Cybersecurity

A State-of-the-art Review: Phase 2

Final report

Erik Silfversten, Victoria Jordan, Kevin Martin, Diana Dascalu, Erik Frinking

This publication presents the final report of a RAND Europe study commissioned by the WODC on behalf of the Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).

Preface

The NCTV (*Nationaal Coördinator Terrorismebestrijding en Veiligheid* – 'National Coordinator for Security and Counterterrorism') partners with government, science and business in order both to protect the Netherlands against threats that can disrupt society and ensure that Dutch vital infrastructure is – and remains – safe. This document presents the final report of the second part of a RAND Europe study commissioned by the WODC (*Wetenschappelijk Onderzoek- en Documentatiecentrum* – 'Research and Documentation Centre'), on behalf of the NCTV. The two studies examine the current state-of-the-art in the field of cybersecurity as part of a broader programme of work that aims to develop a broad research agenda for the NCTV. This programme of work also includes two other state-of-the-art studies in the fields of crisis management and counterterrorism, which are published separately by the WODC.

This report investigates two of the priority areas identified in the first phase of cybersecurity state-of-the-art project in more detail; namely, cybersecurity governance from a national security perspective, and critical infrastructure protection. The report should be of interest to individuals and organisations involved in cybersecurity policymaking in the Netherlands and beyond.

RAND Europe is a not-for-profit, independent policy research organisation that aims – through objective research and analysis – to improve policy- and decision making in the public interest. RAND Europe's clients include national governments, multilateral institutions and other organisations with a need for rigorous, independent interdisciplinary analysis. Part of the globally operating RAND Corporation, RAND Europe has offices in Cambridge (United Kingdom) and Brussels (Belgium).

For more information about RAND Europe or this document, please contact Erik Silfversten (erik_silfversten@rand.org).

RAND Europe
Rue de la Loi 82, Bte 3
1040 Brussels
Belgium
Tel: +32 (2) 669 2400

RAND Europe
Westbrook Centre, Milton Road
Cambridge CB4 1YG
United Kingdom
Tel: +44 1223 353 329

Summary

The National Coordinator for Security and Counterterrorism (NCTV) is a government organisation under the Dutch Ministry of Justice and Security. Its mission is to protect the Netherlands against threats that can disrupt society and ensure that Dutch critical infrastructure is – and remains – secure. To fulfil its mission, the NCTV is preparing a research agenda to intensify cooperation with the scientific community, stimulate scientific discussion in fields of importance to the NCTV and help identify blind spots in the NCTV's or scientific community's knowledge. Part of the scoping and development work for this research agenda comprises the delivery of three 'state-of-the-art' studies in the fields of counterterrorism, crisis management and cybersecurity.

This RAND Europe report is part of that process to develop an overview of the 'state-of-the-art' knowledge in the area of cybersecurity, which was divided in two phases. In Phase 1 of this study, RAND was commissioned to perform an initial scan of cybersecurity-related research and the subtopics discussed in this field, as well as to highlight underexposed subjects that deserve more attention. The overarching aim of Phase 1 was to discern which current cybersecurity topics would merit further exploration through additional research in Phase 2.

Four such topics emerged as the most prominent, most urgent and most relevant areas for the NCTV to consider:

- Cybersecurity governance from a national security perspective;
- Trust in information and data;
- Critical infrastructure security and protection; and
- Supply chain security.

Study objectives and methodology

From the list of priority research areas that emerged from Phase 1, the NCTV prioritised two of the four themes for further examination in Phase 2:

- Cybersecurity governance from a national security perspective; and
- Critical infrastructure security and protection.

For both research areas, research questions (RQs) were derived from the Phase 1 research and input from the NCTV. These two research areas and the associated RQs for Phase 2 are listed in the table below.

Table 0.1 Overview of Phase 2 research questions

Overarching research area	Research questions
1. Cybersecurity governance from a national security perspective	1.1 How can the current model of governance and current cybersecurity initiatives in the Netherlands be aligned and improved?
	1.2 How can system responsibility for cybersecurity be set up?
	1.3 What lessons can be identified through international comparisons of different national cybersecurity governance models?
	1.4 How can capabilities and skills required across stakeholders and functions to ensure national cybersecurity be identified and managed?
	1.5 How could efficiency and effectiveness be measured for cybersecurity policymaking?
2. Critical infrastructure security and protection	2.1 What are the risks and challenges resulting from the interplay between legacy critical infrastructure technologies and new technologies?
	2.2 How can current levels of cybersecurity maturity within the critical infrastructure sector be measured and understood?
	2.3 What can be done to improve security of operational technology deployed in critical sectors?
	2.4 What can be done with a view to potential threats from actors and organised groups or networks of actors in order to prevent damage to the vital infrastructure?

Guided by these research questions, the overarching objectives for Phase 2 were to:

- Explore and develop additional knowledge across the identified RQs;
- Highlight possible areas where additional knowledge or research is required; and
- Identify possible areas for intervention by the NCTV and provide recommendations for future improvement.

The study used a mixed-methods approach consisting of desk research and a literature review, case studies, interviews and expert workshops.

Summary of key findings in relation to cybersecurity governance from a national security perspective

Governance can be understood as the approaches used by multiple stakeholders to identify, frame and coordinate the response to a collective problem. Cybersecurity governance from a national security perspective can, therefore, be seen as the approaches used by multiple stakeholders to identify, frame and coordinate proactive and reactive responses to potential national security risks stemming from the cyber domain.

This study explored how both the current model of governance and current cybersecurity initiatives in the Netherlands could be aligned and improved, and how system responsibility for cybersecurity could be established. The study found that the governance of cybersecurity is a prominent area of discussion in the

Netherlands, and that there are several ongoing initiatives exploring how the governance of cybersecurity in the Netherlands is working, and how it could be improved in the future.

The current cybersecurity governance model in the Netherlands is anchored in the *Polder* model of consensus-driven decision making. In practice, this means that the Dutch governance structure is a network-governance model that includes several organisations – each of which is responsible for cybersecurity within their mandate and area of responsibility – working to ensure national cybersecurity. Within this context, this study identified a series of challenges to the current governance of cybersecurity from a national perspective in the Netherlands:

- **Unclear roles and responsibilities within the cybersecurity governance structure, and a lack of agility and proactiveness in cybersecurity policymaking.** The study identified that the distributed governance model might make it difficult to have clear roles and responsibilities across the entire system. The study also highlighted that there could be a mismatch of resources and efforts placed on crisis management and reactive response, rather than proactively building and improving the resilience of digital society in the Netherlands.
- **Information-sharing challenges.** Adequate and productive information-sharing is fundamental to both the prevention and response phases of addressing cybersecurity threats. This study found two information-sharing areas as potential areas for improvement: information-sharing and knowledge relating to the state of cybersecurity within the national government, and information-sharing between organisations with a cybersecurity responsibility.
- **Challenges related to lacking or duplicating regulations and standards could add complexity within the governance system.** The current governance structure could lead to a lack of coherence in regulation, with competing or contradicting requirements that could potentially undermine efforts to strengthen cybersecurity. Within this context, more proactive and enforceable minimum cybersecurity standards might, therefore, help harmonise the cybersecurity arrangements and help address varying maturity levels across government.
- **The distinction between vital and non-vital infrastructure.** This distinction plays a pivotal role in the Dutch governance structure, in which critical infrastructure operators are subject to additional legislation and regulation, have mandatory incident-reporting requirements, and are part of the National Cyber Security Centre (NCSC) information-sharing structure. This might mean that non-critical providers and services are subject to less stringent security requirements and could miss out on important security advice, whilst still being vital to societal resilience or national security.
- **Challenges of oversight and evaluation.** This study found that there is currently not an enforceable government-wide cybersecurity standard, and each government organisation maintains its own cybersecurity arrangements. Additionally, the NCSC primarily works in an advisory capacity. This makes it challenging to enforce, evaluate and assure cybersecurity arrangements across the various actors in the Dutch ecosystem.

The study also explored potential lessons for the Netherlands from different national cybersecurity governance models. To help answer this question, the study team developed five case-study country profiles of national governance approaches in Estonia, Germany, Sweden, the United Kingdom and the

United States. However, these international case studies can only offer limited lessons for the Dutch governance system. Case-study analysis can illustrate how different countries have approached their governance structure, but cannot fully answer what makes them work (or not work) within their national structures or how each nation's performance compares to other approaches.

Managing the cybersecurity capabilities and skills required for national security

This study also explored how to identify and manage the capabilities and skills required to ensure national cybersecurity. The Dutch government has emphasised the importance of having appropriate and sufficient depth of capabilities and skills in place to ensure a digitally secure Netherlands – particularly from a national security perspective – with several initiatives already implemented and underway. Within this context, the study identified three overarching challenges in relation to cybersecurity skills from a national security perspective:

- **The distributed responsibility for workforce management issues**, which could pose challenges in coordinating the cybersecurity workforce across different government organisations and agencies;
- **The lack of commonly accepted and shared language**. Within the Dutch context, there is not a single, commonly agreed and widely used taxonomy for cybersecurity skills or professions, which makes it challenging to understand the current capacity and skills in the Netherlands, and how to best improve them.
- **Recruitment and retention issues**. Recruitment and retention challenges are well-known and prevalent in cybersecurity. In such a competitive labour market, government organisations could face challenges recruiting cybersecurity professionals and ensuring access to the right skills for national security, especially in-house personnel but also through outsourcing and partnership arrangements with the private cybersecurity industry.

This study identified several approaches and interventions that could help address the three challenges outlined above, including the use of:

- An easily accessible knowledge base to foster a shared understanding of the cybersecurity field;
- Workforce strategies to help align cybersecurity skills efforts across government;
- Competency frameworks and career paths to streamline workforce management, skills development and sustainment; and
- Training-needs analysis to help identify required skills across functions and stakeholders from a national security perspective.

Measuring performance for cybersecurity policymaking

The study further sought to explore how efficiency and effectiveness of national cybersecurity could be measured or evaluated to better inform policy and decision making. The study identified several approaches to measuring performance, including:

- Frameworks for thinking about the evidence needed for cybersecurity policymaking;
- Approaches that have previously been used for evaluation in the cyber domain; and
- Approaches from other sectors that could be used for evaluation in the cyber domain.

The various approaches presented have different uses, potential strengths and benefits, and it is therefore useful to consider some fundamental evaluation questions when reviewing them (i.e. *why* we need to measure performance, *what* we need to measure and *how* we should measure it). Table 0.2 below presents an overview of the identified approaches and where they might add the most value.

Table 0.2 Overview of approaches to improve evaluation and performance measurement in cybersecurity

Approach or framework	Use case and added value
Evidence model for cybersecurity policymaking	To assess and improve the evidence used for cybersecurity policymaking.
Post-incident and lessons learned analysis	To analyse, assess and improve the response mechanisms to incidents or attacks, including the governance of cybersecurity both within the overall system and within crisis management or incident response structures.
Self-assessments of cybersecurity maturity	To assess and help improve the cybersecurity maturity of organisations.
Programme evaluation	To evaluate the impact of specific programmes or interventions within national cybersecurity.
Performance auditing and Value for Money	To evaluate the wider performance-specific programmes or the overall national approach to cybersecurity (e.g. its economy, efficiency and effectiveness).
Exercises and games	To explore poorly understood areas of cybersecurity and develop better evidence for policymaking. To exercise, test and assess governance structures and plans, particularly in relation to incident response and crisis management.
Measuring the value of national cybersecurity	To define and measure the overall contribution and value of the national cybersecurity system.
Decision making under deep uncertainty methods	To assess and refine future polices and improvements to national cybersecurity.

Summary of key findings in relation to critical infrastructure and security

Critical infrastructure encompasses those services deemed necessary for the functioning of society (e.g. power plants, water supply systems, transport infrastructure, democratic institutions and government processes, etc.). Recent trends to Internet-enable parts of critical infrastructure, and the adoption of emerging technologies or solutions, present new challenges linked to the cybersecurity of critical infrastructure, and have led governments to investigate how best to secure them.

Critical infrastructure and technology

In relation to critical infrastructure and technology, the study particularly explored the risks and challenges resulting from the interplay between legacy critical infrastructure technologies and new

technologies. The study team found that the interplay between legacy and new technologies is well understood among Dutch experts, but that risks and challenges are not always addressed or adequately managed. These risks are linked to:

- **Liability and obsolescence** of some parts of critical assets, which carry the risk of enabling system failure or malicious exploitation. These challenges should be addressed through better understanding of the assets concerned and of the interplay between suppliers and buyers, for instance through asset management and clearly defined security agreements between suppliers and buyers.
- **The connectivity of operational technologies** and the resulting cascading effects, which increase potential platform attacks and multiply the potential damage. The implementation of the Network and Information Security (NIS) directive partly addresses this risk through the identification of essential providers dependent on Information and Communications Technology (ICT), but it is necessary to better-map the risks linked to cascading effects.
- **The gap between Operational Technology (OT) and Information Technology (IT)** remains an obstacle to tackling already identified risks. As this interplay increases, do does the urgency of bridging this gap through education, awareness, training and cooperation between experts of IT and of operational technologies.

Critical infrastructure and cybersecurity maturity

The study further explored how current levels of cybersecurity maturity within the critical infrastructure sector could be measured and understood. The study identified several approaches and models for assessing cybersecurity maturity in critical infrastructure. However, the study also identified several challenges linked to measuring cybersecurity maturity:

- **Existing models for measuring maturity in the critical infrastructure sector face several challenges**, including for instance the difficulty in defining useful and measurable indicators and the continuous evolution of the cybersecurity field, which requires constant actualisation of standards and models.
- **The tension between measuring maturity at a general level and measuring it at the sectorial level** was underlined as a trade-off between general applicability and further precision. Experts suggested the government should provide sectorial recommendations and guidelines on this issue.
- **The debate about the benefits of adopting a regulatory approach to cybersecurity maturity and of relying on a cooperative approach** suggests there might be a risk that measuring cybersecurity maturity becomes a 'checklist exercise'. Understanding the motivations behind assessments and the benefits linked to regulations was therefore identified as an area for further research.
- **Including supply-chain risks and interdependencies in maturity assessments** emerged as an essential factor in accurately measuring cybersecurity maturity and building a better and more comprehensive understanding of risks.

Critical infrastructure and improving cybersecurity

Lastly, the study explored measures for improving the security of operational technology deployed in critical sectors and protecting against potential threats from actors and organised groups or networks of actors. The study identified the following essential areas of action for improving the security of operational technology:

- **Critical infrastructure security should rely on an integrated and multi-faceted approach**, considering assets as well as their environment. Such an approach could benefit from future technological developments such as supply-chain management relying on hash chain or cryptographic audit logs, zero-trust architecture, and inventory management augmented by automated processes, AI and self-healing.
- **Cross-sectorial information-sharing emerged as crucial to improving the security of Dutch critical infrastructure**. This was identified as an area where the government could play a coordinating role to help bridge challenges linked to trust and confidentiality.
- **Changes in organisation structures** – especially towards multi-disciplinary teams – and better coordination between operations, security, management and legal teams would help to both improve security and gain a better understanding of existing risks.

This study found little evidence available on the protection of critical infrastructure from the angle of existing threats from actors and organised groups. Consultations with experts, however, did provide valuable insights on the issue:

- **The current priority should be on tackling immediate threats**, which might be less disruptive than Advanced Persistent Threats (APTs) but are more common due to current low maturity levels of several critical infrastructure providers.
- **Providing a clear definition of roles and responsibilities between the government and private sector** is necessary to ensure prevention against APTs and improve the reaction to and investigation of such attacks.
- **This question was identified as a geopolitical issue that therefore requires a geopolitical approach from the government**, including by relying on international cooperation to identify and tackle external threats.

Summary of recommendations

To address these challenges, this study identified a set of recommendations for the NCTV, as summarised below.

1. The NCTV should further explore the role of the distinction of critical and non-critical infrastructure within the Dutch governance model

As noted above, there might be a need to revisit the distinction between critical and non-critical infrastructure services or processes. It could therefore be useful for NCTV to further examine the process of how critical infrastructure is identified and categorised, how cybersecurity dependencies and risks are

mapped, understood and shared, and what requirements are placed on organisations of varying criticality within the Netherlands. As such, the NCTV should seek to:

- **Explore and assess alternative approaches to the identification and classification of critical infrastructure**, including more horizontal and sector-agnostic approaches;
- **Explore how dependencies between critical sectors and organisations can be better mapped and understood** (see also the recommendations below relating to critical infrastructure security); and
- **Explore how to improve information-sharing between critical and non-critical sectors** to ensure that organisations receive the right information at the right time.

2. The NCTV should further explore and invest in proactive and preventative approaches to national cybersecurity, going beyond the current more reactive paradigm

Within the decentralised model of governance found in the Dutch system, cybersecurity responsibilities are distributed across multiple ministries, government departments and organisations. Since the cybersecurity domain is continuously evolving and requires constant adaptation, it is important that the Dutch government remains agile, flexible and proactive in its approach to national cybersecurity.

As such, the NCTV should further explore and invest in proactive approaches to cybersecurity, including:

- **Ensuring that regular and extensive exercises take place** to stress-test and exercise governance structures and incident-response plans, so that all stakeholders have a well-developed understanding of their roles and responsibilities and develop good working relationships with their peers.
- **Exploring if and how the NCTV and the NCSC could set up and deliver more proactive cybersecurity services**, for example proactive vulnerability-scanning of Dutch networks.
- **Investing in further research to identify how cybersecurity dependencies and system risks can be better identified and reduced** (see also the recommendations on critical infrastructure security below).

3. The NCTV should explore the role of minimum security standards and the potential need for further compliance mechanisms

This study also identified potential issues in relation to a lack of harmonised cybersecurity requirements across government and a lack of minimum cybersecurity requirements and standards, which could make it difficult to ensure a sufficient cybersecurity baseline across all organisations in the Netherlands. The study also found that there could be challenges to ensure organisations comply with cybersecurity advice or guidance, even when specific vulnerabilities or threats have been identified.

Within this context, the NCTV should further investigate and explore the possibility of:

- **Developing and implementing minimum cybersecurity standards for national government** in order to strengthen the minimum cybersecurity baseline across the various government ministries and departments, as well as to harmonise government IT infrastructure.
- **Developing and implementing minimum cybersecurity standards for private sector companies that supply IT services to national government**, in order to reduce supply-chain weaknesses and cybersecurity dependencies between sectors.
- **Investigating the need for increased authority for the NCSC or other government agency to evaluate, provide oversight and enforce cybersecurity advice** or standards beyond the 'comply-or-explain' framework that is currently in place.

4. The NCTV should make investing in skills development in cybersecurity and engineering an urgent priority for the protection of Dutch critical sectors

The current skills and knowledge gap in critical infrastructure results in significant challenges, ranging from undermining the cybersecurity of assets themselves to limiting the ability for assessors to provide valuable insights into the cybersecurity maturity of an organisation. Findings from this study show that immediate-term measures are needed to address the skills gap and to bridge the current OT–IT divide. The NCTV should, therefore, work with the responsible ministries to:

- **Invest in operational technology research and awareness within the government** to ensure dedicated bodies – such as the NCSC – can provide appropriate recommendations and guidelines, especially in cases of malicious attacks. This would also help to build trust and benefit collaboration between the government and industries.
- **Create synergies between academia, industry, regulators and the government** by implementing measures such as job rotations in critical sectors, secondments for public servants, compulsory internships for students, and guest lectures from stakeholders across the industry supply-chain and with regulators.
- **Integrate elements of OT and IT academic curricula** to build shared understanding across both disciplines, and further collaboration at both academic and industry levels.
- **Increase cybersecurity awareness among OT specialists** by teaching elements of cybersecurity to students of engineering as well as providing cybersecurity trainings to OT specialists working in critical sectors.

5. The NCTV should support the development tools required to understand and address risks linked to the critical infrastructure supply chain

The maturity of cybersecurity across complex globalised supply chains is expected to be one of the key issues dominating the field of cybersecurity in the next decade. Understanding vulnerabilities and risks linked to critical infrastructure's supply chains is therefore essential to the protection of Dutch critical sectors. Within this context, areas for further research and action include:

- **Broadening existing risk-mapping models to include the whole critical infrastructure supply chain**, including consideration of relevant externalities**.** This could rely on supply-chain

management and leveraging new technologies, or on assessing risks based on service delivery and service continuations – rather than on operators – in order to better identify interdependencies.

- **Investigating potential avenues for international cooperation to address critical infrastructure supply-chain vulnerabilities**. This could include developing geopolitical alliances and European or alliance-based approaches to tackling uncertainties linked to international supply chains, e.g. to inform risk-mapping models that include externalities, and tackle foreign threats.
- **Enabling information- and knowledge-sharing specific to operational technology in order to gain better understanding and visibility of operational technology products' supply-chain and associated risks**. For example, this could be done through initiatives such as the development of an OT-specific information-sharing platform, or an OT Information Sharing and Analysis Centre (ISAC) – a project currently under discussion between the NCSC and TNO (*Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek*).

Additional areas that warrant the attention of the NCTV

In addition to these recommendations, this second phase of the study also identified additional areas that warrant the attention of the NCTV. Some of these areas are already the subject of existing efforts to develop new capability. In these cases, the NCTV should seek to:

- Continue working with the Ministry of Education and other responsible ministries in the ongoing efforts to develop a replacement to dcypher, as well as exploring the possibility and potential value of developing a cybersecurity workforce management body for national government. This body could promote shared knowledge of the cybersecurity field, a common competency framework and better-aligned training requirements and career paths.
- Continue working with Chief Information Officer (CIO) Rijk and Chief Information Security Officer (CISO) Rijk to develop a comprehensive overview and understanding of the state of cybersecurity within the national government.
- Continue working with the Ministry of the Interior and Kingdom Relations and other relevant stakeholders to assist in ongoing efforts to harmonise cybersecurity legislation and regulation.

