherlands will take the initiative in building smaller international coalitions to address specific incidents or threats and to stimulate EU and NATO policymaking on (diplomatic) response and attribution.	2022 - 2026	BZ Involved DEF, BZK, J&V, NCSC

Defensive and offensive cyber capabilities

Action summary	Timeline	Owner
The Ministry of Defence will invest in its overall cyber capabilities chain, partly by structurally embedding and enlarging cyber rapid response teams (CRRTs) and cyber mission teams (CMTs). It will also invest in increasing personnel readiness via training and exercises.	2022 - 2026	DEF Involved BZ

Action summary	Timeline	Owner
The Ministry of Defence will expand support structures to provide assistance to other organisations in major incidents, for example via the National Response Network (NRN).	2022 - 2026	DEF Involved J&V

Action summary	Timeline	Owner
Explore the possibilities for and implementation of active cyber defence measures in the context of the implementation of NIS2 and the (temporary) blocking of malicious traffic by Dutch internet service providers, with the necessary judicial safeguards in the context of national risk mitigation, preventing additional victims and reducing the threat.	2023 - 2024	J&V Involved EZK, BZK, DEF, NCSC, AIVD, MIVD, BZ

Aim 3: States adhere to the normative framework for responsible state behaviour in cyberspace

Normative framework

Action summary	Timeline	Owner / Involved
The UN's normative framework for cyber-space will be reinforced and consolidated in multilateral negotiations through effective focus on Dutch priorities, which include protecting the internet's core functionality and the multistakeholder model for internet governance.	2022 - 2026	Owner: BZ Involved: DEF, EZK, J&V, BZK
Observance and implementation of the UN's normative framework will be fostered by contributing to the establishment of the Programme of Action as an implementation mechanism. The government will be transparent about the implementation of the normative framework in the Netherlands.	2022 - 2026	Owner: BZ Involved: DEF, J&V, EZK, BZK

Internet governance

Action summary	Timeline	Owner / Involved
Participation by the Dutch multistakeholder community in the international debate will be encouraged (as will a similar commitment from the EU in respect of the European multistakeholder community) in order to amplify calls for an open, free and secure internet.	2022 - 2026	Owner: EZK Involved: BZ
The Netherlands will actively participate in international discussions about technical internet standards and other norms that affect the openness, freedom and security of the internet. This will include coordinating points of view at EU level and with like-minded countries.	2022 - 2026	Owner: EZK Involved: BZ
Multistakeholder organisations should be more effective in recognising and addressing social and technological challenges with regard to internet governance. This will enable consensus/decisions on solutions to those challenges to be reached more quickly. The government aims to stimulate this by taking an active part in discussions, encouraging like-minded countries to step up their presence, and by putting the outcome of the ICANN discussions on the agenda in both the Internet Governance Forum and the EU.	2022 - 2026	Owner: EZK Involved: BZ

Increasing digitalisation opens up countless opportunities for education, for example by offering online lectures and unlocking knowledge. At the same time, this greater reliance on technology carries its own risks. A number of universities have been targeted by ransomware attacks in recent years.

Pillar IV
Cybersecurity labour market, education and cyber resilience of the public

Aim 1: The public are properly protected against cyber risks

Public information campaigns

Action summary	Timeline	Owner
The Ministries of Justice and Security (J&V), Economic Affairs and Climate Policy (EZK), and the Interior and Kingdom Relations (BZK) will organise target-group-specific cybersecurity information campaigns focusing on basic cybersecurity measures. The effects will be measured after each campaign. The campaigns will be organised in collaboration with municipalities to ensure optimum use of the available municipal communication channels.	2022 - 2026	J&V, EZK, BZK Involved Subnational authorities

Action summary	Timeline	Owner
As part of City Deal Cybercrime[3], pilot projects will be rolled out with a view to increasing public and corporate resilience against cybercrime. The pilots will focus on greater integrality to ensure better and wider use of local best practices, with a view to developing nationwide support services.	2022 - 2023	BZK, J&V Involved Subnational authorities

Action summary	Timeline	Owner
The annual Alert Online cybersecurity awareness month will be held every October together with the partner network.	2022	EZK, J&V Involved BZK