Other recommendations focused on areas where there is little to no existing effort include the following areas that the NCTV could consider taking a leading role in:

- Developing the evidence base on cybersecurity maturity models by conducting robust and independent evaluations of the effectiveness of maturity models, and by comparing existing models.
- Developing the evidence base on current approaches to cybersecurity regulations in critical infrastructure by investigating the differences between general and sector-specific standards, and their impact on cybersecurity of critical infrastructure.
- Developing government capability for tackling APTs through the development of a forensics function within the Dutch government.

Beyond this state-of-the-art study, there are several ongoing efforts being carried out simultaneously to develop further the necessary evidence for ensuring cybersecurity in the Netherlands, and addressing the risks entailed. The challenges and recommendations identified in this study should therefore be considered alongside the results of other past and ongoing research efforts. Some of these challenges could be addressed by additional research, while others might perhaps be better addressed outside a research agenda. It could be the case that there is an understanding of what needs to be done, but perhaps not the political will, funding or operational ability to adequately implement these measures. These issues nevertheless warrant the attention of the NCTV. Similarly, areas where existing efforts are already underway might still require or benefit from the support of the NCTV.

Table of contents

Figures

Tables

Boxes

Abbreviations

ACD	Active Cyber Defence
AI	Artificial Intelligence
APT	Advanced Persistent Threat
ATPs	Adaptation Tipping Points
BfV	Federal Office for the Protection of the Constitution
BKA	Federal Criminal Police Office
BMI	Federal Ministry of the Interior, Building and Homeland Affairs
BMVg	Federal Ministry of Defence
BND	Federal Intelligence Service
BPVS	*Beveiliging en Publieke Veiligheid Schiphol*
BSI	*Bundesamt für Sicherheit in der Informationstechnik* – 'Federal Office for Information Security'
BSI Act	Act on the Federal Office for Information Security
C2M2	Cybersecurity Capability Maturity Model
CCA	Centre for Cyber Assessment
CCP	Central counterparty
CDU	Cyber Defence Unit
CERT	Computer Emergency Response Team
CERT-EE	Estonian Computer Emergency Response Team
CERT-UK	UK Computer Security Incident Response Team
CERT-SE	Swedish Computer Security Incident Response Team
CESG	Communication-Electronics Security Group
CI	Critical Infrastructure
CIO	Chief Information Officer
CIP	Critical Infrastructure Project
CIR	Cyber and Information Space

CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CiSP	Cyber Security Information Sharing Partnership
CompTIA	Computing Technology Industry Association
CPNI	Centre for the Protection of National Infrastructure
CSC	Cyberspace Solarium Commission
CSIRT	Computer Security Incident Response Team
CSOC	Cyber Security Operations Centre
CSR	Cyber Security Council
Cyber SR	German National Cyber Security Council
CyBOK	Cyber Security Body Of Knowledge
DAP	Dynamic Adaptive Planning
DAPP	Dynamic Adaptive Policy Pathways
DCMS	Department for Digital, Culture, Media and Sport
DFID	Department for International Development
DHS	Department of Homeland Security
DIB	Defence Industrial Base
DIGG	Agency for Digital Government
DMARC	Domain-based Message Authentication, Reporting & Conformance
DMDU	Decision Making under Deep Uncertainty
DNS	Domain Name Service
DOD	Department of Defence
DODIN	DOD Information Network
DOJ	Department of Justice
DTC	Digital Trust Center
ECSEPA	Evaluating Cyber Security Evidence for Policy Advice
ECTF	Electronic Crimes Task Force
EDLA	Estonian Defence League Act
EiaB	Exercise in a Box
ENISA	European Union Agency for Cybersecurity
EQAM	Evidence Quality Assessment Model for Cybersecurity Policymaking
ESMT	European School of Management and Technology
EU	European Union
FBI	Federal Bureau of Investigations
FCDO	Foreign, Commonwealth and Development Office

FISMA	Federal Information Security Management Act
FIU-NL	Dutch Financial Intelligence Unit
FMV	Swedish Defence Materiel Administration
FOC	Full operating capability
FRA	National Defence Radio Establishment
FRG	Federal Republic of Germany
GAO	Government Accountability Office
GCHQ	Government Communications Headquarters
GDPR	General Data Protection Regulation
HBC	Host Based Capability
HBO	*Hoger beroepsonderwijs*
HM	Her Majesty's
ICS	Industrial Control Systems
ICT	Information and Communications Technology
IIoT	Industrial Internet of Things
IOC	Initial operating capability
ISAC	Information Sharing and Analysis Centre
ISO	International Organization for Standardization
IT	Information Technology
KA	Knowledge Areas
KPIs	Key Performance Indicators
LGA	Local Government Association
LME	Logging Made Easy
LSI	Office for Information Security
MAD	Military Counter-Intelligence Service
MEAC	Ministry of Economic Affairs and Communications
MOD	Ministry of Defence
MOJ	*Justitiedepartementet* – Swedish Ministry of Justice
MSB	Swedish Civil Contingencies Agency
MUST	Military Intelligence and Security Service
NAO	National Audit Office
NATO	North Atlantic Treaty Organisation
NCA	National Crime Agency
NCAZ	German National Cyber Defence Centre
NCC	National Coordinating Center for Communications

NCCIC	National Cybersecurity and Communications Integration Center
NCIRP	National Cyber Incident Response Plan
NCPS	National Cybersecurity Protection System
NCSA	Dutch Cyber Security Agenda
NCSC	National Cyber Security Centre
NCSRA	National Cyber Security Research Agenda
NCTV	*Nationaal Coördinator Terrorismebestrijding en Veiligheid* – 'National Coordinator for Security and Counterterrorism'
NDN	Dutch National Detection Network
NICE	National Initiative for Cybersecurity Education
NIS	Network and Information Security
NIST	National Institute of Standards and Technology
NRMC	National Risk Management Center
NSIT	National Cooperative Council against Serious IT Threats
NWO	Netherlands Organisation for Scientific Research
OCS	Office for Cyber Security
OECD	Organisation for Economic Cooperation and Development
OMB	Office of Management and Budget
OT	Operational Technology
PDNS	Protective Domain Name System
PPD	Presidential Policy Directive
PTS	Swedish Post and Telecom Authority
PVF	Pubic Value Framework
RA	Research Area
RDM	Robust Decision-Making
RIA	State Information System Authority
RQ	Research Question
SAC	Scientific Advisory Committee
SAMFI	Cooperation Group for Information Security
SÄPO	Swedish Security Service
SCADA	Supervisory Control and Data Acquisition
SIM3	Security Incident Management Maturity Model
SSA	Sector-Specific Agencies
TNA	Training Needs Analysis
TNO	*Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek – 'Netherlands Organisation for Applied Scientific Research'*

UK	United Kingdom
UK NCSC	UK National Cyber Security Centre
URL	Uniform Resource Locator
VFM	Value for Money
Wbni	*Wet beveiliging netwerk- en informatiesystemen* – 'NIS Directive'
WODC	*Wetenschappelijk Onderzoek- en Documentatiecentrum* – 'Research and Documentation Centre'
WRR	Netherlands Scientific Council for Government Policy
ZCO	Bundeswehr Cyber Operations Centre
ZKA	Customs Investigation Bureau

Acknowledgements

This report has been made possible through the valuable contributions of various individuals. First of all, we wish to express our gratitude to the Chair and the members of the Steering Committee, consisting of Prof. Dr W.Ph. Stol (NHL Stenden University of Applied Sciences), Dr M.E.M. Spruit (The Hague University), R.S. van Wegberg (Delft University of Technology), Dr M.T. Croes (Ministry of Security and Justice) and Dr G. Haverkamp (WODC) for their valuable time, feedback and insights, which ultimately improved the quality of the study.

We would also like to express our gratitude to all interviewees and workshop participants, listed in Annex B, for their willingness to participate in this research, and the insights that they have been willing to share. Lastly, we also express a special thank you to the Quality Assurance reviewers of this report, Stijn Hoorens and James Black, who offered helpful and constructive feedback and advice throughout the project.

1. Introduction

This document represents the second and final report of a RAND Europe study commissioned by the WODC (*Wetenschappelijk Onderzoek- en Documentatiecentrum* – 'Research and Documentation Centre') to examine two research areas identified in the first part of this cybersecurity state-of-the-art project.[1] This introductory chapter presents the background to the study, its objectives and scope, as well as an overview of the methodology and limitations of the study. The chapter concludes with an outline of the report's structure.

1.1. This report builds on the findings from Phase 1 of the cybersecurity state-of-the-art project

The National Coordinator for Security and Counterterrorism (NCTV) is a government organisation operating under the Dutch Ministry of Justice and Security. Its mission is to protect the Netherlands against threats that can disrupt society, and to ensure that Dutch critical infrastructure is – and remains – secure. To fulfil its mission, the NCTV is preparing a research agenda to intensify cooperation with the scientific community, stimulate scientific discussion in fields of importance to the NCTV and help identify blind spots in the NCTV's or scientific community's knowledge. Part of this programme of scoping and development work comprises the delivery of three 'state-of-the-art' studies in the fields of counterterrorism, crisis management and cybersecurity.

This report is part of the process to develop an overview of the 'state-of-the-art' knowledge in the area of cybersecurity, which was divided in two phases. In Phase 1 of this study, RAND Europe was commissioned by the WODC on behalf of the NCTV to perform an initial scan of cybersecurity-related research and subtopics discussed in this field, as well as to highlight potential underexposed subjects that deserve more attention. The overarching aim of Phase 1 was to discern which current cybersecurity topics would merit further exploration through additional research in Phase 2. Four topics emerged as the most prominent, most urgent and most relevant areas for the NCTV to consider:

1. Cybersecurity governance from a national security perspective;
2. Trust in information and data;
3. Critical infrastructure security and protection; and
4. Supply chain security.

[1] See Silfversten et al. (2019).

1.2. The study covers two overarching research areas and their associated research questions

From the list of priority research areas (RAs) emerging from Phase 1, the NCTV prioritised two of the four themes for further examination in Phase 2:

- Cybersecurity governance from a national security perspective; and
- Critical infrastructure security and protection.

These two research areas and the associated research questions (RQs) for Phase 2 are listed in the table below.

Table 1.1 Overview of Phase 2 research questions

Overarching research areas	Research questions (RQs)
1. Cybersecurity governance from a national security perspective	1.1 How can the current model of governance and current cybersecurity initiatives in the Netherlands be aligned and improved?
	1.2 How can system responsibility for cybersecurity be set up?
	1.3 What lessons can be identified through international comparisons of different national cybersecurity governance models?
	1.4 How can capabilities and skills required across stakeholders and functions to ensure national cybersecurity be identified and managed?
	1.5 How could efficiency and effectiveness be measured for cybersecurity policymaking?
2. Critical infrastructure security and protection	2.1 What are the risks and challenges resulting from the interplay between legacy critical infrastructure technologies and new technologies?
	2.2 How can current levels of cybersecurity maturity within the critical infrastructure sector be measured and understood?
	2.3 What can be done to improve security of operational technology deployed in critical sectors?
	2.4 What can be done with a view to potential threats from actors and organised groups or networks of actors in order to prevent damage to the vital infrastructure?

These research questions were identified in the Phase 1 report of the cybersecurity state-of-the-art project and by the NCTV. The overarching objectives for Phase 2 of the state-of-the-art project were to:

- Explore and develop additional knowledge across the identified research questions;
- Highlight possible areas where additional knowledge or research is required; and
- Identify possible areas for intervention by the NCTV and provide recommendations for future improvement.

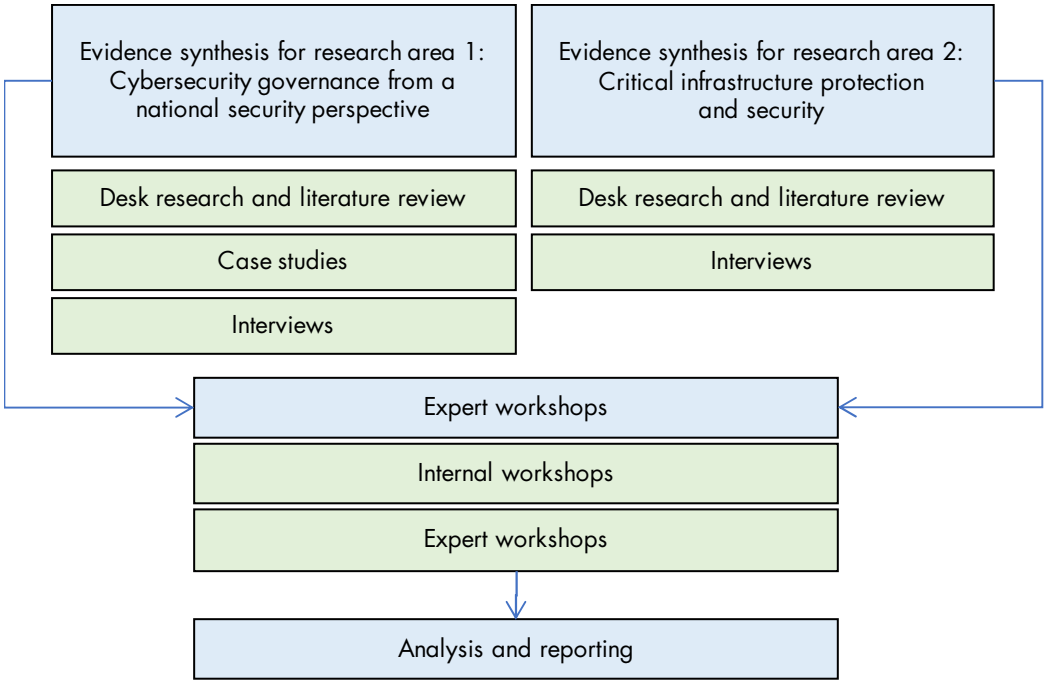
1.3. The study examined the research areas using a mixed-methods approach

To address the research questions, the study used a mixed-methods approach consisting of desk research and a literature review, case studies, interviews and expert workshops. Overall, the approach to this study was divided into four tasks:

- Task 1: Evidence synthesis for research area 1 (Cybersecurity governance from a national security perspective);
- Task 2: Evidence synthesis for research area 2 (Critical infrastructure security and protection);
- Task 3: Expert workshops; and
- Task 4: Analysis and reporting.

A high-level overview of the study approach is shown in Figure 1.1. For a complete overview of the methodology and approach adopted under each task, please refer to Annex A of this report. Annex B provides a complete list of stakeholders – and their affiliations – who were consulted.

Figure 1.1 Overview of research approach



Following the initial evidence synthesis for both research areas, the study team organised expert workshops to share the emerging findings with Dutch stakeholders, and to give them an opportunity to discuss, challenge and validate them, and ensure their relevance to the Dutch context. In addition, the expert workshops served to help identify next steps or actionable recommendations for the NCTV in relation to each research area.

The results of these external workshops led to the identification of specific knowledge gaps, priority areas for the Netherlands and specific recommendations to inform the NCTV research agenda. The study team then analysed and consolidated these outputs in a series of internal workshops before drafting the final report.

1.4. This report has two important caveats

It should be noted that the findings presented in this report are subject to two caveats, including:

- Both research areas cover topics within the field of cybersecurity that were identified as suffering from a perceived lack of research or a low-quality evidence base during Phase 1. It is therefore logical that the study team encountered a degree of difficulty in identifying and generating a robust evidence base for some of these questions under the timeframe and resources available for this study.
- This study cannot claim to capture the full perspectives of all stakeholders in the field of cybersecurity, either globally or within the Dutch context. In particular, the timeline of consultations – which were carried out during summer months and with COVID-19 restrictions on face-to-face meetings – led to lower response rates and engagement from stakeholders. However, the study team has reviewed relevant literature and conducted telephone interviews with both Dutch and international stakeholders and experts to produce analysis that is as comprehensive and representative as possible within the timeframe and resources available.

1.5. This report is structured into ten chapters and three annexes

This report outlines the findings of Phase 2 of the overarching cybersecurity state-of-the-art study, and provides a set of recommendations to inform a future NCTV research agenda.

In addition to this introduction, the report comprises nine additional chapters and three annexes:

- **Chapter 2: Cybersecurity governance in the Netherlands** explores how the current model of governance and cybersecurity initiatives in the Netherlands could be aligned and improved, and how system responsibility for cybersecurity could be set up.
- **Chapter 3: Managing cybersecurity capabilities and skills required for national security** features an overview of current challenges in the Netherlands as regards the first research area, and discusses different approaches to identify and manage skills and capabilities.
- **Chapter 4: Measuring performance for cybersecurity policymaking** explores the challenges that are relevant to the first research area when measuring performance in cybersecurity, and sets out potential approaches that could be used to overcome them.
- **Chapter 5: Recommendations for the NCTV to improve cybersecurity governance** presents a set of recommendations for the NCTV relating to the first research area.

- **Chapter 6: Critical infrastructure and technology** explores risks and challenges that are relevant to the second research area, resulting from the interplay between legacy critical infrastructure technologies and new technologies.
- **Chapter 7: Critical infrastructure and cybersecurity maturity** explores how current levels of cybersecurity maturity within the critical infrastructure sector can be measured and understood in relation to the second research area.
- **Chapter 8: Critical infrastructure and improving cybersecurity** features a discussion on what could be done to improve security of operational technology deployed in critical sectors and in relation to threats from actors and organised groups or networks of actors in the second research area.
- **Chapter 9: Recommendations for the NCTV to improve critical infrastructure protection and security** presents a set of recommendations for the NCTV relating to the second research area.
- **Chapter 10**: **Concluding remarks** are given in the final chapter, along with a summary of key findings and recommendations for the NCTV across both research areas.
- **Annex A: Methodology** sets out the approach the study team undertook to deliver this study.
- **Annex B: Interviewees and workshop participants** are listed in a separate annex.
- **Annex C: Case study country profiles** presents national cybersecurity governance approaches in Estonia, Germany, Sweden, the United Kingdom and the United States.

2. Cybersecurity governance in the Netherlands

This chapter explores the first three questions of the first research area, and consists of three sections:

- **Section 2.1** offers a brief introduction to cybersecurity governance and the Dutch governance structure, based on desk research and a literature review.
- **Section 2.2** discusses the first two research questions: how the current model of governance could be improved, and how system responsibility could be set up. This section primarily draws on interview and workshop contributions from the experts consulted by this study.
- **Section 2.3** discusses lessons from international comparisons of different national cybersecurity governance models, which is based on the case studies done for this study.

2.1. The Netherlands has a decentralised governance structure for cybersecurity

Cybersecurity governance from a national security perspective relates to three interconnected concepts, each with their own contested definitions. There is considerable debate surrounding the definitions and constituent parts of the concepts of cybersecurity, governance and national security.[2]

This study employed the NCTV's definition of cybersecurity understood as the entirety of measures employed to prevent damage due to disruption, failure or misuse of information and communications technology (ICT), and to recover capability should damage occur.[3] Similarly, the study also used the definition of national security adopted by the Dutch National Security Strategy, where national security is jeopardised if one or more critical interests of the Dutch state and/or society are threatened to such an extent that this results or could result in social disruption.[4] National security in the Netherlands spans six national security interests, as outlined in Table 2.1.

[2] For further discussion about cybersecurity, see Silfversten et al. (2019); for governance, see Adams et al. (2015); for national security, see Retter et al. (2020).
[3] Silfversten et al (2019).
[4] Ministry of Justice and Security (2019).

Table 2.1 The six national security interests of the Netherlands

National security interests	Description
Territorial security	The unimpeded functioning of the Netherlands and its EU and NATO allies as independent states in a broad sense, or territorial security in a narrow sense.
Physical security	The ability of people to go about their lives in an unimpeded manner within the Netherlands and their own physical environment.
Economic security	The unimpeded function of the economy in an effective and efficient manner.
Ecological security	The unimpeded continued existence of the natural living environment in and around the Netherlands.
Social and political stability	The continued and unimpeded existence of a social climate in which individuals are free to go about their lives and groups to coexist within and in accordance with the Netherlands' democratic and lawful state and its shared values.
International rule of law	The functioning of the international system of rules, standards and agreements established for the purposes of international peace and security

Source: Ministry of Justice and Security (2019).

Within the Dutch conceptualisation of national security, cybersecurity is seen as being interwoven into all six national security interests. It is also integrated into the territorial security interest, which then includes the availability, confidentiality and integrity of critical information services (i.e. addressing the security and protection of critical national infrastructure – see Chapter 6 for discussion).[5]

Governance can be understood as the approaches used by multiple stakeholders to identify, frame and coordinate the response to a collective problem.[6] There is a distinction between *government* and governance, where the former indicates that the government is the sole actor responsible for addressing the problem, as well as between *regulation* and governance, where regulation refers to sustained and focused control exercised by a public agency over private activities.[7] Government and regulation, therefore, play a part in governance, but governance also includes wider activities across multiple stakeholders or networks, including a wide array of relevant actors. Van Asselt and Renn (2011) argue that the concept of governance can also include descriptive analysis (e.g. observing the actors and relationships within a particular system) and normative analysis (e.g. discussing ideal ways of organising actors and their relationships).[8] Considering its constituent parts, the working definition of cybersecurity governance from a national security perspective can therefore be seen as the approaches used by multiple stakeholders to identify, frame and coordinate proactive and reactive responses to potential national security risks stemming from the cyber domain.[9]

The current cybersecurity governance model in the Netherlands is anchored in the *Polder* model of consensus-driven decision making. In practice, this means that the Dutch governance structure is a network governance model with several organisations working to ensure national cybersecurity (see Figure

[5] Ministry of Justice and Security (2019).
[6] Adams et al. (2015).
[7] Helderman et al. (2012).
[8] Van Asselt and Renn (2011).
[9] Adapted from Adams et al. (2015).

2.1), whereby each organisation is responsible for cybersecurity within their mandate and area of responsibility.[10] The main responsibility for coordinating national cybersecurity and ensuring governance from a national security perspective lies with the Ministry of Justice and Security, and specifically with the NCTV. However, due to the decentralised form of governance in the Netherlands, the Ministry and the NCTV do not have a mandate to direct other ministries or government organisations.[11]

The NCTV's responsibility is, therefore, focused on coordination of the Dutch cybersecurity response in both day-to-day operations (i.e. the 'cold' phase) and in crisis (i.e. the 'hot' phase of crisis management).[12] Its responsibilities in times of crisis are further set out in the recently published Digital Crisis Management Plan, which outlines the response to a digital crisis that could have significant social consequences.[13] The Ministry of Justice and Security also hosts the National Cyber Security Centre (NCSC), which aims to realise a safe, open and stable information society by sharing knowledge, providing insight and offering pragmatic advice.[14]

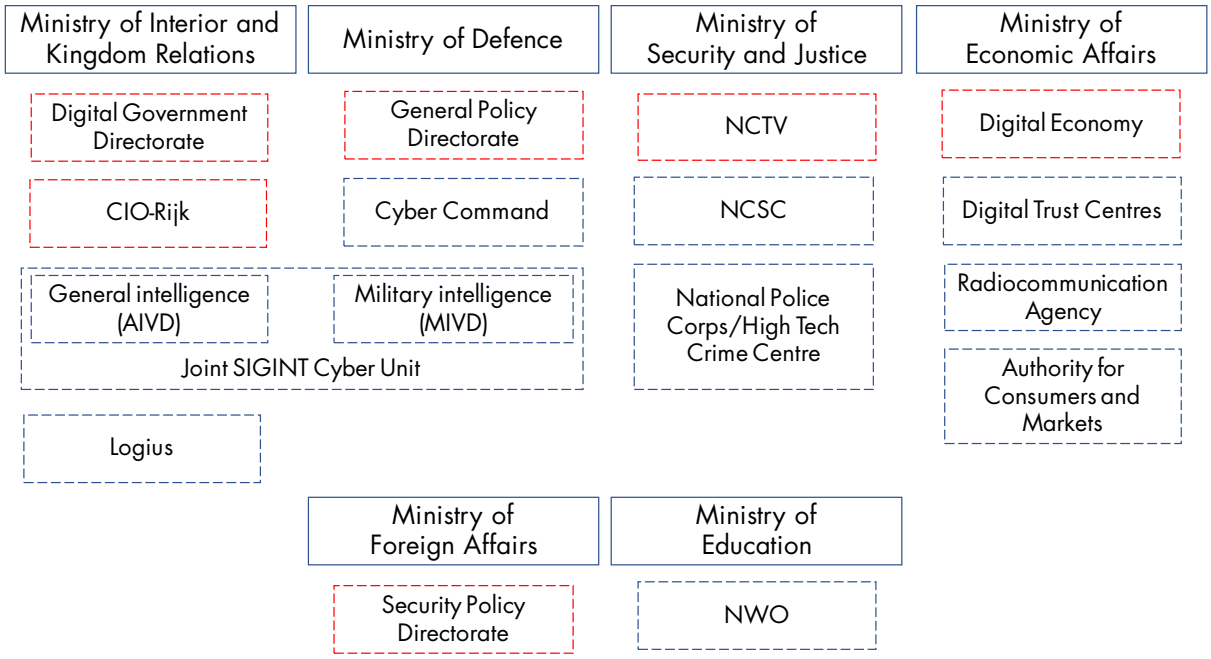
Beyond the Ministry of Justice and Security and the NCTV, the key government cybersecurity actors include the:

- Ministry of Defence;
- Ministry of Economic Affairs and Climate Policy;
- Ministry of Education, Culture and Science;
- Ministry of Foreign Affairs; and
- Ministry of the Interior and Kingdom Relations.

In addition to these government organisations, there are also several public-private partnerships that play important parts in the Dutch cybersecurity ecosystem, notably the critical infrastructure Information Sharing and Analysis Centres (ISACs), the Dutch Cyber Security Council and – up until its disbandment on 1 October 2020 – the dcypher platform.[15] Dcypher was a cybersecurity platform for higher education and research in the Netherlands launched by the Ministries of Security and Justice, Economic Affairs, Education, Culture & Science and the Netherlands Organisation for Scientific Research (NWO). Notable outputs from the dcypher platform include the National Cyber Security Research Agenda (NCSRA) and the National Cybersecurity Education Agenda.

[10] Boeke (2016).
[11] Hathaway and Spidalieri (2017).
[12] Silfversten et al. (2019).
[13] NCTV (2020).
[14] NCSC-NL (2019a).
[15] Dcypher (N.d.).

Figure 2.1 Overview of key organisations and departments with cybersecurity responsibilities



Source: RAND Europe.

2.2. This study identified potential challenges to effective governance in the Netherlands

The governance of cybersecurity is a prominent area of discussion from both a government and political perspective in the Netherlands. There are also several ongoing initiatives examining and discussing how the governance of cybersecurity in the Netherlands is working and how it could be improved in the future. This includes parliamentary discussions, questions and answer sessions in the Permanent Parliamentary Committee for Justice and Security following the Citrix incident (see Box 1),[16] and a report on digital disruption from the Netherlands Scientific Council for Government Policy (WRR).[17] The governance of cybersecurity is also emphasised in current research efforts, and is included in the NCSC research agenda[18] and in a research call on a secure and trustful digital domain from the NWO.[19] There are also upcoming initiatives that will seek to evaluate the governance of cybersecurity in the Netherlands, including an evaluation of the National Cyber Security Agenda by the WODC and an evaluation of the response to the Citrix incident by the Dutch Safety Board.[20] Lastly, the development of the National Digital Crisis Management Plan has also sought to clarify roles and responsibilities when responding to and managing incidents and crises in the digital domain.[21]

[16] Parlementaire Monitor (2020).
[17] WRR (2019).
[18] NCSC-NL (2019b).
[19] NWO (2020).
[20] RAND Europe workshop, 8 September 2020.
[21] NCTV (2020).

Box 1 Overview of the Citrix incident

In December 2019, vulnerabilities were disclosed in the Citrix Application Delivery Controller (ADC) and Citrix Gateway that, if exploited, could allow an unauthenticated attacker to perform arbitrary code execution. The two Citrix products are common networking tools that are widely used in government and private sector organisations, including in the Netherlands.[22]

Initially, Citrix published advice for administrators to take mitigating measures without applying security patches, which was considered to address the vulnerabilities. However, the advice was not entirely successful, and some systems remained vulnerable. This was further complicated by the publication of proof-of-concept exploit code, which enabled more attackers to exploit the vulnerability.[23]

The Dutch NCSC advised administrators to turn off systems until an official patch was ready and then, once patches were available, update their systems as required.[24]

Overall, participants in the RAND Europe expert workshop emphasised that while the Dutch system has its strengths and has been subject to improvements in recent years, there are several areas that could be perceived as enduring weaknesses or potential areas for improvement.[25] The WRR report on preparing for digital disruption also presents a similar view. The report concludes that, whilst the Dutch government has invested in national cybersecurity, the 'government has insufficient resources to respond adequately, certainly in view of the fact that such disruption may have adverse consequences in the physical and social realms as well, even including public confidence in constitutional democracy itself.'[26]

Altogether, this RAND study has identified the following challenges to the current governance of cybersecurity from a national perspective in the Netherlands:

- Lack of agility and proactiveness in cybersecurity policymaking;
- Unclear roles and responsibilities within the cybersecurity governance structure;
- Lack of or insufficient information-sharing;
- Lack of or duplication of regulations and standards;
- The separation of vital and non-vital infrastructure; and
- Challenges of oversight and evaluation.

The following sections discuss each of these in further detail, and present possible measures that could be taken to improve the situation in the future.

2.2.1. Unclear roles and responsibilities and a lack of proactiveness could weaken cybersecurity governance

As highlighted above, the governance of cybersecurity in the Netherlands is predominantly coordinated by the Ministry of Justice and Security and the NCTV. However, cybersecurity involves a complex ecosystem of actors spanning central, regional and local government, critical-sector industry, non-critical private-sector businesses and other cybersecurity organisations As responsibilities are ultimately

[22] Serna (2020).
[23] Cimpanu (2020).
[24] NCSC-NL (2020).
[25] RAND Europe workshop, 8 September 2020.
[26] WRR (2019).

distributed and spread out across multiple actors, some workshop participants noted that having clear roles and responsibilities across the entire system is challenging.[27] The division of responsibilities and power across different ministries may also lead to a lack of coherence in cybersecurity policy and interventions.[28] This may be due partly to competing interests between different ministries, which could also make the ministries themselves reluctant to change or giving up power, according to one interviewee.[29]

However, interviewees from national government emphasised that they believed the current model to be well-functioning and that it is important to continue working with the government organisation that has existing mandates in relation to cybersecurity matters.[30] It therefore seems that the lack of clarity of roles and responsibilities is more apparent between the national government organisations and the rest of society, rather than within national government itself. The workshop discussions suggested two possible reasons for this: the difference between the prevention and response phases of cybersecurity (e.g. the cold and hot phases) and the distinction between critical and non-critical infrastructure. The latter point is discussed separately in Section 2.2.4.

Some workshop participants emphasised that there could be a mismatch of resources and efforts placed on crisis management and reactive response, rather than in building and improving the resilience of digital society in the Netherlands. One participant also emphasised that the digital domain is fast-moving and continuously evolving, and thus different to other policy domains in which the current governance model might be better suited.[31] If resources are mainly spent on reacting to incidents and managing crises when they occur, important system-level improvements and preventative measures may be missed or neglected. Some participants noted that in a decentralised governance model within a dynamic environment, such as cyber, it is important to continuously and proactively reflect on where the system is not performing as expected and how it could be improved.[32] Some participants further noted that a proactive and preventative approach requires both a sense of urgency, adequate resources and political support, which might not currently be available. The current COVID-19 pandemic was highlighted as a good example of urgency driving and resulting in change, but it was emphasised that it is not sufficient or responsible to simply wait for significant incidents or crises to occur before seeking improvement.[33]

Even in areas with a degree of proactive change, such as digital crisis management, further work might be required. Some workshop participants expressed a need for improved clarity of responsibilities in a crisis, even though a digital crisis-management plan has been developed. Whilst a plan was noted as a strong starting point, real-life incidents are rarely straightforward and require a high level of agility and adaptability. Therefore, participants emphasised the need to improve clarity in digital crisis-management by extensively exercising their roles and responsibilities in non-emergency situations.[34]

---

[27] RAND Europe workshop, 8 September 2020.
[28] Ibid.
[29] INT03.
[30] INT05, INT06.
[31] RAND Europe workshop, 8 September 2020.
[32] Ibid.
[33] Ibid.
[34] Ibid.

2.2.2. Information-sharing challenges may reduce the effectiveness of the governance system

Adequate and productive information-sharing is fundamental to both the prevention and response phases of addressing cybersecurity threats. Insufficient information-sharing between organisations with cybersecurity responsibilities appeared as a prominent challenge in this study. Specifically, two aspects were found to be perceived as potential areas for improvement:

1. Information-sharing and knowledge relating to the state of cybersecurity within the national government; and
2. Information-sharing between organisations with a cybersecurity responsibility.

Some interviewees noted the need to comprehensively understand the state of information technology (IT) and cybersecurity across all levels of government.[35] National government ministries and departments are responsible for their own operations, investment portfolio and applications, etc., which means that all of national government retains a high degree of independence in their IT infrastructure and cybersecurity. Without clear structures in place for information gathering and sharing in order to strengthen cybersecurity, it is challenging to fully understand the varying levels of cybersecurity within national government and how to best address it.[36] However, this is actively worked on by the *CIO-Rijk* – particularly through the recently established *CISO-Rijk* position.[37] According to one interviewee, there are also challenges in understanding and sharing information between different levels of government due to the decentralised governance structure, particularly in relation to local and regional government. However, this is also an issue that the Ministry of the Interior is currently working on improving.[38]

Wider information-sharing challenges were identified during the study in relation to information-sharing between organisations with a cybersecurity responsibility within and beyond the Netherlands, including:

- Weaknesses revealed during the Citrix incident;
- Limitations and potential inefficiencies in information-sharing between NCSC, critical sectors and the rest of society; and
- A lack of focus on supply chains and dependencies in information-sharing.

The assessment of the Citrix incident illustrated that some stakeholders did not receive the right information during the incident response and crisis management phase, thereby limiting the efficiency of the response. It also showed that there are still many business sectors that do not have their own Computer Security Incident Response Team (CSIRT) or information-sharing mechanisms in place, which could mean that they are left outside key information-sharing structures.[39]

The NCSC is the main information-sharing coordinator for national government and critical infrastructure and it mainly provides vulnerability information and advisories. However, the NCSC

[35] INT01, INT04, INT06.
[36] INT04.
[37] Rijksoverheid (2020).
[38] INT01.
[39] Parlementaire Monitor (2020).

cannot receive or share information beyond its constituents, and has no central authority for distribution of threats and vulnerabilities beyond the NCSC.[40] The workshop participants also emphasised that there are restrictions to what the NCSC can do with the information it has, particularly due to the NIS Directivend the General Data Protection Regulation (GDPR) limitations.[41] The NCSC is supported in information-sharing by the Digital Trust Center (DTC) programme, which was launched in 2017 by the Ministry of Economic Affairs and Climate Policy and the Ministry of Justice and Security. The DTC's aim is to leverage the information developed by the NCSC by tailoring and distributing it to its audience of small- and medium-sized businesses outside the critical infrastructure sectors.[42] However, it should be noted that at this stage, the DTC has no information position itself but depends on information from NCSC, and does not currently gather or share information to the NCSC.[43]

Most workshop participants highlighted that the most prominent limitation of the current information-sharing structure is its foundation in the distinction between critical and non-critical infrastructure. As the NCSC can only share information to national government and critical infrastructure organisations, some workshop participants stressed that information may not adequately reach the NCSC or be adequately distributed to those organisations that need it.[44] Therefore, some participants argued for a more 'bottom-up' information-sharing approach to enable more horizontal information-sharing across industry, regardless of their status as critical infrastructure or not. Several potential options were presented, including:

- Setting up a network or system whereby those who have found the vulnerability can contact the affected party directly, rather than waiting for the NCSC to reach out to industry. One way of implementing this approach could be to include a company's IT department contact details in the Chamber of Commerce's registry of IP addresses.[45]
- Engaging in more proactive scanning of sectoral networks for vulnerabilities. As sector-related organisations are more likely to work together, they would more likely know who to contact in order to mitigate any identified vulnerabilities. [46]
- Expanding the mandate of the NCSC beyond national government and critical infrastructure. This would not necessarily mean that the NCSC would have to serve all organisations, but rather a targeted expansion to those organisations that may have the most security impact, for example Dutch network operators. [47]

The workshop discussions further emphasised the need to understand information-sharing dependencies. Some sources of information on vulnerabilities and threats that are used by the Netherlands to develop situational awareness and strengthen digital resilience might originate from foreign partners (e.g.

[40] INT03.
[41] RAND Europe workshop, 8 September 2020.
[42] Ministry of Economic Affairs and Climate Policy (2018).
[43] INT03.
[44] RAND Europe workshop, 8 September 2020.
[45] Ibid.
[46] Ibid.
[47] Ibid.

international Computer Security Incident Response Team (CSIRTs), etc.) or the private sector (e.g. companies outside the Netherlands). This may present a potentially overlooked aspect of information-sharing, and could be important to consider in relation to digital sovereignty and autonomy.[48] Lastly, workshop participants noted a lack of wider information-sharing beyond vulnerability information, particularly in relation to supply-chain structures and dependencies.[49]

2.2.3. Challenges related to lack of – or duplicated – regulations and standards could add complexity within the governance system

Some experts argued that the decentralised governance model and division of powers amongst different ministries could lead to a lack of coherence in regulation, with competing or contradicting requirements.[50] Two interviewees noted that this is particularly challenging in relation to local and regional government, and how national regulations or standards translate into the local and regional context is sometimes unclear.[51] Beyond national government, the current governance structure is built on units of governance that are as small as possible, with the most possible responsibility within their area. Municipalities are largely independent, and each town has its own council, with a degree of decision-making power. However, some functions may be centralised.[52] The two interviewees noted that this system was originally created to solve local problems, which it is well-suited for, but it may be less suited to the virtual and boundaryless nature of cybersecurity. In practice, this could mean that one department or organisation might receive several cybersecurity regulations or guidance from different authorities, making it challenging to implement, as well as improve and assure cybersecurity overall.[53]

In addition to potential duplication of regulations and standards, several interviewees also highlighted the lack of common or minimum cybersecurity standards for government (across all levels), and a lack of common or minimum security standards for service providers to government or industry at large.[54] As each public sector organisation is responsible for their own cybersecurity, there is no single, overarching and legally binding or minimum cybersecurity standard for government (beyond the EU Directive on security of network and information systems (Network and Information Security (NIS) Directive)).[55] More proactive and enforceable minimum standards could, therefore, help to harmonise cybersecurity arrangements and address varying maturity levels across government.

2.2.4. The distinction between critical and non-critical infrastructure may hamper efforts within the governance system

One of the most prominent issues that emerged from the interviews and workshop discussions was the pivotal role that the distinction between critical and non-critical infrastructure plays in the Dutch governance structure. Originally, approaches to critical infrastructure protection were developed to

[48] RAND Europe workshop, 8 September 2020.
[49] Ibid.
[50] INT01; RAND Europe workshop, 8 September 2020.
[51] INT01.
[52] VNG (2018).
[53] INT01.
[54] INT01, INT04, INT05, INT06, INT07.
[55] The NIS Directive is referred to as *Wet beveiliging netwerk- en informatiesystemen (Wbni*) in Dutch.

address the security of largely physical infrastructure.[56] However, modern Dutch society is increasingly characterised by a focus on a digital Netherlands and a growing dependency on digital infrastructure and connectivity, which entails a closer integration of physical and digital infrastructure across all critical sectors.[57] This might mean that the approaches, processes and structures currently in place for protecting critical infrastructure could be less well-suited for the protection of modern digital infrastructure.[58]

The distinction between critical and non-critical infrastructure has several implications for cybersecurity: critical infrastructure is subject to additional legislation and regulation[59] and mandatory incident-reporting requirements,[60] and is part of the NCSC information-sharing structure.[61] As noted above, this could mean that non-critical providers and services are subject to less stringent security requirements, and may miss out on important security advice. The aftermath of the Citrix incident and the WRR report on digital disruption also highlighted that the process of identifying critical services might require improvement.[62] Currently, each ministry and sector regulator identifies and designates critical processes and providers within their sector (if it has been designated as a critical sector). This high-level assessment takes place largely without input from the NCSC and is also done on a sector-by-sector basis, and not on a whole-of-society level.[63] As illustrated in the Citrix case, this may mean that the process fails to adequately capture dependencies, both across sectors and across supply chains, and the pervasive connections between digital and physical services.[64] One workshop participant further noted that even though a criticality is assessed on a sectoral basis, not every process in the sector is vital, and it could be more constructive to take a more granular approach to the identification of critical infrastructure.[65]

During the workshop two possible approaches were raised to overcome these challenges: a more generic approach to critical infrastructure identification that is less tied to specific sectors, and a more 'bottom-up' approach where providers can self-assess and identify themselves as critical. Participants emphasised that trying to identify specific sectors as critical could be challenging, given the high levels of interdependencies and interconnectivity between digital services. Instead, they discussed the possibility of adopting a more generic approach that is applicable across sectors, dictates responsibility and accountability for failure and emphasises minimum security and resilience standards for all organisations. However, there was no agreement in relation to the feasibility of such an approach.[66] Participants also discussed the possibility of companies self-assessing and self-identifying as critical rather than relying on the government to nominate critical providers. However, participants expressed concerns that such an approach could result in inaccurate assessments (e.g. non-critical providers identifying as critical), and

[56] RAND Europe workshop, 8 September 2020.
[57] WRR (2019).
[58] RAND Europe workshop, 8 September 2020.
[59] E.g. the NIS Directive.
[60] See NCSC-NL (n.d.).
[61] INT03.
[62] RAND Europe workshop, 8 September 2020; WRR (2019).
[63] INT03.
[64] RAND Europe workshop, 8 September 2020.
[65] Ibid.
[66] Ibid.

voiced concerns about its feasibility, as organisations may not understand their current security postures or how critical they are to other organisations (thereby not realising that they are vulnerable or critical).[67]

2.2.5. Challenges of oversight and evaluation may make it difficult to understand how well the system is working

The final challenge highlighted in interviews and the workshop discussion was the difficulty of enforcing, evaluating and assuring cybersecurity across the various actors in the Dutch ecosystem. As noted above, currently there is no enforceable government-wide cybersecurity standard – each government organisation maintains its own cybersecurity arrangements. The NCSC is also limited in this regard by its largely advisory role. The NCSC gathers and shares information and vulnerability advisories to its constituents (national government and critical infrastructure private-sector organisations), but it does not have a good understanding of how this information is used or actioned. This means that known vulnerabilities and security weaknesses could go unaddressed.[68] However, the NCSC and CIO-Rijk have recently begun to operate a 'comply or explain' approach where national government and critical infrastructure organisations must act on recommendations or explain why they are not following the security advice to the NCSC or CIO-Rijk. However, there are currently no clear penalty structures or financial costs to organisations in the case of non-compliance.[69] Interviewees from the NCSC also emphasised that the responsibility for evaluating the cybersecurity of critical infrastructure providers is not within the mandate of the NCSC, but lies with each sector's inspectorate/supervisory authority, which could also make it challenging to produce a view of the maturity across different sectors.[70]

The workshop participants expressed different opinions on how to improve oversight in this regard. One participant noted that it may be necessary for the NCSC to have an enforcement role and to be able to force organisations to implement security advice. On the other hand, two participants highlighted that this approach might actually be detrimental to the NCSC's ability to build trust and proactively work with its constituents, particularly within the private sector. These organisations may also become more reluctant to share information with the NCSC, which could reduce the overall value proposition of the NCSC.[71] One of the participants further noted that the comply or explain approach could be difficult to achieve as many private organisations simply do not know that they are vulnerable or that their mitigation measures are ineffective.[72] There was some agreement that legislation is required in order to ensure compliance, but less agreement to exactly what would need to be changed. Two participants highlighted that there is already significant legislation, but what is missing is harmonisation and standardisation.[73]

[67] RAND Europe workshop, 8 September 2020.
[68] INT05.
[69] INT04, INT05.
[70] INT05.
[71] RAND Europe workshop, 8 September 2020.
[72] Ibid.
[73] Ibid.