3 Collaboration between J&V and municipalities on cybercrime resilience

Security advice for the public

Action summary	Timeline	Owner
Digital Government Information Units will be equipped to answer people's questions about cybersecurity and refer them where necessary to existing support centres, information helpdesks and local support initiatives by private partners.	2022	BZK

Action summary	Timeline	Owner / Involved
The public-private website *veiliginternetten.nl* will be developed further and expanded as a one-stop shop for cybersecurity information and advice for the public on what action to take.	2022 - 2023	Owner: EZK Involved: BZK

Action summary	Timeline	Owner / Involved
The 'cyber weather forecast' will be published periodically and its effectiveness will be evaluated after two years.	2022 - 2024	Owner: J&V Involved: EZK

Reliability of digital public services

Action summary	Timeline	Owner
The government will set up a uniform domain name extension so that members of the public can see at a glance whether or not they are actually dealing with a government agency. This will help to combat online fraud, such as phishing.	2022 - 2026	BZK

Action summary	Timeline	Owner
To improve the government's online recognisability, a 'registry of public sector internet domains' is being developed, so that the public can easily check whether or not a domain name belongs to the government. In case of doubt as to the authenticity of a website, people will be able to consult a contact point.	2022 - 2023	BZK

Aim 2: Members of the public respond to cyber incidents swiftly and efficiently

Action summary	Timeline	Owner / Involved
The police will make it possible to report more cybercrime phenomena online from 2023.	2023	Owner: J&V Involved: Police

Aim 3: School pupils are taught digital skills, with an emphasis on security

Curriculum

Action summary	Timeline	Owner
The Netherlands Institute for Curriculum Development (SLO) has been tasked with working with the teaching profession to develop specific core objectives for basic skills, including cybersecurity skills, for both primary and secondary education. These detailed core objectives will be submitted to the House of Representatives in a bill in 2025.	2022 - 2025	OCW

Action summary	Timeline	Owner
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. The first schools will start on this when the 2022-2023 academic year begins.	2022 - 2026	OCW

Aim 4: The Dutch labour market can meet the growing demand for cybersecurity experts

Cybersecurity labour market

Action summary	Timeline	Owner / Involved
Educational institutions will develop upskilling and reskilling programmes to enhance employees' cybersecurity expertise. To this end, they will working alongside the business community and other relevant parties. Any obstacles or limitations in that collaboration that stem from legislation will be identified and examined to see how they can be resolved.	2022 - 2026	Owner OCW Involved OCW, educational institutions and employers

Action summary	Timeline	Owner / Involved
The government will invest in higher professional education in the sciences, including cybersecurity. Resources will be allocated to (1) higher intake, (2) lower drop-out and switch rates, (3) higher lateral intake, and (4) induction in/hot transfer to the labour market. This measure is intended to mitigate the shortfalls in the labour market.	2023 - 2029	Owner OCW Involved HBOs

Action summary	Timeline	Owner
Subject to the definitive advice of an independent committee (which is expected in late September/early October 2022), cybersecurity investments will be made for a number of specific areas of university education, working from the sector plans. The aim of this funding is to stimulate collaboration. For each sector/domain, universities will perform an analysis identifying opportunities and problems, and proposing measures to respond to them. The sector plan submitted for 'Technology' will include a focus on cyber-security. University cybersecurity courses will benefit too in this manner.	2023 - 2026	OCW Involved Universities

Action summary	Timeline	Owner
The qualitative and quantitative shortages on the cybersecurity labour market will be examined, and recommendations will be made on how to address them.	2023	EZK Involved OCW, J&V, employers, CBS, University Committee for Academic Practice

Action summary	Timeline	Owner
The government will explore whether the initiatives designed to shed light on ICT-wide shortages and the development of an ICT dashboard for education and the labour market also provide sufficient insight into regional shortages of cybersecurity specialists.	2023 - 2024	EZK Involved OCW, SZW, BZK

Action summary	Timeline	Owner
Via the 'Human Capital Agenda ICT', the government aims to increase the supply of cybersecurity and ICT specialists to the labour market, and enhance the quality of that supply. This will be done in close collaboration with the business sector, regional and local government organisations and educational institutions.	2022 - 2026	EZK

Action summary	Timeline	Owner
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 product development.	2022 - 2026	EZK Involved dcypher

October 2022

This publication was produced by the National Coordinator for Counterterrorism and Security (NCTV) on behalf of central government
info@nctv.minjenv.nl