2.3. International case studies can only offer limited lessons for the Dutch governance system

One of the research questions (RQ1.3) for this study referred to the lessons that could be identified through international comparisons of different national governance models for cybersecurity. To help answer this question, the study team developed five case-study country profiles of national governance approaches for Estonia, Germany, Sweden, the United Kingdom and the United States. The case studies were selected in consultation with the NCTV and the study's Scientific Advisory Committee (SAC), and were chosen to illustrate a range of different governance approaches and national systems, including smaller and larger economies. The case studies were pursued to develop brief country profiles that could help inform two overarching aspects:

1. A high-level overview of the national governance approach used in the country; and
2. The results of any evaluations or assessments of the governance approach that could help identify lessons or good practice for the Netherlands.

This section summarises the lessons that emerged from these case studies; the full country profiles can be found in Annex C to this report.

One of the overarching challenges when comparing national governance approaches is the lack of evaluation and performance metrics of cybersecurity governance, which makes it difficult to understand how well each respective governance system is functioning.[74] In other words, case study analysis can illustrate how different countries have approached their governance structure but cannot fully answer what makes them work (or not work) within their national structures, or how each nation's performance compares to other approaches. Nevertheless, several findings and lessons can be drawn from the four case studies:

- While the case study countries have different governance structures in place, all of them emphasise a 'whole-of-society' approach to national cybersecurity that involves a broad spectrum of government ministries, departments and organisations, as well as public-private partnerships in key areas such as critical infrastructure protection.
- The primary strategic objectives and priorities as outlined in national cybersecurity strategies are largely coherent across the case study countries.
- Governance structures have largely emerged out of the specific historical, cultural and political contexts within each country. This is largely also the case with the Netherlands (as was discussed in Section 2.1).
- The publicly available assessments, evaluations and investigations into the performance or outcomes of national cybersecurity governance illustrate that countries continue to struggle with the performance of their national cybersecurity ecosystems. Whereas all countries have continued to invest in national cybersecurity capabilities, they are also reported to suffer from weaknesses,

[74] Different approaches to evaluating cybersecurity are discussed further in Chapter 4.

inefficiencies and vulnerabilities in this space – including in their governance structure. This illustrates that the governance of cybersecurity from a national perspective is still a work in progress, and that countries continue to adjust their structures and adapt in response to an agile and evolving cyber domain. Again, this highlights the need for clear and transparent assessment and evaluation of cybersecurity governance so that those resources can be used to improve governance regimes in the future.

- Several of the identified weaknesses or challenges also align with those identified in the Netherlands. Particularly, the challenge of unclear roles and responsibilities is reported in both Germany and the US, illustrating the overarching difficulties in organising governance in federal or distributed political systems with many involved stakeholders.
- Some countries, particularly Estonia and the UK, use cybersecurity standards or minimum requirements to build harmonised cybersecurity capabilities across the national cybersecurity governance ecosystem. This does not necessarily strengthen the governance structure itself, but can help strengthen national cybersecurity overall.

Overall, the case studies illustrate the choices and challenges governments face in determining how to best organise the governance of cybersecurity from a national security perspective, and that it very much remains a work in progress. They also illustrate the limited value that brief country profiles can offer to the Dutch governance system in terms of lessons learned or good practice, highlighting that more in-depth reviews or comparative benchmarking may be required to fully inform future cybersecurity governance. Particularly, longitudinal comparative evaluations of governance mechanisms and the underlying factors that contribute to success or failure are currently lacking. Nevertheless, the case studies also highlight that there could be specific aspects of other national governance structures from which the Netherlands can learn, as highlighted in the following chapters.

3. Managing cybersecurity capabilities and skills required for national security

This chapter covers the fourth research question of the first research area, exploring how capabilities and skills required across stakeholders and functions for national cybersecurity can be identified and managed. It consists of three sections:

- **Section 3.1** offers a brief introduction of Dutch efforts to strengthen cybersecurity capabilities and skills based on desk research and literature review.
- **Section 3.2** highlights three overarching challenges identified by interviewees and workshop participants in relation to cybersecurity skills from a national security perspective.
- **Section 3.3** features an overview of several possible approaches to mitigate the cybersecurity skills and workforce challenges facing the Netherlands, drawing on further desk research and a literature review.

3.1. There have been several national efforts to strengthen Dutch capabilities and skills within the cyber domain

This study was tasked with exploring the evidence base on the capabilities and skills that are required – across stakeholders and across functions – to ensure national cybersecurity in the Netherlands. The Dutch government has emphasised the importance of having appropriate and sufficient depth of capabilities and skills in place to ensure a digitally secure Netherlands, particularly from a national security perspective. Building a domestic pool of relevant cybersecurity capabilities and skills also helps the Netherlands avoid a reliance on other countries, enhancing sovereignty, freedom of action and security of supply.[75]

Cybersecurity knowledge and skills are also recognised as a priority area in the current Dutch Cyber Security Agenda (NCSA), which sets out the ambition for the Netherlands to lead the way in the field of cybersecurity knowledge development. This priority area contains three interrelated objectives for:

- The Netherlands to conduct high-quality cybersecurity research.
- The Netherlands to have a long-term knowledge development programme under which the academic community develops and improves high-quality knowledge, and there are sufficient academics available to acquire an independent knowledge position in the area of cybersecurity.

[75] NCSC-NL (2018).

- Citizens and businesses to be able to see the importance of addressing digital threats and becoming more resilient to cybercrime.[76]

Given these ambitions, there have also been several national efforts to strengthen Dutch capabilities and skills within the cyber domain, including the establishment of dcypher by the Ministry of Justice and Security, the Ministry of Education, Culture and Science, and the Netherlands Organisation for Scientific Research (NWO) in 2016. Most of these efforts have not been specifically designed to meet national security objectives, but have helped the Netherlands to become more digitally secure. Amongst other things, dcypher developed a National Cybersecurity Education Agenda and a series of National Cybersecurity Research Agendas.[77] As of 1 October 2020, the dcypher platform has now been disbanded and, under the leadership of the Ministry of Economic Affairs and Climate Policy, the various departments originally involved plan to set up a new innovation platform for cybersecurity that also includes education and training.[78]

Although considerable investment has been made into cybersecurity capabilities and skills within the Netherlands in recent years, this study also identified three challenges to managing skills from a national security perspective that are explored in the following section. The focus of this study was not to identify specific skills gaps or requirements, but rather to explore potential methods or approaches for addressing skills and workforce issues, which are presented in Section 3.3.

3.2. Cybersecurity capabilities and skills are essential to national security, but are challenging to understand in detail

Interviewees and workshop participants highlighted three overarching challenges in relation to cybersecurity skills from a national security perspective[79]:

1. The distributed responsibility for workforce management issues;
2. The lack of commonly accepted and shared language; and
3. Recruitment and retention issues.

Each of these challenges is discussed in the following sections.

3.2.1. The distributed responsibility for workforce management issues

Within the decentralised governance structure of the Netherlands, each ministry is responsible for its own cybersecurity workforce and its cyber skills development and sustainment. While this is not necessarily a challenge in itself, some interviewees expressed a concern about the lack of a comprehensive governmental and national view of the cybersecurity skills that are available and needed.[80] This could mean that there is limited agreement on the specific types and quantity of skills that are needed for national cybersecurity, particularly as different organisations organise their national cybersecurity capacities in different ways. As

[76] NCSC-NL (2018).
[77] Dcypher (n.d.).
[78] INT05.
[79] RAND Europe workshop, 8 September 2020; INT03, 04, 05.
[80] INT03, 04, 05.

noted in the section above, there have been various efforts to develop cybersecurity skills in the Netherlands, for example through the National Cybersecurity Education Agenda, but according to one interviewee it remains a priority area to address.[81] Another interviewee argued that this is particularly the case for skills from a national perspective, an area in which the NCTV is trying to develop its role further.[82]

Lastly, one interview also noted that distributed responsibility also applies to universities and other education institutes, and that a decentralised approach to cybersecurity education could lead to a practical-theoretical disconnect. This might result in university education that is not well-suited for the needs of national security organisations in the Netherlands.[83]

3.2.2. The lack of commonly accepted and shared language

One of the inherent challenges in examining the capabilities and skills required across Dutch stakeholders and governmental functions to ensure national cybersecurity is the diverse definitions utilised when describing such employees, their roles and their skill sets. As with the concept of 'cybersecurity' itself, definitions are plentiful and contested, ranging from including 'professionals in information technology' to 'information security' to anyone who has a cybersecurity responsibility in their job role, regardless of their level of actual qualifications or training. Cybersecurity emerged from the field of computer science and was for a long time regarded as a technical domain, particularly concerned with securing the confidentiality, integrity and availability of technical systems, networks and information. However, the increasing digitisation of society has led to significant growth in both the number of cyber-related occupations and the breadth of work roles that have come to comprise a cyber component. The cyber domain is fast moving and continuously evolving, and so are its associated knowledge areas and skills. While early cybersecurity professionals largely had a technical focus, recent years have seen increasing demand for individuals with additional management or commercial skills in order to better integrate cybersecurity into day-to-day operations and services. Cybersecurity is no longer seen as a niche technical area, but rather as a consideration in all areas of society; just as the Dutch National Security Strategy recognises the importance of cybersecurity across all six national security interests, there is a need for cybersecurity capabilities and skills across all areas.[84]

This may be a simple requirement for a basic level of cybersecurity awareness for everyone, or a more complex requirement for cybersecurity skills integratied into established, roles such as government procurement officers or lawyers. Cybersecurity capabilities and skills are as such not confined to a single technical profession, but instead represent an 'umbrella' profession that can include a variety of work roles and encompass an extensive breadth of cybersecurity knowledge, skills and occupations.[85] Within the Dutch context, there is not a single, commonly agreed taxonomy for cybersecurity skills or professions, which makes it challenging to understand the current situation in the Netherlands and how to best

[81] INT04.
[82] INT05.
[83] INT03.
[84] Ministry of Justice and Security (2019).
[85] NCSC-NL (2018).

improve it.[86] However, the Platform for Information Security (PvIB) has produced broadly accepted cybersecurity job profiles, knowledge and skills based on the European e-Competence Framework (c-CF), which could see more uptake and use in the coming years. Within the Dutch system, it is also impossible to track cybersecurity personnel in the government, as the current system registers personnel to functions rather than specific cyber roles (e.g. a Chief Information Officer may be registered as a generic manager).[87] This makes it challenging to understand the distribution of capabilities and skills that exist across stakeholders within the system.

3.2.3. Recruitment and retention challenges

Interviewees also emphasised that a wide range of skills is needed for cybersecurity from a national security perspective, including technical cybersecurity skills, skills to communicate the issue efficiently to stakeholders and to transfer knowledge to stakeholders, skills for cybersecurity policymaking, and skills to cooperate with other countries.[88] The growing importance of cybersecurity is not only reflected in the breadth of skills required but also in increasing difficulties to find the right people, and recruit and retain them – particularly as government organisations recruit largely from the same finite labour pool.[89]

Recruitment and retention challenges are well-known and common challenges in the cybersecurity domain for government and the private sector alike, though the latter might at least benefit from the ability to offer more lucrative pay than is possible in the public sector.[90] Many organisations have engaged in new ways of recruitment, including the use of aptitude tests, challenges, competitions, hackathons, education initiatives and strategic partnerships to attract cybersecurity professionals. This also includes the use of financial incentives and other benefits such as recruitment bonuses and tuition waivers and scholarships. In such a competitive labour market, government organisations might face challenges in recruiting cybersecurity professionals and ensuring access to the right skills for national security, especially in-house, but also through outsourcing and partnership arrangement with the private cybersecurity industry.

3.3. This study identified several possible approaches to mitigate cybersecurity skills and workforce challenges facing the Netherlands

Through desk research and a literature review, this study identified several approaches and interventions that may help to address the three challenges outlined above, including the use of:

- An easily accessible knowledge base to foster a shared understanding of the cybersecurity field;
- Workforce strategies to help align cybersecurity skills efforts across government;

[86] INT03.
[87] INT04.
[88] INT04, INT05, INT06.
[89] INT06.
[90] E.g. Lyon (2020).

- Competency frameworks and career paths to streamline workforce management, skills development and sustainment; and
- Training-needs analysis to help identify required skills across functions and stakeholders from a national security perspective.

These are explored in further detail in the following sections.

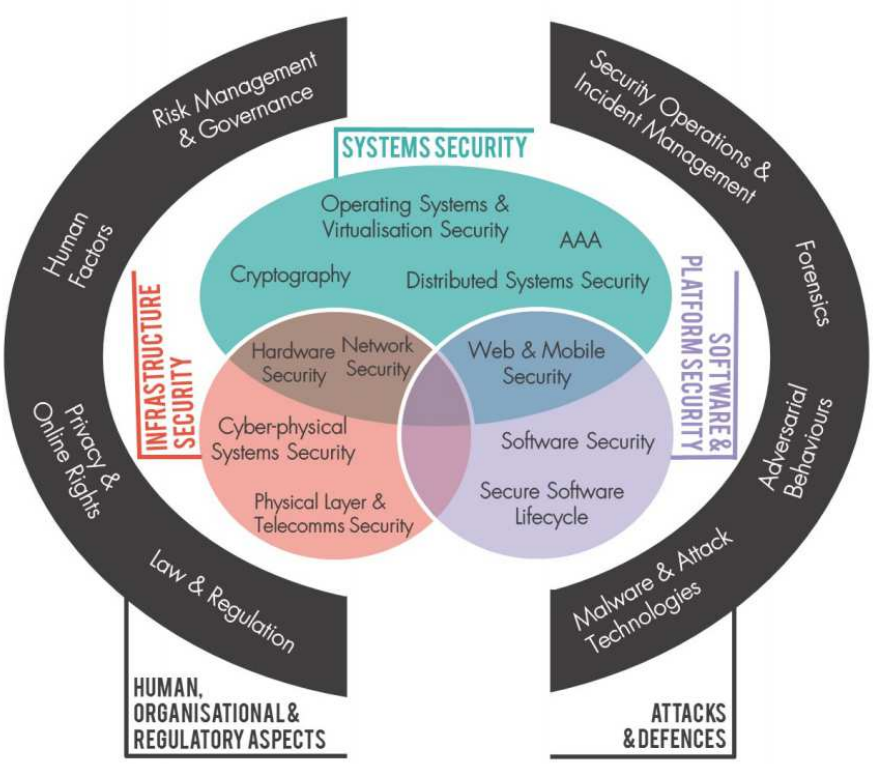
3.3.1. A common body of knowledge to help create a shared understanding of the cybersecurity field

The first phase of this cybersecurity state-of-the-art project previously investigated the cybersecurity field and noted the difficulties in defining and delineating the domain itself.[91] More mature scientific disciplines, such as chemistry, mathematics and physics, have established foundational knowledge, research paths and clear progression from primary and secondary school to university. In contrast, cybersecurity is still perceived as an emerging area where foundational knowledge is not adequately understood and a clear progression of learning is missing.[92]

Within this context, a common body of knowledge can help to build a shared understanding of the cybersecurity field and the knowledge and skills required within its various areas. The Cyber Security Body Of Knowledge (CyBOK) project – led by the University of Bristol and funded by the UK National Cyber Security Centre (UK NCSC) – seeks to bring cybersecurity into line with the more established sciences by distilling knowledge from major internationally recognised sources to form a body of knowledge that will provide the foundations for the emerging cybersecurity field. Ultimately, the CyBOK project aims to inform and support education and professional training in cybersecurity, particularly in relation to the knowledge dependencies for particular learning pathways.[93] As shown in Figure 3.1, the CyBOK is divided into 19 top-level Knowledge Areas (KAs), grouped into five broad categories, and covers the full spectrum of the cybersecurity domain. The CyBOK also acknowledges that the KAs and their groupings into categories are not orthogonal (i.e. they might overlap), and that there are dependencies across the KAs, as well as several unifying principles and cross-cutting themes that underpin the CyBOK.

[91] Silfversten et al. (2019).
[92] Silfversten et al. (2019).
[93] CyBOK (n.d.).

Figure 3.1 The CyBOK Knowledge Areas



Source: Martin et al. (2019).[94]

The CyBOK project is a publicly available resource that could be used to help develop a better understanding of the knowledge and skills required across cybersecurity in the Netherlands, which in turn could help target subsequent efforts to strengthen the cybersecurity workforce. Within the Dutch context, the PvIB's job profiles for information security could also be useful when examining knowledge and skills requirements for cybersecurity professionals.[95]

3.3.2. Workforce strategies to help align cybersecurity skills across government and further the understanding of collective capabilities and skills

Some countries develop and implement cybersecurity workforce strategies to manage and develop their national cybersecurity skills and workforce. Within this context, a national cybersecurity workforce strategy is intended to assist government organisations in achieving a cohesive workforce approach that can join strategic priorities and desired cybersecurity capability outcomes with a range of workforce interventions. A US Government Accountability Office (GAO) review of good practice in workforce planning shows that a workforce strategy should comprise at least the following components:

1. Alignment of workforce plans to an overarching strategic plan (e.g. the translation of desired outcomes into activities needed to be carried out to achieve the stated goals and objectives).

[94] CyBOK© Crown Copyright, The National Cyber Security Centre 2018, licensed under the Open Government Licence (National Archives, n.d.).
[95] PvIB (2017).

2. Identification of the type and number of cyber professionals needed to carry out the desired activities, alongside the definition of roles, responsibilities, knowledge, skills and abilities for these professionals.
3. Development of strategic recruitment interventions to address current, mid- and long-term recruitment needs.
4. Development of appropriate compensation and retention benefits.
5. Development of appropriate training, education and professional development opportunities to achieve the strategic aims and objectives.[96]

In the cybersecurity domain, the US Federal Cybersecurity Workforce Strategy illustrates how this could be translated into a cybersecurity context. This strategy, launched in 2016 by the Office of Management and Budget (OMB), was developed to 'identify, expand, recruit, develop, retain, and sustain a capable and competent workforce in key functional areas to address complex and ever-evolving cyber threats'.[97] The OMB's strategy comprised four overarching priorities to:

1. **Identify cybersecurity workforce needs** to improve government-wide understanding of the cybersecurity workforce and identify key capability and capacity.
2. **Expand the cybersecurity workforce through education and training by** working with educational partners on cybersecurity education, from primary school through to university level, in order to significantly expand the pipeline of skilled cybersecurity talent.
3. **Recruit and hire highly skilled talent** by engaging in government-wide and agency-specific efforts to expand the cybersecurity workforce.
4. **Retain and develop highly skilled talent** by promoting a government-wide approach to retention and development to support the continued enhancement of the cybersecurity workforce.[98]

The workforce strategy was further supported by the National Initiative for Cybersecurity Education (NICE) National Cybersecurity Workforce Framework, which is used by federal agencies to examine specific cybersecurity and cyber-related work roles and identify personnel or skills gaps.[99] This type of competency framework is further discussed in the following section.

Addressing issues related to cybersecurity skills and workforces is a complex policy challenge. Such policy challenges typically benefit from a strategic approach that coordinates multiple government ministries, funding streams and policy initiatives towards a common strategic aim, with clearly defined roles and responsibilities. Within the Dutch context, an overarching cybersecurity workforce strategy could enable central and local government to develop joint situational awareness of the size, shape and gaps in the national cybersecurity workforce, identify joint priorities and ensure sufficient cybersecurity skills within government, including from a national security perspective.

[96] US GAO (2011).
[97] Executive Office of the President (2016).
[98] Executive Office of the President (2016).
[99] NIST (2017).

3.3.3. Competency frameworks to be used to create a shared vocabulary for cybersecurity capacities and skills

As noted in the section above, the ability to clearly define and understand the cybersecurity workforce is one of the primary enablers to strategic workforce management. A competence framework can help organisations to map the roles, responsibilities, knowledge, skills and abilities that are relevant to the cybersecurity activities and tasks they carry out.[100] While competence or workforce frameworks might have different focuses, they typically share a number of common components, such as descriptions of:

- Broad categories of responsibilities and the respective occupations or work roles within each individual category;
- Expected tasks for each role;
- Expected knowledge, skills and abilities for each role; and
- Competence levels that the knowledge, skills and abilities can be assessed against (which could include formal qualifications or certifications).

Within the cybersecurity field, the US Workforce Framework for Cybersecurity (NICE Framework)[101] (outlined above) is one of the most prominent competence frameworks, and acts as a fundamental reference for describing and sharing information about cybersecurity work in the United States.[102] The NICE Framework establishes a taxonomy and common vocabulary to describe cybersecurity work intended to be applied in the public, private and academic sectors. The NICE Framework effort has three overarching objectives: [103]

1. **Accelerate learning and skills development** and inspire a sense of urgency in the public and private sectors to address the shortage of cybersecurity workers and skills.
2. **Nurture a diverse learning community** to strengthen education and training across the ecosystem and diversify the cybersecurity workforce.
3. **Guide career development and workforce planning** and support public and private sector employers to address market demands and enhance the recruitment, hiring, development and retention of cybersecurity professionals.

The NICE Framework consists of three levels of information[104]:

- **Categories (7):** a high-level grouping of common cybersecurity functions;
- **Specialty Areas (33):** distinct areas of cybersecurity work; and

[100] According to the US GAO, the adoption of the NIST NICE framework and the implementation of associated workforce initiatives have led to overall improvements in the US federal cybersecurity workforce (see US GAO, 2017).
[101] Also referred to as NIST Special Publication 800-181.
[102] There are also other competence frameworks within this field, such as the European e-Competence Framework (e-CF), see European e-Competence Framework (n.d.).
[103] NIST (2020).
[104] A more detailed overview of the NICE Framework can be found on the framework website. See NIST (N.d.a).

- **Work Roles (52):** groupings of cybersecurity work with specific knowledge, skills and abilities required to perform tasks in a work role.

The NICE Framework was developed by the US federal government but aims to help both public and private sector employers, current and future cybersecurity professionals, training and certification providers, education providers and technology providers.[105] The CyberSeek initiative – a recruitment platform run by Burning Glass Technologies and the Computing Technology Industry Association (CompTIA) and the National Institute of Standards and Technology (NIST) – also uses the NICE Framework to provide detailed, actionable data about supply and demand in the cybersecurity job market and facilitate the recruitment of cybersecurity professionals.[106] The CyberSeek platform makes it easier to understand where there are cybersecurity vacancies and in which roles demand is high, and offers a one-stop platform for jobseekers and employers.

3.3.4. Training-needs analysis and career paths to help identify the required skills across functions and stakeholders and facilitate progression of cybersecurity professionals

At the more granular level, training-needs analysis (TNA) can be used to identify particular development needs for the skills required across functions and stakeholders in cybersecurity. TNAs are an established way of approaching education, training and skills development. A TNA is designed to identify the training needs of a target audience (i.e. what is their role or occupation, and do they need to acquire new knowledge to carry out their work?). A training gap can be one of two types:

- A gap in terms of the difference between education and training currently available and the desired provision of education and training.
- The difference between the current skills or performance of a worker and the desired skills or performance.

Competence frameworks could, therefore, help organisations to understand where performance gaps currently exist by comparing their workforce to a standardised list of roles and their associated knowledge and skills.[107]

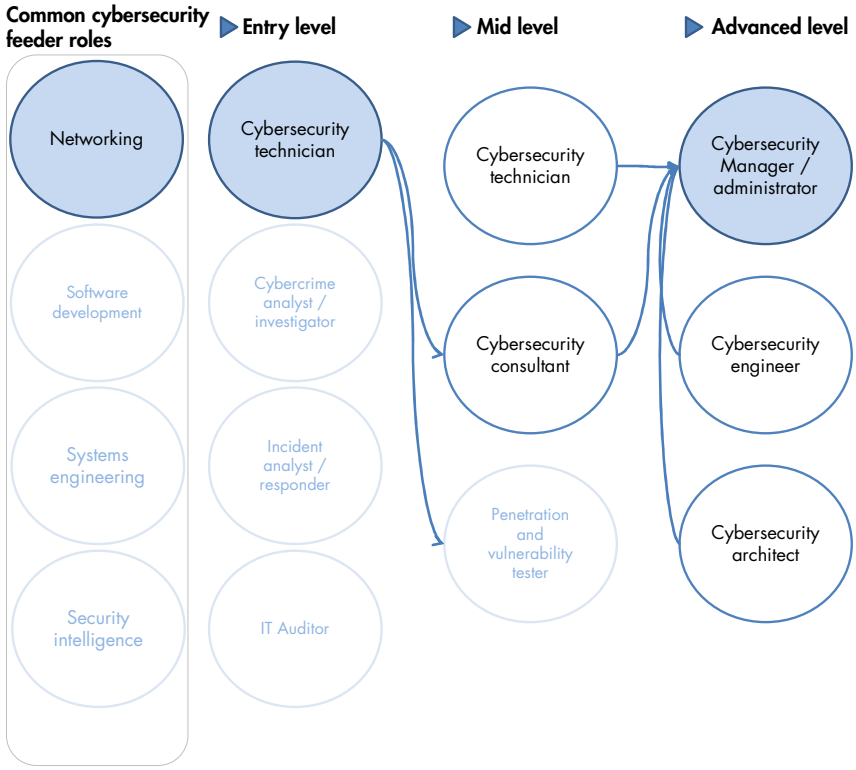
In addition to identifying training needs, it is also important to be able to detail the career progression of cybersecurity skills and knowledge (i.e. how personnel can progress in a specific role within a competence framework or move between different roles). Career paths are typically understood as a series of structured skills and knowledge requirements, often aligned with the relevant education and training programmes, that allow a cyber professional to consolidate and advance their skills and ultimately, their seniority, responsibility and rewards package. US GAO (2011) and Chappelle et al. (2013) argue that cyber career paths are important to organisations for several reasons[108]:

[105] NIST (n.d.b).
[106] See Cyber Seek (n.d.a). See also the CyberSeek interactive heatmap for the US cybersecurity labour market (Cyber Seek, n.d.b).
[107] US GAO (2017).
[108] US GAO (2011) and Chappelle et al. (2013).

- Clearly defined work roles and progression between roles make it easier to map requirements and develop workforce projections.
- Clear progression requirements make it easier to develop appropriate education, training and professional development interventions.
- Clear career paths can assist and help improve retention and employee job satisfaction, which is essential in a competitive labour market.

Career pathways are not always linear and often allow for several different paths that a cyber professional can take to reach any given position or seniority level, as seen in Figure 3.2. This helps to ensure flexibility in progression opportunities, which is especially well-suited to the dynamic and constantly changing nature of the cybersecurity labour market.

Figure 3.2 NICE Cybersecurity career pathway[109]



Source: RAND Europe based on Cyber Seek (N.d.c).

The development and application of coordinated TNA and career paths across government in the Netherlands could, therefore, help strengthen national cybersecurity in several ways, including by:

- **Facilitating the recruitment and development** of cybersecurity professionals.
- **Making it easier for cybersecurity professionals to move** between government agencies, thereby increasing information-sharing, skills sharing and retention of skills and expertise within the government.

[109] An interactive version of the CyberSeek career path can be found at the CyberSeek website. See Cyber Seek (n.d.c).

- **Further strengthening the education pipeline** of current and future cybersecurity professionals in the Netherlands.
- **Helping to minimise the risk of discrepancies** between theoretical knowledge and cybersecurity education and the practical skills needed in the private and public sectors.

4. Measuring performance for cybersecurity policymaking

This chapter covers the fifth research question of the first research area, exploring how efficiency and effectiveness could be measured for cybersecurity policymaking. It consists of three sections:

- **Section 4.1** offers a brief introduction to performance measurement, including definitions of key concepts and terms.
- **Section 4.2** explores why measuring performance is challenging within the cybersecurity domain.
- **Section 4.3** features an overview of several possible approaches to measure and evaluate different aspects of cybersecurity performance to better inform policymaking.

This chapter primarily draws on sources identified through desk research and literature review.

4.1. Performance measurement can take many forms and encompasses a variety of auditing and evaluation approaches

This chapter pertains to how the effectiveness of cybersecurity policies, governance structures and other interventions can be measured, thereby ensuring accountability and enabling improvement over time. The process of measuring performance can take many forms and encompasses a variety of auditing and evaluation approaches:

- **Auditing** refers to an independent, objective assurance activity designed to add value and improve an organisation's operations. A distinction is made between regularity or financial auditing – focusing on compliance – and performance auditing, which focuses on relevance, economy, efficiency and effectiveness.[110]
- **Evaluation** refers to the systematic and objective process of examining the implementation and impacts of policy interventions, in order to better understand and assess their intended and unintended costs, effects and outcomes. The evaluation of public expenditure, activities and results is integral to the transparency and accountability of national governments, including in the field of cybersecurity. Evaluation can, therefore, assist in understanding the nature and causality of the effects of government interventions to help improve existing policy and to better inform decision-making for future interventions and policies.[111]

[110] OECD (2010).
[111] NAO (2013).

According to McPhee (2006), programme evaluation and performance auditing share similar aims, approaches, methodologies and techniques, but can be observed to have three overarching differences[112]:

1. Evaluation tends to focus on policy and to make a qualitative assessment of policy effectiveness, whereas performance audit tends to focus on assessing the economy, efficiency and effectiveness of public administration.
2. Audits are typically independent, whereas evaluations may not be.
3. In the public sector, evaluations are typically reported to the relevant minister or agency and not always made public, whereas an independent audit is typically reported direct to Parliament.

An overview of key performance measurement terminology has been included in Table 4.1 to facilitate the exploration of how cybersecurity performance could be measured. The remainder of this section firstly explores why measuring cybersecurity policy is especially challenging, before proceeding to an exploration of possible approaches and methods that could feasibly be used to improve the measurement of cybersecurity initiatives and better inform policymaking.

Table 4.1 Overview of key performance measurement terms

Term	Definition
Counterfactual	The situation or condition that hypothetically may prevail for individuals, organisations, or groups were there is no development intervention.
Effect	Intended or unintended change due directly or indirectly to an intervention.
Effectiveness	The extent to which the development intervention's objectives were achieved, or are expected to be achieved, considering their relative importance.[113]
Efficiency	A measure of how economically a resource/input (funds, expertise, time, etc.) is converted to results.
Impacts	Positive and negative, primary and secondary long-term effects produced by a development intervention, directly or indirectly, intended or unintended.
Inputs	The financial, human and material resources used for the development intervention.
Output	Products, capital goods and services that result from a development intervention; may also include the resultant changes that are relevant to the achievement of outcomes.
Outcome	The likely or achieved short-term and medium-term effects of an intervention's outputs.

Source: OECD (2010).

[112] McPhee (2006).

[113] Note: Also used as an aggregate measure of (or judgment about) the merit or worth of an activity, i.e. the extent to which an intervention has attained, or is expected to attain, its major relevant objectives, efficiently, in a sustainable fashion and with a positive institutional development impact (OECD 2010).

4.2. Measurement of cybersecurity performance is challenging due to several characteristics of the cyber domain

The first phase of this cybersecurity state-of-the-art study revealed that evaluation and performance measurement in cybersecurity is scarce and very much still an emerging research area – particularly in relation to evaluating the performance of cybersecurity governance approaches. There is some existing research exploring different approaches to cybersecurity from a national security perspective, but it is limited in scope and scale and rarely provides an answer as to how well the different approaches perform.[114] There have also been some studies specifically examining the Dutch system or its response to significant incidents, but again these are limited in both number and the depth of insight that they provide.[115]

According to previous RAND research, several changes in how modern digital societies work have created challenges in the evaluation of the efficiency and effectiveness of policymaking, including[116]:

- **Evolving agency in the decision-making process**: In contrast to centralised government in the past, modern government policy- and decision-making typically involves a multitude of actors, which make it challenging to answer the questions of who made key determining decisions and through what process they were taken. These changes are two-fold: policymaking has in recent years become increasingly horizontally integrated, where policymakers seek to create integrated programmes by integrating different services (e.g. integrating healthcare and education) or by integrating previously separate agencies delivering related services. Policymaking has also become vertically integrated, where local, national, regional and supranational levels of government can all be involved in policy- and decision-making processes, potentially creating complex networks, power dependencies and relationships.
- **Increasing difficulty in attributing policy effects**. With increasingly complex agency relationships in the policymaking process, it also becomes more difficult to attribute policy effects or outcomes – particularly when it comes to understanding what was causally necessary or sufficient for a particular outcome to be achieved.
- **Growing complexity in measuring effect**. Measurement is at the core of evaluation and performance evaluation and has seen a growing complexity in recent years in measuring the effects and outcomes of policymaking. The increasing complexity and numbers of stakeholders involved in policy- and decision-making makes it difficult to understand not only *what* exactly to measure, but also *when* to measure it. This is particularly true when the government intervenes in complex adaptive systems in which it is not fully in control of the outcomes of interventions, and/or those outcomes may take a long time to become manifest.
- **Increasing intricacy of articulating benefit**. In the context of measuring effect, it is typically also necessary to consider the benefits of a particular policy or intervention. The growing complexity

[114] See for example Adams et al. (2015); Boeke (2017).
[115] See for example Dutch Safety Board (2013); Boeke (2016); Claver (2018).
[116] Ling and van Dijk (2009).

of governance and policymaking has made it more challenging to articulate, understand and evaluate the costs and benefits. Costs and benefits may be unevenly distributed between actors, or incommensurate (i.e. not being comparable by the same standard, e.g. an economic saving for one party compared to a privacy loss of another party). This poses a particular challenge to quantitative rather than qualitative measures.

These challenges are not unique to the field of cybersecurity, but are exacerbated by three characteristics of the cyber domain – its complex dynamics often require a consideration of its interacting systems, changing environments, and conflicts over the public interest.[117] Table 4.2 features a summary of these three characteristics and how they introduce additional complexity when measuring the efficiency and effectiveness of policymaking in the cyber domain.

Table 4.2 Overview of complex characteristics of the cyber domain

Characteristic	Cyber domain complexity	Implications for evaluation
Complexity of interacting systems	Socio-technological systems; breadth of system coverage	Challenging to understand relationships, dependencies, cause and effect
Changing environments	Rate of technological change; continuously evolving adversary environment	Challenging to develop clarity in risks and vulnerabilities, understand adversary behaviour, actions and consequences
Conflicting public interest perspectives	Competing stakeholder interests (e.g. security vs commercial interests, privacy vs usability, etc.)	Challenging to align evaluation goals and performance indicators (e.g. lack of agreement of what the system should achieve)

Source: Adapted from Julnes (2019).

Lastly, national cybersecurity typically involves managing risks rather than delivering measurable outcomes, as the risk might have been well-managed whatever the outcome, which further makes performance measurement and evaluation challenging.[118]

Additionally, a fundamental enabler for cybersecurity policymaking is sufficient evidence of appropriate fit and quality. One of the overarching challenges in the cyber domain is access to relevant data of sufficient quality to inform policy- and decision-making. As the first phase of the cybersecurity state-of-the-art study showed, the field of cybersecurity is subject to frequent and persistent knowledge or research gaps, often further exacerbated by the scarcity of reliable, verifiable data, and particularly large scale, longitudinal datasets.[119] This makes it challenging to define, articulate and ultimately understand the nature of the challenge or problem, as well as what could potentially be done to mitigate it. The lack of data or appropriate methods may also make it challenging for policymakers to understand on what basis decisions should be taken and understand how well decisions have performed over time to assess their impact.

[117] Rowe (2019).
[118] Julnes (2019).
[119] Silfversten et al. (2019).

4.3. This study identified several possible approaches that may improve evaluation or performance measurement in cybersecurity

The focus in this second phase of the cybersecurity state-of-the-art study has been to explore how efficiency and effectiveness of national cybersecurity could be measured or evaluated to better inform policy- and decision-making. The findings presented in the following sections cover several approaches to measuring performance, including:

- Frameworks for thinking about the evidence needed for cybersecurity policymaking;
- Approaches that have previously been used for evaluation in the cyber domain; and
- Approaches from other sectors that could be used for evaluation in the cyber domain.

The various approaches presented have different uses, potential strengths and benefits and it is, therefore, useful to consider some fundamental evaluation questions when reviewing them (i.e. *why* we need to measure performance, *what* do we need to measure, and *how* should we measure it). These approaches, therefore, serve different purposes, have different application areas and cannot be directly compared against each other, as they are not mutually exlcusive. It should also be noted that this is a not a fully exhaustive review of possible approaches for evaluating cybersecurity interventions or policies or measuring cybersecurity performance (i.e. there may be additional approaches that are not covered within this chapter).

Table 4.3 presents an overview of the various approaches presented in this chapter and where they may add the most value.

Table 4.3 Overview of approaches to improve the measurement of cybersecurity performance and cybersecurity policymaking

Approach or framework	Use case and added value
Evidence model for cybersecurity policymaking	To assess and improve the evidence used for cybersecurity policymaking.
Post-incident and lessons learned analysis	To analyse, assess and improve the response mechanisms to incidents or attacks, including the governance of cybersecurity both within the overall system and within crisis management or incident response structures.
Self-assessments of cybersecurity maturity	To assess and help improve the cybersecurity maturity of organisations.
Programme evaluation	To evaluate the impact of specific programmes or interventions within national cybersecurity.
Performance auditing and Value for Money	To evaluate the wider performance of specific programmes or the overall national approach to cybersecurity (e.g. its economy, efficiency and effectiveness).
Exercises and games	To explore poorly understood areas of cybersecurity and develop better evidence for policymaking. To exercise, test and assess governance structures and plans, particularly in relation to incident response and crisis management.

Measuring the value of national cybersecurity	To define and measure the overall contribution and value of the national cybersecurity system.
Decision making under deep uncertainty methods	To assess and refine future polices and improvements to national cybersecurity.

4.3.1. An evidence model for cybersecurity policymaking

The importance of evidence for policymaking has been widely highlighted in recent years, which has also prompted questions as to what evidence policymakers rely upon for decision making in the cyber domain. This was the context in which the Evaluating Cyber Security Evidence for Policy Advice (ECSEPA) was launched. ECSEPA is a UK project developed in collaboration with a range of partners including University College London, Coventry University, the Sociotechnical Security Group at the UK NCSC and the Cyber Policy team at the Foreign, Commonwealth and Development Office (FCDO).[120] A key output of this project is the Evidence Quality Assessment Model for Cybersecurity Policymaking (EQAM), which is a model to help policy advisers and decision makers assess evidence fitness and credibility for use in policymaking.[121]

Policymakers may encounter a wide range of types of evidence and sources in their work, including experimental controlled trials and studies, social surveys, econometrics and economic modelling, expert advisory groups, public attitudes, policy evaluations, research and statistics and expert knowledge. The EQAM was developed to address three characteristics of the cyber domain that make the assessment of evidence for policymaking challenging:

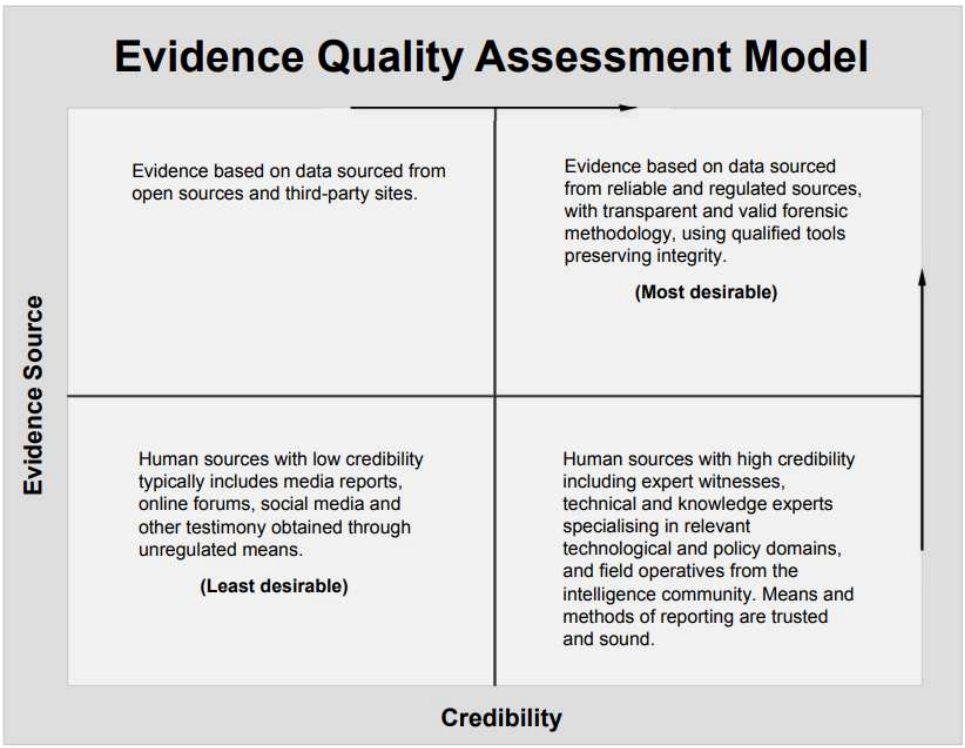
- The evidence base lacks soundness and credibility when it contains elements that are contradictory and/or are the instrument for deliberate agendas.
- It is complex and difficult to attribute cyberattacks and quantify their cost. The absence of clear knowledge over the financial implications of cyber weaknesses and incidents – as well as the intent and role of different actors in committing attacks – may lead to a disconnection between the policy response and the real threats and risks.
- Cybersecurity is an area with wide-ranging implications that require policy advisers to balance competing interests, including those of national security, fundamental rights, economic security and infrastructure weaknesses. The contrasting understandings of cybersecurity by policy communities ultimately hinders a united response. [122]

The EQAM functions as a simple bi-dimensional framework with four quadrants. While the vertical axis represents the evidence source, the horizontal axis reflects the credibility of the evidence. The quality of evidence is therefore determined across these two dimensions, as shown in Figure 4.1. On the vertical axis, evidence is classified and examined according to its source: either it comes from data or human sources. On the horizontal axis, evidence is considered based on its credibility. The authors note that the

[120] See ECSEPA (n.d.).
[121] Hussain et al. (2018).
[122] Hussain et al. (2018).

horizontal axis should be regarded as a continuum, where credibility has to be judged on a case-by-case basis for each piece of evidence, and that the four quadrants are framed simply to help map evidence sources in relative position to each other (rather than to offer distinct categories of evidence).

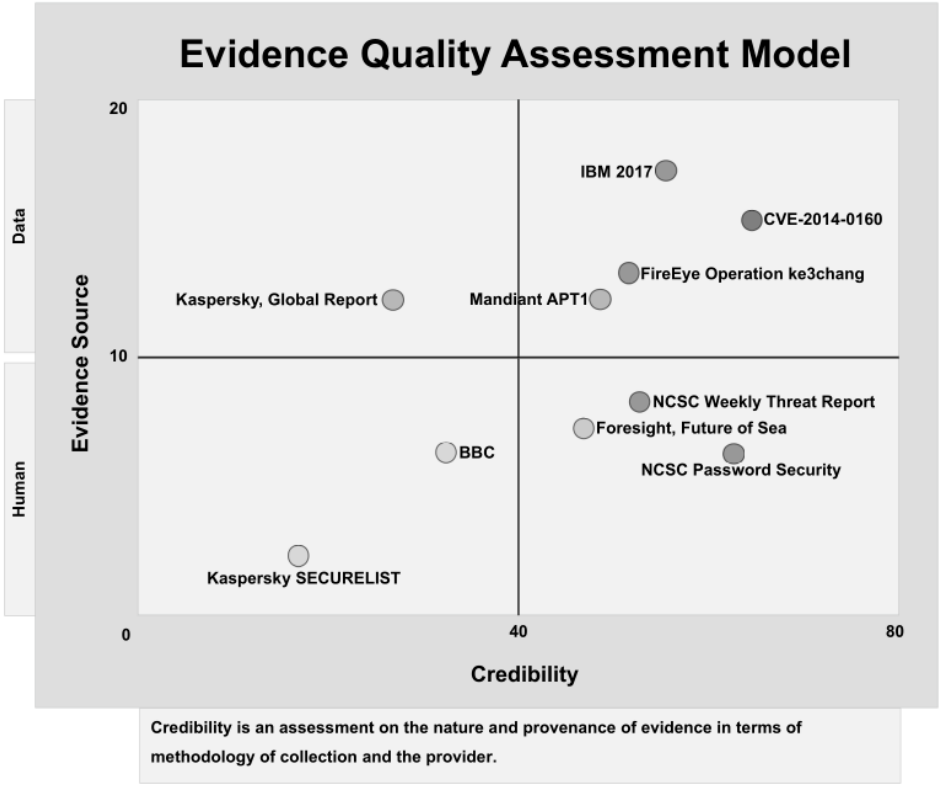
Figure 4.1 The Evidence Quality Assessment Model



Source: Hussain et al. (2018).

This framework can then be used to score evidence sources to help assess evidence fitness and credibility of evidence for use in cybersecurity policymaking, ensuring that decisions are taken with the best available data. Within their paper, the authors illustrate a populated EQAM with different sample evidence sources that shows how different attributes could be used for a comparison (see Figure 4.2).

Figure 4.2 Sample populated EQAM



Source: Hussain et al. (2018).

The EQAM should, as such, not be considered a standalone tool for evaluating or measuring efficiency and effectiveness, but rather as a tool to improve cybersecurity policymaking overall. As such, the EQAM could help evaluate the quality and fitness of the evidence used in decision making and inform an evaluation of a policy or intervention's effects or outcomes.

4.3.2. Post-incident and lessons-learned analysis

Lessons-learned analysis is often used in cybersecurity to understand why an incident has occurred, how the response to the incident worked, and how similar situations might be avoided or better addressed in the future. Incident and lessons-learned analysis can be undertaken both at the team or organisational level – to improve the internal response to incidents – or be led independently by a third-party organisation not directly involved in the incident. Post-incident analysis can both be done at a technical level and qualitatively at the process or system level. Box 2 highlights an example of how a qualitative post-incident analysis of the system-level can be performed.

Box 2 Post-incident analysis example: Dutch Safety Board investigation of the DigiNotar incident

The Dutch Safety Board is an independent administrative body that works independently to the Dutch government. The Board seeks to examine and better understand the causes of significant incidents, structural safety failings and administrative processes that have an impact on safety, which is done partly through post-incident and lessons-learned analysis.[123]

In 2011, DigiNotar B.V, a supplier of digital security certificates used by Dutch public authorities, was compromised and used to generate and issue fraudulent certificates. The compromise could have rendered DigiNotar certificates unusable, potentially disrupting essential data flows within the Netherlands and causing significant economic harm and societal disruption.[124] Drawing on qualitative research methods, including literature review, interviews and round table discussions, the Dutch Safety Board tried to answer why the involved parties had misplaced such trust in the digital certification system. The Board ultimately identified two overarching reasons:

1. **Insufficient risk awareness among administrators**. The Board found that the parties involved were simply not sufficiently aware of the factors that could put the system at risk, particularly at the senior decision-maker and political level.
2. **Executive inability to take responsibility**. The Board found that cybersecurity is often left to the operational level, with limited or no involvement of executives, highlighting the underlaying weak governance of cybersecurity in many of the affected parties.

The Safety Board report also featured several recommendations to the Dutch government to avoid similar incidents in the future. The Dutch Safety Board is currently also investigating the Citrix incident through a post-incident and lessons-learned exercise.[125]

4.3.3. Self-assessments of cybersecurity maturity

Self-assessments have been used to assess cybersecurity arrangements in both private and public sector organisations. Self-assessments are useful when there are limited resources for the evaluator, as the burden to provide answers to the assessment exercise is placed on the participating organisations. Self-assessments can also be helpful in assessing the uptake of particular policies and cybersecurity interventions, and how well they are received by the participating organisations. The drawbacks of any self-assessment exercise include potential biases by the respondents, the unknown quality of evidence used by respondents and a lack of interaction between evaluators and participating organisations. Box 3 features an example of a cybersecurity self-assessment evaluation used for the local-government sector in the UK.

[123] Dutch Safety Board (n.d.a).
[124] Dutch Safety Board (2012).
[125] Dutch Safety Board (n.d.b).

Box 3 Cybersecurity self-assessment example: UK LGA Cyber Security Self-Assessment tool

The Local Government Association is the national membership body for local authorities in the UK (e.g. the 339 English councils and 22 Welsh councils). In cybersecurity, the LGA works with the UK Cabinet Office under the National Cyber Security Programme to help improve the cybersecurity of local government within the UK. As part of this endeavour, the LGA has developed an online self-assessment tool to support local authorities in evaluating their cybersecurity at regular intervals. The self-assessment seeks to:

- Assess what arrangements are currently in place;
- Identify good practice within the council or shared service; and
- Identify risks and areas for improvement.

The self-assessment tool is designed around guidance from the UK NCSC and features questions in five areas of cybersecurity:

- Leadership, reporting and ownership;
- Governance, structures and policies;
- Partnerships, information, advice and guidance;
- Technology, standards and compliance; and
- Training and awareness.

The LGA uses the results from the self-assessments to further develop their cybersecurity improvement offer (e.g. training interventions, support from central government, etc.), as well as to identify good practice from local government so that strong performing councils can help coach and develop the capacities of other councils with weaker cybersecurity arrangements.[126]

4.3.4. Programme evaluation

As outlined in Section 4.1, programme evaluation is an essential part of the programme development cycle, which is used to determine how well a programme works, to help improve it and provide evidence for further support or funding for the programme.[127] This type of evaluation is suitable for the evaluation of a single programme or one part of a larger cybersecurity intervention, and typically comes in three forms:

1. **Process evaluation**, which seeks to evaluate if the programme was carried out according to plan;
2. **Impact assessment**, which seeks to evaluate if the programme brought about the planned change in the intended target group; or
3. **Outcome evaluation**, which seeks to evaluate the outcomes of the programme and is often used to measure the effectiveness of the programme.[128]

A programme evaluation can be carried out using both qualitative and quantitative methods, as shown in Table 4.4. It is also possible to combine various methods in a mixed-methods approach so that different forms of evidence can inform the evaluation.

[126] Local Government Association (n.d.).
[127] Calder (2013).
[128] Calder (2013).

Table 4.4 Overview of possible methods for programme evaluation

Method	Description	Most suited for	Strengths and weaknesses
Qualitative methods			
Interviews, focus groups surveys and workshops	Methods to gather qualitative input from organisers or participants relating to the underlying logic of the programme or the programme execution and performance.	Process evaluation	+ Can provide evidence of why a programme may or may not have worked as expected + Inexpensive to deliver – Sample (participants) are not a random sample – Results cannot be easily generalised
Quantitative methods			
Interrupted time-series design	Method to assess the outcome of programme by tracking multiple measures of the outcome of interest before and after the programme.	Impact evaluation Outcome evaluation	+ Practical design if sufficient numbers of events and accurate surveillance systems in place
Controlled before–after study	Method to measure the outcome in a target group before and after and compare that to a control group after the programme has been delivered.	Impact evaluation Outcome evaluation	+ Most practical design – Must have comparable control group
Before–after study (no control group)	Method to measure the outcome in a target group before and after the programme has been delivered.	Impact evaluation Outcome evaluation	+ Inexpensive to deliver – Provides low levels of evidence
Randomised controlled trial	Method to evaluate the outcome of a programme before and after using groups that are randomly allocated either to receive, or not receive, the programme.	Impact evaluation Outcome evaluation	+ Most rigorous evidence – Expensive to deliver – Randomisation not always feasible

Source: WHO (n.d.).

Within a cybersecurity context, programme evaluations are often delivered using quantitative methods to track and measure technical performance indicators. Box 4 features an example of this type of programme evaluation and illustrates the evaluation approach undertaken by the UK NCSC's Active Defence Programme (ACD).

Box 4 Programme evaluation example: UK NCSC Active Cyber Defence Programme

The UK NCSC's 'Active Cyber Defence' (ACD) programme seeks to 'protect the majority of people in the UK from the majority of the harm caused by the majority of the cyber-attacks the majority of the time'.[129] The programme consists of a set of eight tools and services provided free of charge to UK central government and some public-sector organisations:

1. **Protective Domain Name System** (PDNS) – a secure DNS service for the public sector.
2. **Web Check** – a service that helps organisation proactively identify and fix common web vulnerabilities.
3. **Mail Check** – a platform for assessing email security compliance that collects, processes and analyses DMARC reports from across the public sector.
4. **Host Based Capability (HBC)** – a software agent to detect malicious activity on UK government endpoints.
5. **Logging Made Easy (LME)** – a service to help organisations set up basic logging capability, enabling routine end-to-end monitoring of their Windows-based IT systems.
6. **Exercise in a Box (EiaB)** – a framework for running cybersecurity exercises for the government.
7. **Vulnerability Disclosure –** the provision of vulnerability reporting and vulnerability disclosure services.[130]

The ACD Programme is subject to internal programme evaluation by the UK NCSC, which is published in the ACD Annual Reports.[131] These seek to establish a public and transparent evidence base for the effectiveness of the ACD Programme, which is mainly achieved by tracking quantitative performance metrics across the ACD tools and services. For example, for Web Check, the UK NCSC tracks the number of websites scanned, the number of security vulnerabilities identified and security advisories issued, as well as information on if and how long it takes for organisations to remediate their vulnerabilities. In the 2019 report, the UK NCSC concludes that the Web Check service is successful in producing positive effects at scale through relatively simple measures, but also that continuous nudging of public sector organisations is needed to maintain the security of their sites.[132]

The ACD programme evaluation reports also highlight some of the challenges in performing this type of evaluation, particularly in collecting and evaluating cybersecurity data. The UK NCSC acknowledges that its evaluation approach is still a work in progress and that sometimes there are instances that cannot be explained or that simply lack sufficient data to draw conclusions or show causation. The ACD Programme's rationale is to identify causes of harm and develop an intervention that reduces the harm, either by blocking access or removing the cause of the harm. In this context, the UK NCSC acknowledges that both upward and downward results can be positive:

- **Upward trendline**: the UK NCSC is successful in blocking or taking down attacks, making attackers frustrated and increasingly targeting UK targets (i.e. the programme is producing the intended results).

[129] See NCSC-UK (n.d.).
[130] NCSC-UK (n.d.).
[131] NCSC-UK (2019).
[132] NCSC-UK (2019).

- **Downward trendline**: the UK NCSC is making it harder to cause harm so there are fewer attacks to take down or block (i.e. the programme is producing the intended results).[133]

These challenges illustrate the difficulties of quantitative performance measures, even though they may initially appear straightforward. As cybersecurity mostly involves human attackers, who often seek to adapt and overcome security measures, it may be difficult to understand success. In other words, is the programme successful in blocking or taking down an increasing number of attacks because the defensive measures are working or because there are more attacks? And similarly, when attacks are decreasing, is the programme successful in blocking or taking down more attacks or are the attackers becoming better at hiding their attacks? As such, there may be a significant amount of work required in understanding and correlating quantitative cybersecurity performance indicators for effective programme evaluation.

4.3.5. Performance auditing and Value for Money

As noted in Section 4.1, performance auditing is often used to assess the economy, efficiency and effectiveness of public administration. The assessment of economy, efficiency and effectiveness of interventions is sometimes also often referred to as Value for Money (VFM) evaluations. There are two types of VFM evaluations:

1. **Performance evaluation** of existing programmes by assessing performance against set criteria and evidence, and comparing actual with planned performance and external benchmarks.
2. **Economic appraisal** of programme proposals using an appraisal process to decide whether or not to invest in the programme before its implementation. This is typically done by the perceived net value (i.e. do the benefits outweigh the costs) and comparing various options (including the 'do nothing' option).[134]

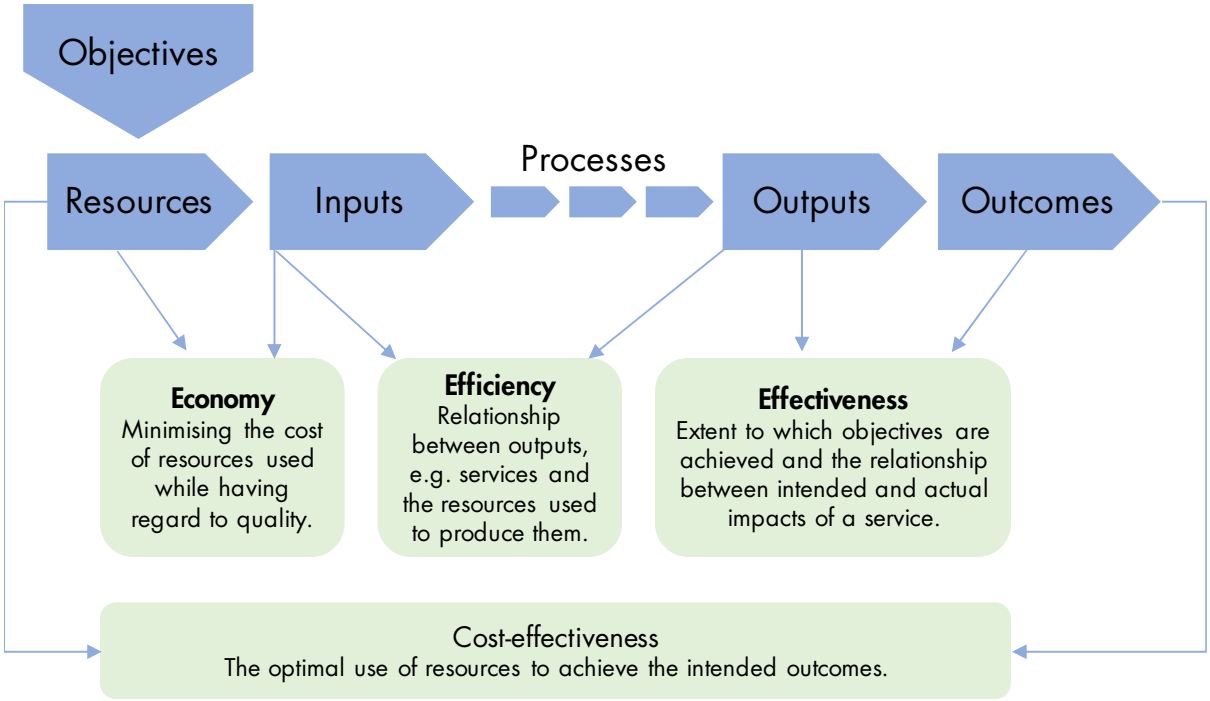
VFM can be summarised as is the optimal use of resources to achieve the intended outcome, particularly when using public funds. The UK's National Audit Office, equivalent to the US GAO, further specifies the three components of VFM as:

- **Economy**: minimising the cost of resources used or required for the intervention (i.e. *spending less*);
- **Efficiency**: the relationship between the output from the intervention and the resources to produce them (i.e. *spending well*); and
- **Effectiveness**: the relationship between the intended and actual outcomes of the intervention – (i.e. *spending wisely*).[135]

Performance and VFM evaluations often use logic models to structure their evaluations. A logic model involves identifying the strategic elements of an intervention (e.g. its inputs, outputs, outcomes, impact) and their causal relationships and indicators, and the assumptions or risks that may influence success and failure of the intervention.[136] Figure 4.3 shows a basic logic model for a VFM framework.

[133] NCSC-UK (2019).
[134] Barnett et al. (2010).
[135] NAO (n.d.a).
[136] OECD (2010).

Figure 4.3 Basic logic model for a VFM framework

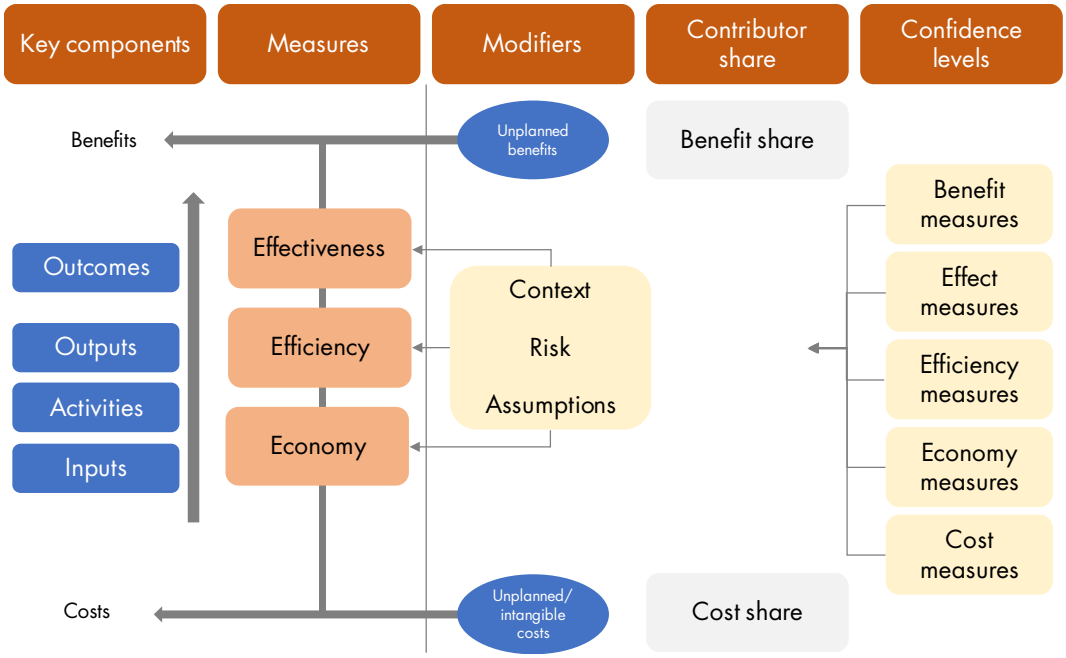


Source: NAO (n.d.b).

VFM is a generic framework for improving decision making and policy evaluation, which can be applied within the cybersecurity domain. However, the use of VFM for cybersecurity evaluation may require a degree of tailoring or adaptation to ensure that the framework is fit-for-purpose. In this case, it may be useful to learn from other sectors that have worked to adopt VFM to their specific context.

As an example, the former UK Department for International Development (DFID) (now part of the Foreign, Commonwealth and Development Office) tried to develop a framework suited for evaluating VFM in international development missions. As part of this process, DFID also used an approach to design VFM frameworks through an iterative and collaborate approach that could be of use to cybersecurity stakeholders. As part of this approach, DFID used a modified logic model with additional components to the basic model featured above, as shown in Figure 4.4.

Figure 4.4 DFID Conceptual VFM framework



Source: Barnett et al. (2010).

DFID's conceptual VFM framework consists of five overarching components:

1. **Key components**: The key VFM components to capture optimal relationship between costs/resources and benefits/outcomes (e.g. inputs, activities, outputs, outcomes).
2. **Measures**: The VFM measures of economy, efficiency and effectiveness.
3. **Modifiers**: DFID acknowledges that the optimal balance of VFM measures also requires the factoring in of context, risk and assumptions that limit the effectiveness, efficiency and economy. Modifiers may also include intangible and unplanned costs and benefits that may affect overall VFM.
4. **Contributor share**: This component highlights the importance of determining how to attribute costs and benefits when making value-for-money judgements.
5. **Confidence levels**: A component that captures data quality (e.g. explicitness of assumptions, relevance and robustness of the data sets used) and the sensitivity of the VFM findings if assumptions or data are changed.[137]

The analysis and discussion of this conceptual framework led to the development of a 'rating and weightings approach', in which key processes and measures associated with economy, efficiency and effectiveness are identified and used to evaluate programmes; and where they can be weighted to reflect their relative importance. The definition and availability of typically performance indicators play an

[137] Barnett et al. (2010).

essential role for VFM evaluation, as they give a measure of efficiency and provide qualitative and quantitative measures of increase or decrease in outcomes (i.e. effectiveness).[138]

To ensure a comprehensive and accurate VFM evaluation approach, DFID identified both qualitative and quantitative assessment indicators spread across three metrics (economy, efficiency and effectiveness), as show in the table below.

Table 4.5 DFID VFM evaluation criteria

	Indicator	Description
Effectiveness	Leverage/Replication	Assessing the degree of leverage with other activities and wider effects described and the potential for additional benefits (e.g. scale-up, multiplier or replication).
	Theory of Change	Assessing if outputs are necessary and sufficient to deliver purpose, if there are realistic and credible assumptions, and likelihood of achieving or exceeding state purpose.
	Relevance and Robustness of Indicators	Assessing whether indicators are relevant (i.e. clear, rule driven, causally linked, gendered, pro-poor and cross-sectoral) and robust (i.e. data to support indicators (including baseline) are available, accessible, credible, ownable and disaggregate-able).
Efficiency	Productivity Measure	Assessing the cost of activities/outputs and the degree to which critical outputs are optimised, e.g. through timing of delivery, increase in proportion of output; decrease in proportion of input.
	Risk Analysis and Mitigation	Assessing to what degree the risk analysis covers key threats and provides comprehensive assessment of overall risk level, monitoring and risk mitigation in place.
Economy	Procurement	Assessing the cost reductions achieved through better use of procurement, and the degree to which risks to outputs/outcomes are identified, assessed and minimised.
	Unit Costs	Assessing whether cost is below benchmark cost, and provides any additional benefits and levels of expected return.

Source: DFID (2010).

The DFID example briefly illustrates how a VFM framework tailored to a specific policy context can be developed through iterative and joint stakeholder consultation processes, which could feasibly be replicated and applied within the cybersecurity policy domain.[139]

4.3.6. Exercises and games

Beyond traditional approaches to evaluation and performance evaluation, exercises and games are, and can be, used for measuring or evaluating cybersecurity performance. In general, cybersecurity exercises and games can contribute to a wide variety of objectives, including:

[138] Barnett et al. (2010).

[139] For more detailed guidance on how to perform a similar VFM development exercise, see DFID (2010).

1. **Increasing collaboration** and facilitating a greater understanding and familiarity of interaction of the various actors in the system by:
    a. Enabling the participants to exchange experiences and information;
    b. Increasing the understanding of the national and international cyber environment and their associated policy, legal and international cooperation requirements; and
    c. Developing and expanding institutional and international collaboration in the ability to handle cyber incidents.
2. **Identifying vulnerabilities** in systems by:
    a. Identifying or exploring the desired security properties in information systems (e.g. being able to withstand a distributed denial-of-service attack); and
    b. Testing preparedness and response plans.
3. **Improving future incident response** by studying exercise interactions and outcomes so that governance, knowledge and skills for cybersecurity and incident response can be improved.[140]

There are several types of games with different use cases for measuring cybersecurity performance or cybersecurity programmes, as shown in Table 4.6. Games can typically be divided into three categories:

- **Seminar-style games:** Also referred to as free-form games or loosely structured games, seminar-style games are characterised by the absence of formal rules to determine game outcomes. Instead, seminar-style games rely on experts to discuss, debate and decide how in-game actions interact and the outcome they will have, which particularly lend these types of games for exploring poorly understood policy challenges.
- **Manual games**: Manual games use physical game pieces and formal rulesets for gameplay to provide a structured and systematic game experience tailored to the policy context and challenge of the game scenario. Manual games include board games, card-driven games and allocation or investment games.
- **Computer-assisted games**: These types of games rely on IT infrastructure and computers to deliver the game experience. This often involves the use of computer-based models to determine outcomes from the players' choices and offers the potential for complex interactions.[141]

[140] Wilhelmson and Svensson (2011).
[141] Pardee RAND Graduate School (n.d.).

Table 4.6 Types of games and their evaluation use cases

Game category	Game type(s)	Description and evaluation use case
Seminar-style games	360° games	A 360° Discovery Game methodology immerses a diverse group of participants in an environment in which complex dynamics can be documented, analysed and understood. Unlike some manual games, players do not compete against each other, but rather against the game scenario. As a result, the game incentivises collaboration, information-sharing and idea generation, as the shared goal of the players is to identify possible solutions that fit each player's role and equity.[142] 360° games are, therefore, useful in exploring poorly understood policy areas, as well as evaluating and testing system dynamics within complex systems. These types of games are particularly helpful in bringing together participants who normally do not interact, which often happens in real-life cyber incidents.[143]
Manual games	Table-top exercises	Table-top exercises are typically paper-driven exercises with injects scripted by exercise planners to progress game-play. Table-top exercises can be used to establish relationships and share information with other organisations, stakeholders or countries; test the readiness of response capabilities; and raise awareness within the cybersecurity community. Table-top exercises are particularly helpful in simulating response mechanisms to cybersecurity incidents or to evaluate and test crisis management plans.
Computer-assisted	Hybrid exercise	Hybrid exercises combine elements of table-top exercises and the use of computers, typically through the use of simulated cybersecurity incidents within exercise IT infrastructure. Hybrid exercises are used in similar evaluation contexts as table-top exercises, but offer additional ability to evaluate or assess technical capabilities and readiness.
Computer-assisted	Full live exercise	Live exercises move the entire exercise or game to a virtual environment within a digital exercise infrastructure. Live exercises are used in similar evaluation contexts as table-top and hybrid exercises but offer additional ability to evaluate or assess technical capabilities and readiness.

Source: RAND Pardee (n.d.); Kick (2014).

Exercises and games can therefore contribute to the evaluation of cybersecurity in several ways, both directly (through a dedicated evaluation exercise or game) or indirectly (through non-evaluation games that nevertheless contribute to a better understanding of cybersecurity challenges or issues within the scope of an evaluation). Box 5 offers an example of a non-evaluation-specific cybersecurity game that also offers important insights into national cybersecurity and the dynamics within it.

[142] Mikolic-Torreira et al. (2016).
[143] INT03.

Box 5 Example of a 360° game for cybersecurity

In 2016, the RAND Corporation used a 360° discovery game to assist in the development of a framework for cybersecurity that considers the roles of government, industry, advocacy organisations, academic institutions and individuals and how these stakeholders' concerns relate to each other.

The game was held in two parts – one in Washington, D.C. and one in Silicon Valley – with participants spanning the public and private sector, academia and advocacy groups. The aims of the game were to explore opportunities for improving cybersecurity, assess the implications of possible solutions and develop a framework for debating and implementing future cybersecurity policies and practices in an equitable way.

Although not an evaluation exercise per se, the game helped identify important considerations that could be used to improve national cybersecurity in the future, including:

- Identification of three fundamental enablers for progress in national cybersecurity:
  - Developing a reasonable way to monetise cybersecurity risks;
  - Finding an acceptable assignment of accountability and liability in the cyber ecosystem; and
  - Selecting, aligning and empowering jurisdictions to enforce accountability and liability.
- Acknowledgement that the background and perspective of participants matter. For example, when discussions related to ideas for possible government regulations, the Washington participants were unable to agree on which government agency or agencies had the responsibility, appropriate authority or capability to oversee it. In contrast, the Silicon Valley participants discussed new regulations on its merits only, and questions of responsibilities and authorities were never raised.

A 360° game can, as such, help shed light on key perspectives on cybersecurity and where potential barriers to progress are located within the system, which are both helpful from an evaluation perspective.

Source: Mikolic-Torreira et al. (2016).

4.3.7. Measuring the value of national cybersecurity

Beyond evaluating the performance of an individual intervention or part of the national cybersecurity system, measuring the overall contribution and value of cybersecurity could also be considered. The provision of cybersecurity from a national perspective is often seen to be an opportunity cost justified by national security concerns (i.e. cybersecurity is a necessary cost in order to protect the nation, but it brings few direct economic benefits or returns). However, this may not always be the case and there is an emerging body of work to help assess and illustrate the indirect benefits that security brings to wider society and welfare. These frameworks have so far not been applied to the cybersecurity domain, but it is feasible that they could be used to assess and measure the value of national cybersecurity as well.

Similar to national defence, cybersecurity outputs and outcomes – such as digital security and safety – may be difficult to define and measure. This presents a two-fold challenge: how to measure and improve the performance of the national cybersecurity system and how to illustrate the value that the system brings to society. Within this context, the Public Value Framework recently developed by UK government may help policymakers define, measure and improve the value generated by national cybersecurity.

The Public Value Framework (PVF)

The Public Value Framework was developed by Her Majesty's Treasury in the UK as a tool to improve understanding of how different activities and outputs deliver public value. The development of PVF was partly driven by the challenge of evaluating public sector performance, particularly when it comes to

assessing non-quantifiable benefits from an economic perspective, such as peace and security, the fight against climate change and so forth.

In summary, the PVF seeks to overcome the limitations of current evaluation approaches that seek to understand and quantify public sector value. Rather than seeking to quantify inputs and outputs and observe the relationship between them, the PVF seeks 'to define everything that a public body should be doing in between to maximise the likelihood of delivering optimal value from the funding it receives. It sets out the activities that are required creating a set of criteria that can then be used to assess the extent to which those activities are taking place and, by extension, how likely it is that value is being maximised.'[144]

The PVF is divided into four pillars, which together represent the main criteria to foster public value:

1. The first pillar refers to the **pursuit of public bodies' fundamental aims** and how they are managing the stepping stones to ensure the ultimate delivery of these goals.
2. The second pillar refers to **managing inputs to test the financial management** of the public sector. These include processes to manage resources, quality of data and forecasts, benchmarking and cost control.
3. The third pillar refers to the necessity to **engage with citizens and users** to convince them of the value being delivered, which subsequently fuels legitimacy.
4. The fourth pillar 'developing system capacity' focuses on the **long-term sustainability of the system**, notably across the capacity to manage the delivery chain, the public bodies' workforce capacity and capacity to evaluate impact.[145]

The PVF functions as a framework for appraisal. To achieve this, the four pillars are subdivided into areas to consider and each of these is accompanied with questions that help to draw an assessment of the extent public bodies deliver public value. For example, the first area to consider in the first pillar is 'understanding vision and goals'. Evaluating this specific area is conducted across a set of three questions:

1. How well-defined is the overall vision for this area of spending?
2. What measurable and SMART[146] objectives have been set to achieve the goals and vision?
3. What evidence does the public body use to link its chosen objectives to the vision/goals in this area of spend?[147]

Ultimately, the main output of an appraisal within the PVF is an adapted Red Amber Green rating that depicts the likelihood to deliver public benefit with regards to associated expenditures.[148] The PVF additionally provides diverse approaches to assessment, some of which are the conduction of continuous assessment, rapid review and individual self-assessment, each of which have different features, advantages and constraints.

[144] HM Treasury (2019).
[145] HM Treasury (2019).
[146] Specific, measurable, attainable, relevant, time-bound.
[147] HM Treasury (2019).
[148] HM Treasury (2019).

The framework can be used for several purposes. First and foremost, the PVF is a robust analysis tool for determining the performance of policies and programmes. It can prove helpful for taking inventory of an area that has not been reviewed for a long time, and should guarantee the alignment and updating of priorities in that area. Reflecting on its evaluation grid, the instrument can serve as a basis for public bodies to design new strategic direction for policies and programmes. With its comprehensive approach, the PVF can contribute to drawing an overarching picture of any issue, and provides multiple angles from which to apprehend challenges. In this regard, it can also encourage organisations to reflect on future new areas and processes that they may not yet have given in-depth consideration to. Finally, the PVF is decisive in constructing a comprehensive evidence base upon policies and programmes since the questions it contains demand the collection of information and data from multiple sources.

Within a national cybersecurity context, the PVF could be used to develop and define a national cybersecurity value proposition that illustrates the various components of national cybersecurity and how they provide value. This type of tool could improve the understanding of how cybersecurity outputs lead to direct and indirect benefits for different stakeholders and society more generally.

4.3.8. Using methods of decision making under deep uncertainty to evaluate robustness of future cybersecurity policy or options

Robust national approaches to cybersecurity from a national security perspective require approaches that are not only well-functioning today, but also resilient and adaptable enough to perform well across a range of possible futures. It is, therefore, important to consider a requisite variety of strategic options when evaluating and looking to improve cybersecurity policymaking (i.e. a good cybersecurity policy is not good if it only works in one possible future).

Future policy- and decision-making are characterised by uncertainty, which refers to the gap between available knowledge and the knowledge that decision makers require to make the best policy choice. Uncertainty can exist in all aspects of a cybersecurity system (e.g. the governance system itself, its outputs and outcomes, the cybersecurity domain it sits within, the wider future world, etc.).[149] When evaluating and deciding on future decisions for national cybersecurity, it may therefore be useful to leverage decision making under deep uncertainty (DMDU) approaches and associated analytic methods for decision-making support.

DMDU approaches may be suitable when three conditions are met:

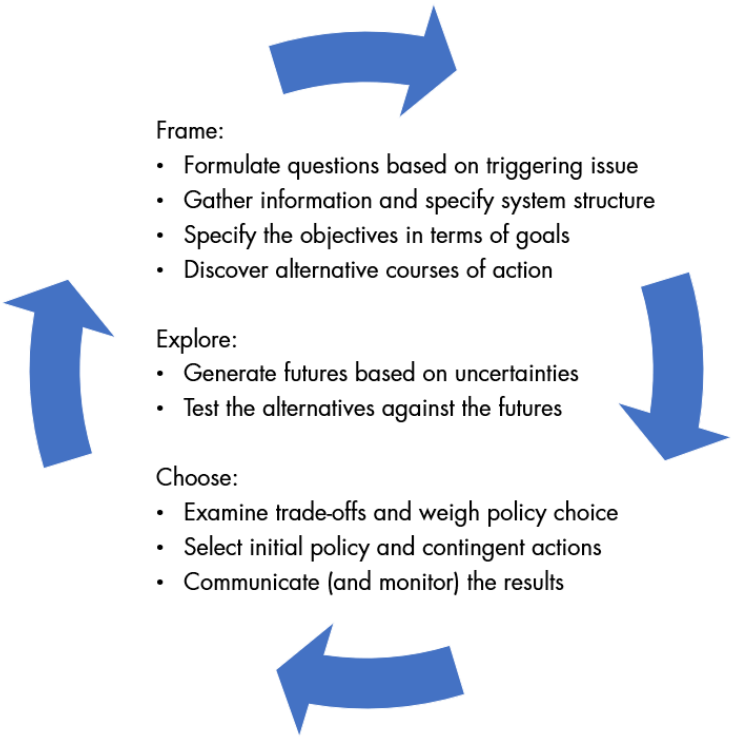
1. The uncertainties faced in the decision-making process are deep[150], rather than well-characterised;
2. There is a wide set of possible policies; and
3. There is a high degree of system complexity where experts do not know and/or disagree on the proper models, probabilities and/or system outcomes.

[149] Marchau et al. (2019).

[150] Deep uncertainty exists when decision makers do not know, or cannot agree on, the system model that relates action to consequences, the probability distributions to place over the inputs to these models, which consequences to consider and their relative importance. Walker et al. (2016).

As noted in Section 4.2, performance measurement and policy development in cybersecurity are often faced with some or all of these characteristics. Although a variety of DMDU approaches exist, they typically involving cycling through iterative loops of analysis along all or most of the steps shown in Figure 4.5.

Figure 4.5 Generic elements of DMDU approaches



Source: Marchau et al. (2019).

By way of example, there are several DMDU methods that could be used to evaluate robustness of future cybersecurity policy options, including:

- **Robust Decision Making (RDM):** RDM tests strategies to help inform decisions that are robust across a range of future scenarios by quantitatively testing policy options across many plausible futures. Visualisation and statistical analysis can then support decision makers to identify key areas of policy vulnerability, so that policies can be adapted to be more robust. RDM enables the identification of strategies that can support multiple objectives over many scenarios.[151]
- **Dynamic Adaptive Planning (DAP):** DAP involves the implementation of an initial plan before all significant uncertainties have been resolved and subsequent adaptations to the plan over time as new knowledge becomes available. An integral part to DAP is monitoring developments and developing responses when specific triggers are met. DAP occurs in two phases:
    1. The design phase, where the dynamic adaptive plan, monitoring programme, and various pre- and post-implementation actions are designed.

[151] Lempert et al. (2003).

2. The implementation phase, where the initial plan and the monitoring programme are implemented, and adjustment actions taken (if necessary).[152]

- **Dynamic Adaptive Policy Pathways (DAPP):** DAPP revolves around producing an overview of alternative routes into the future that are based on Adaptation Tipping Points (ATPs). The ATPs focus on understanding under what conditions that plan will fail, thereby requiring either an adaption to the plan or the pursuit of an alternative plan.[153]

Given the complex, dynamic and uncertain future development of the cybersecurity environment, DMDU approaches may, as such, be helpful for policy- and decision-makers when measuring cybersecurity performance and developing better cybersecurity policy in the future.

[152] Walker et al. (2001).
[153] Haasnoot et al. (2013).

5. Recommendations for the NCTV to improve cybersecurity governance

As noted in Section 2.1, a significant amount of current and upcoming work is focusing on developing a better understanding of the Dutch governance system and various ways to improve it. Several of the areas for improvement and potential improvement actions identified as part of this study have also been identified by other efforts or are currently being worked on by other stakeholders. The NCTV should, therefore, seek to coordinate and work with the relevant lead ministries or organisations within these areas within its role as the coordinator for national security. It is also essential that the NCTV monitors, reviews and addresses any outcomes from other evaluations, particularly the ongoing Dutch Safety Board evaluation of the Citrix incident and the upcoming evaluation of the NCSA.

This second phase of the cybersecurity state-of-the-art study has sought to highlight these areas of existing efforts, and aims to develop recommendations for areas where further knowledge or action may be required and where the NCTV may take on a lead or lead-coordinator role. As such, the NCTV should seek to:

1. **Continue working with the Ministry of Education and other responsible ministries** in the ongoing efforts to develop a replacement to dcypher, as well as exploring the possibility and potential value of developing a cybersecurity workforce management approach for national government with shared knowledge of the cybersecurity field, a common competency framework and better aligned training requirements and career paths.
2. **Continue working with *CIO Rijk* and *CISO Rijk*** to develop a comprehensive overview and understanding of the state of cybersecurity within the national government.
3. **Continue working with the Ministry of the Interior and Kingdom Relations** and other relevant stakeholders to assist in ongoing efforts to harmonise cybersecurity legislation and regulation.

In addition to these ongoing efforts, there are three overarching recommendations for the NCTV to consider for improving the governance of cybersecurity from a national security perspective:

1. Revisit the distinction between critical and non-critical infrastructure within the Dutch governance model.
2. Further investigate and invest in proactive approaches to national cybersecurity.
3. Further explore the role of minimum security standards and potential need for further authority to ensure compliance.

5.1. The NCTV should further explore and examine the role of the distinction of critical and non-critical infrastructure within the Dutch governance model

This study has identified the distinction between critical and non-critical infrastructure as one of the priority areas that both requires a better understanding and which could be improved in the future. The distinction between critical and non-critical infrastructure services or processes may be outdated and less fit-for-purpose due to the pervasive and interconnected digital environment. As explored in Section 2.2.4, this distinction also has significant implications within the governance structure, including for:

- The ability to identify critical services and dependencies across critical infrastructure sectors and society overall.
- Information-sharing flows between the NCSC, critical infrastructure organisations and the rest of society.
- The extent to which organisations face legal requirements and mandatory incident-reporting regimes.

As emphasised by workshop participants, it is therefore necessary to further explore and examine the process of how critical infrastructure is identified, how cybersecurity dependencies and risks are mapped, understood and shared, and what requirements are placed on organisations of varying criticality within the Netherlands. As such, the NCTV should seek to:

- Explore and assess alternative approaches to the identification and classification of critical infrastructure, including more horizontal and sector-agnostic approaches.
- Explore how dependencies between critical sectors and organisations can be better mapped and understood (see also the recommendations in 9 relating to critical infrastructure security).
- Explore how to improve information-sharing between critical and non-critical sectors to ensure that organisations receive the right information at the right time.

5.2. The NCTV should further explore and invest in proactive and preventative approaches to national cybersecurity, going beyond the current, more reactive paradigm

Within the decentralised model of governance found in the Dutch system, cybersecurity responsibilities are distributed across multiple ministries, government departments and organisations. The cybersecurity domain is also continuously evolving and requires constant adaptation, so it is important that the Dutch government remains agile, flexible and proactive in its approach to national cybersecurity.

As such, the NCTV should further explore and invest in proactive approaches to cybersecurity, including:

- Ensuring that regular and extensive exercises take place to stress-test and exercise governance structures and incident-response plans, so that all stakeholders have a well-developed understanding of their roles and responsibilities and develop good working relationships with their peers. These types of exercises should also include all possible parties, including central, regional or local government and the private sector.

- Exploring if and how the NCTV and the NCSC could set up and deliver more proactive cybersecurity services, including for example proactive vulnerability scanning of Dutch networks. It is possible that the UK ACD Programme can offer insight to possible ways of delivering these services, and which methods may have a positive impact to Dutch government and society.
- Investing in further research to how cybersecurity dependencies and system risks can be better identified and reduced (see also the recommendations in Chapter 9 on critical infrastructure security).

5.3. The NCTV should explore the role of minimum security standards and the potential need for further compliance mechanisms

This study also identified potential issues in relation to a lack of harmonised cybersecurity requirements across government and a lack of minimum cybersecurity requirements and standards, which may make it difficult to ensure a sufficient cybersecurity baseline across all organisations in the Netherlands. The study also found that there may be challenges to ensuring organisations comply with cybersecurity advice or guidance, even when specific vulnerabilities or threats have been identified.

Within this context, the NCTV should further investigate and explore the possibility to:

- Develop and implement minimum cybersecurity standards for national government in order to strengthen the minimum cybersecurity baseline across the various government ministries and departments, as well as to harmonise government IT infrastructure.
- Develop and implement minimum cybersecurity standards for private sector companies that supply IT services to national government in order to reduce supply-chain weaknesses and cybersecurity dependencies between sectors. This could also include the use of layered or sectoral standards, rather than one single standard for all.
- Explore the need for further authority for the NCSC or another government agency or department to evaluate, provide oversight and enforce cybersecurity advice or standards beyond the current 'comply-or-explain' framework that is currently in place. This could apply to national government or national government and private sector organisations, and could help improve verifiable cybersecurity across the Netherlands.

6. Critical infrastructure and technology

This chapter explores the first question of the second research area and consists of two sections:

- **Section 6.1** offers a brief introduction of critical infrastructure and technologies in the Dutch context based on desk research and a literature review.
- **Section 6.2**. discusses the first research question: the interplay between legacy critical infrastructure technologies and new technologies. This section draws on desk research and a literature review as well as interview and workshop contributions from the experts consulted by this study. Please note that any reference to 'workshop participants' in Chapter 6-8 should be understood as referring to all participants present.

6.1. Critical infrastructure, sectors and processes are all concepts that are widely used in the Dutch context

Critical infrastructure encompasses those services deemed necessary for the functioning of society (e.g. power plants, water supply systems, transport infrastructure, democratic institutions and government processes, etc.). Critical infrastructure, sectors and processes are all concepts that are widely used in the Dutch context as well as globally in legislation and policymaking. In this chapter, the following definitions are used:

- **Critical sectors** are those sectors whose assets, systems and networks (whether physical or digital) are deemed vital. This means that their interruption or destruction would cripple national security as well as the functioning of the economy and society.[154]
- **Critical infrastructure** refers to an asset or a system that is essential for the maintenance of vital societal functions, and whose destruction, damage or disruption would have a significant negative impact on national or EU security and the well-being of its citizens.[155]
- **Critical processes** are those whose failure or disruption could result in severe social disruption.[156]

The protection of critical infrastructure has been a major policy since the concept's introduction in 2002 when the government's Critical Infrastructure Project (CIP) was established in the Netherlands.[157] Since

[154] US Department of Homeland Security (2019).
[155] European Commission (2019).
[156] NCTV (n.d.a).
[157] Luiijf et al. (2017).

then, the definition has evolved and been updated to encompass all processes which, if disturbed or interrupted, would cause severe disruption and translate into a national security threat.[158] These processes are grouped into two categories – A and B. Category A consists of: national distribution and transportation of electricity; production, national distribution and transportation of gas; oil supply; drinking water supply, flood defence and water management; and storage, production and processing of nuclear materials. Category B includes regional distribution of electricity and gas, the military and the police.[159] Table 6.1 below summarises the meaning of these categories and which sectors they include.

Table 6.1 Classification of critical infrastructure in the Netherlands

Category	A	B
Definition	Critical infrastructure falls into category A if disruption, damage or failure would have an impact meeting *at least one* of the economic, physical or social criteria below and to cascade consequence, i.e. where the incident would result in at least two other sectors failing: • Economic impact of approximately 50 billion EUR in damage or around 5 per cent drop in real income terms; • Physical impact of over 10,000 persons dead, seriously injured or chronically ill; and/or • Social impact of over 1 million persons experiencing emotional consequences or social survival issues.	Category B refers to critical infrastructure where an incident would result in an impact meeting *at least one* of the criteria below: • Economic impact of around 5 billion EUR, or around 1 per cent drop in real income terms; • Physical impact of over 1,000 people dead, seriously injured or chronically ill; and/or • Social impact of over 100,000 persons experiencing emotional consequences or social survival issues.
Sectors concerned	Energy, drinking water, water, nuclear	Chemical production, IT/telecom, transport, finance, public order and security/safety, digital government processes, defence

Source: NCTV (n.d.a).

Ensuring the security of critical processes outlined above is perceived as one of the pillars of national cybersecurity and is also of particular concern due to its geopolitical importance, with demonstrated foreign nation-state activities and operations within critical sectors.[160] Recent trends to Internet-enable part of critical infrastructure and the adoption of emerging technologies or solutions present new challenges to the cybersecurity of critical infrastructure, and have led governments to investigate how best to secure them.

[158] NCTV (n.d.a).
[159] NCTV (n.d.b).
[160] Silfversten et al. (2019)

6.2. The interplay between legacy infrastructure technologies and new technologies creates several challenges

Legacy technology refers here to old methods, technologies, systems or application programmes that are outdated yet still in use. Applied to the computing context, legacy systems may refer to systems, programming languages or application software that are used instead of more up-to-date versions. This usually results from the high costs of replacing them combined with the rapid evolution of technologies used in parts of these systems. This section provides an overview of the main challenges identified as resulting from the interplay between legacy infrastructure and new technologies:

1. Risks resulting from liability and obsolescence challenges (Section 6.2.1);
2. The connectivity of operational technology and cascading effects (Section 6.2.2); and
3. The divide between specialists in operational technology and in information technology (Section 6.2.3).

Operational technology (also referred to as OT) is an umbrella term for the hardware and software that execute and control industrial processes. Operational technology is also referred to as Industrial Control Systems (ICS).[161] In the Netherlands, due to their long lifespans, legacy infrastructure technologies are still in use in numerous critical sectors. As a result, as one interviewee noted, while a significant focus on critical infrastructure cybersecurity has only been applied in the past five to ten years, it is crucial that cybersecurity capabilities in this domain, especially insofar as protecting legacy systems, are built quickly and efficiently.[162] This section outlines the risks and emerging solutions linked to the interplay between legacy infrastructure technologies and new technologies, resulting from desk research and consultations with experts. This interplay is also referred to as the 'physical–cyber convergence' or the 'OT/IT convergence'.

6.2.1. Liability and obsolescence challenges linked to legacy infrastructure technologies create a high risk of system failure or malicious exploitation

Many critical infrastructure providers, particularly in the operational technology space, rely on parts that are no longer supported by the suppliers (e.g. out of warranty or out of service). This creates liability challenges when actual use of products surpasses supplier or manufacturer responsibility (e.g. who is responsible in the case of an incident). In addition, high cost or resource requirements, lack of interoperability with legacy systems or a lack of skills may prevent necessary upgrades in critical systems – particularly in high-availability systems.[163] In fact, according to Paulsen (2020), several systems currently used in critical infrastructure have not been supported by their original manufacturers for over a decade, have no authorised replacement parts and do not have available patches to protect them from

[161] TNO (2019).
[162] INT11.
[163] Gartner (2019).

vulnerabilities. This creates a high risk of system failure or malicious exploitation, with the potential to cause major disruptions.[164]

In the Netherlands, consultations of category A critical infrastructure providers carried out by Garner suggest that issues linked to liability and obsolescence are known and addressed. Providers tend to adopt a standardisation approach to tackle these challenges: they use only standardised parts of operational technology in their assets and replace parts when they are no longer supported by the supplier.[165] However, consultations also suggested that the issue would benefit from a clearer understanding of the assets concerned and of the interplay between suppliers and buyers.[166]

Fox et al. (2019) point out that asset management and maintenance management with a clear, long-term approach – together with communication on risks of insufficient overview and possible consequences of failing to replace/update assets when required – may also offer a solution to this challenge.[167] Indeed, this was confirmed by experts consulted over the course of interviews as well as during the workshop for this study.[168] In addition, one expert consulted suggested that vendor requirements and/or service-level agreements between suppliers and buyers should address the question of security responsibilities, as is the case in several Asian counties.[169] Workshop participants also highlighted the need for clear agreements on security between vendors and buyers in order to better define the interplay between them and its impact in terms of security. Understanding this interplay, according to the experts, goes beyond the product or service itself and should be considered in relation to the asset as a whole and as part of a changing security environment.

6.2.2. The connectivity of operational technology and cascading effects between legacy and new or emerging technologies increase potential attack platforms

In addition to challenges linked to securing and maintaining legacy technology, a key challenge is linked to the connectivity of operational technology. The literature reviewed and experts consulted highlight the vulnerability of operational technology devices exposed on the Internet.[170] While the introduction of ICTs enables remote access and monitoring of critical infrastructure, it also brings ICTs and the networks they are connected to closer to the core function of critical infrastructure operators.[171] As such, new technologies may compensate for low cybersecurity on legacy systems, but they also introduce new vulnerabilities to these systems, which were previously more secure outside of their interaction with ICT.[172] This is particularly evident in the case of legacy systems, which do not have basic cyber protection mechanisms, nor the processing capability to perform basic cyber protection tasks. This lack of cyber protection mechanisms in legacy systems adds to the general risks that connectivity poses to all existing

[164] Paulsen (2020).
[165] Gartner (2019).
[166] INT08; INT16; RAND Europe workshop, 7 September 2020.
[167] Fox et al. (2019).
[168] INT11; INT13.
[169] INT16; RAND Europe workshop, 7 September 2020.
[170] Chromik (2020); INT08; INT11; INT12.
[171] INT08; INT10; INT12.
[172] INT12.

technologies.[173] The use of ICT-based technologies in monitoring and control of critical physical processes is crucial, but it also deepens global interdependencies and may bring new risks due to unknown technological developments. In the Dutch context in particular, cloud solutions used for remote access and remote monitoring would benefit from a more developed approach to security.[174] Emerging technologies like Industrial Internet of Things (IIoT) devices, blockchain technology, artificial intelligence and high bandwidth 5G connections will further increase the vulnerability of systems by providing new attack vectors.[175]

In answer to this challenge, the most common approach is to isolate key parts of operational technology by placing them behind a firewall and monitoring their access through management solutions.[176] However, as pointed out by one interviewee, this approach does not fully overcome vulnerabilities: if an attacker is able to overcome the encryption or to hack into an administrator's account, there may be no additional protective barriers.[177] Addressing risks related to this connectivity therefore requires the implementation of security by design. 'Security by design' was explained by one interviewee as a 'resilient life cycle management process', through which it can be ensured, from the point of design onwards, that a critical asset can adapt to current and future technological advances and needs through an integrated ability to sustain the addition of new technological elements.[178] This approach should be implemented when operational technology needs to be replaced.[179] This is a solution going forward, which is currently applied in some critical sectors, but does not solve the issue for ten-year old operational technology that does not yet need replacement, or where the resources needed to do so are lacking, as replacing legacy hardware is an expensive process.[180]

However, one suggestion of a potential solution that relies on good network architectureis that legacy systems should remain in use in the low-risk networks of the sector in question, but are replaced with new systems in high-risk networks. Such a solution would require risk analysis being carried out within a sector.[181] According to another expert, relying fully or partly on closed networks is already a practice in a few advanced sectors in the Netherlands, although this is not consistently applied.[182]

Through the implementation of the NIS Directive (Wbni) in 2018, the identification of ICT-dependent services is an essential step towards mapping connectivity of critical infrastructure. Article 5(2) of the Directive provides criteria for identifying operators of essential services:

1. An entity provides a service which is essential for the maintenance of critical societal and/or economic activities;
2. The provision of that service depends on network and information systems; and

[173] INT08; INT13; INT17.
[174] INT12.
[175] Luiijf et al. (2017); Bobowska et al. (2018); Taylor and Sharif (2017).
[176] Gartner (2019).
[177] INT08.
[178] INT11.
[179] Fox et al. (2019).
[180] INT08.
[181] INT12.
[182] INT08.

3. An incident would have significant disruptive effects on the provision of that service.[183]

According to the Wbni, providers of essential services have a duty of care to give notification of any digital incident to the NCSC. Providers of essential services are classified as shown in the table below.

Table 6.2: Classification of essential providers in the Netherlands

Sector	Subsector	Type of entity
Energy	Electricity	• Transmission system operator TenneT • Regional Distribution system operators
	Gas	• Transmission system operators • Regional Distribution system operators • Natural gas undertaking *De Nederlandse Aardolie Maatschappij B.V.*
	Oil	• *Stichting Centraal Orgaan Voorraadvorming Aardolieproducten* • Operators of oil production, refining and treatment facilities, storage and transmission
Transport	Air transport	• Royal Schiphol Group N.V. • *Luchtverkeersleiding Nederland* • Maastricht Upper Area Control Centre • *Koninklijke Marechaussee* • Each aircraft operator with over 25% of the total air movements at Schiphol in a year
	Harbour	• *De Divisie Havenmeester van het Havenbedrijf Rotterdam* N.V.
Financial	Banking	• Credit companies appointed by *De Nederlandse Bank* according to EU 575/2013 art. 4.1 (payments and securities trading)
	Financial infrastructure	• Operators of trading platforms as defined in point (24) of Article 4 of Directive 2014/65/EU of the European Parliament and of the Council • Central counterparties (CCPs) as defined in point (1) of Article 2 of Regulation (EU) No 648/2012 of the European Parliament and of the Council
	Settlement companies	• Appointed by *De Nederlandse Bank* based on *Wet financieel toezicht art. 1:1*
	Central securities depository	• Appointed by *De Nederlandse Bank* based on EU 909/2014 art. 2.1

[183] European Parliament and the Council of the EU (2016).

Health		• No essential providers identified by the Ministry of Health, Welfare and Sport
Drinking Water	Drinking water supply and distribution	• Suppliers and distributors of water as defined in the *Drinkwaterwet art. 1.1.*
Water	Flood defences, water management and surface water quality	• As determined by the Minister of Infrastructure and Water Management
Digital infrastructure	IXP	• Operators of IXPs as defined by art. 4, under 13 of EU 2016/1148 connecting more than 300 autonomous systems
	TLD name registries	• Any IANA registered TLD operator of a TLD register managing over 1 million domain names
	DNS service providers	• Any IANA registered TLD operator managing over 1 million domain names and operating as a DNS service provider as defined by art. 4, under 14 and 15 of EU 2016/1148
	Electronic communication networks and services/ICT	• Any operator of an ICT network or service, directly or indirectly used for telephone, SMS, Internet access for at least 1 million end users
Nuclear	Holder of permit Kernenergiewet art. 15b	• Nuclear energy production, processing and storage facilities
	Facilities appointed under *Geheimhoudingsbesluit Kernernergiewet, toepassingsbesluit 24/09/1971/nr 671/524*	• Protection of nuclear facilities • Guaranteeing security and confidentiality of data, equipment and materials used in the uranium enrichment process by separating isotopes using gas ultracentrifuges

Source: Ministerie van Justitie en Veiligheid (2018); Fraunhofer, CIPedia (n.d.).

A 2019 Netherlands Court of Audit report illustrates the importance of understanding cascading effects between legacy and new technologies. An incident in one part of a system or in one critical sector may result in significant consequences elsewhere in the system or society.[184] These cascading effects are challenging to map and fully understand, particularly as dynamic systems do not lend themselves to static mapping exercises (e.g. dependencies may quickly change as technology is upgraded or replaced). According to the WRR, the country currently lacks a coherent policy to prepare and protect critical infrastructure by planning for back-up options, isolation of chains and networks, cyber exercises and communication on how to respond to incidents. One of the WRR's recommendations to the government

[184] Algemene Rekenkamer (2019).

in 2019 was to prepare a Cyber-Dependency Assessment Report, with a detailed overview of parties, processes and services that are key for Dutch critical processes to function.[185]

6.2.3. Bridging the OT–IT divide is essential to tackling risks resulting from the interplay between legacy and new technologies

According to Radvanovsky (2018), the existing interplay between legacy infrastructure and new technologies is driven by two factors: 'the increasing pressure toward network-enabled systems and also the decreasing supply of those able to work in past logical environments'. Addressing associated risks therefore requires solutions addressing both a change in technology application and a change in organisational approaches to security.[186] Considering skills and training needs is indeed essential for addressing risks associated with this interplay.

A recent TNO report points out that several organisations in the Netherlands currently rely on a dedicated IT security team to be in charge of security for operational technology. However, this may not be a sustainable solution as it requires a single team to be in charge of too broad a set of responsibilities, all linked to security.[187] Furthermore, several experts pointed out that operational technology and IT currently function with different governance procedures and different risk identification processes.[188] This means that IT experts too often do not have sufficient knowledge of the functioning and maintenance of OT systems in order to effectively secure them,[189] while operational technology experts often demonstrate a lack of cyber awareness.[190] The introduction of new technologies, which are increasingly reliant on ICT, further translates into a need for critical infrastructure operators to expand their knowledge regarding cybersecurity in order to ensure the continued and safe functioning of the infrastructure.[191] Discussions emerging from the expert workshop also confirmed this skills gap and the associated challenge of bridging the divide between IT and operational technology specialists. While there is an important skills gap in the operational technology sector, there is also little understating of cybersecurity and IT-related issues among specialists in operational technology. As the interplay between both disciplines increases, bridging this gap is becoming crucial.

In particular, experts recommend investing in further research in operational technology as well as educational programmes specialised in operational technology.[192] This was reiterated at the time of the study workshop, where discussions focused on the need to address these issues through better knowledge transfer and skills- and capability-building. The lack of a shared vocabulary between the two disciplines plays an important role: experts highlighted that terms such as 'safety', 'security', 'reliability' or 'integrity' are used with different meanings in each discipline and that no shared language exists to address overlapping areas. This stands as an obstacle to bridging the gap between the two disciplines.

---

[185] WRR (2019).
[186] Radvanovsky (2018).
[187] Fox et al. (2019).
[188] INT10; INT13.
[189] INT10; INT12; INT13.
[190] INT10; INT11; INT12; INT13; INT14; INT15.
[191] INT10.
[192] INT09; INT11; INT12; INT14; INT15; INT16.

While overall, there is a clear understanding of interplay between legacy and new technologies and of associated risks among the Dutch critical sector, there is little action taken to address these risks. Consultations suggest that current solutions tend to be ad-hoc, patchwork solutions for a systemic issue that would require a holistic approach from both public and private sectors.[193]

[193] INT08; INT11.

7. Critical infrastructure and cybersecurity maturity

This chapter covers the second research question of the second research area, exploring how to understand and measure the cybersecurity maturity of critical infrastructure. It consists of four sections:

- **Section 7.1** offers a brief introduction to existing models for assessing cybersecurity maturity and presents related challenges identified by this study.
- **Section 7.2** discusses the tension between measuring cybersecurity maturity for critical infrastructure at the general level or at the sectorial level.
- **Section 7.3** explores the debate about the benefits of adopting a regulatory approach to cybersecurity maturity and of relying on a cooperative approach.
- **Section 7.4** stresses the need to consider supply-chain risks and interdependencies when measuring cybersecurity maturity.

This chapter draws on sources identified through desk research and a literature review, as well as interview and workshop contributions from the experts consulted over the course of this study.

7.1. This study identified several challenges related to existing cybersecurity maturity models

There are several global models in place with sets of indicators that are used to assess cybersecurity maturity in critical infrastructure. A maturity model can be understood as a benchmark for organisations to assess their capability in a given field against a set of indicators. These establish a baseline for consistent evaluation and allow organisations to set goals and priorities for improvement, based on their maturity level.[194] Models may also offer best practices, guidelines and principles to consider.[195] Existing cybersecurity maturity models can be general, for example the NIST in the United States, the International Organization for Standardization (ISO/IEC) standards or the European Union Agency for Cybersecurity's (ENISA) Security Incident Management Maturity Model (SIM3). Others are sector-specific like the US Department of Energy's Cybersecurity Capability Maturity Model (C2M2). In the Netherlands indicators used by assessors are based on general models, such as ISO.[196]

[194] Knowles et al. (2015); Department of Homeland Security (2014); Department of Energy (2014); Miron and Muita (2014).
[195] Miron and Muita (2014); ENISA (2019); Department of Energy (2014).
[196] INT10.

Existing models to assess maturity rely on measurable parameters, which are usually grouped around the three main components of cybersecurity: people, processes and technologies. These indicators tend to be qualitative (e.g. presence of code of conduct, of incident tracking system, incident prevention process, etc.); there are few quantitative indicators used in existing models and standards for ICS cybersecurity, and therefore for critical infrastructure cybersecurity.[197] The standards may be used by bodies evaluating cybersecurity in critical sectors (e.g. Dutch Court of Audit report, US Government Accountability Office, etc.). ENISA's SIM3, for instance, relies mostly on qualitative indicators, with measurable parameters grouped into five components derived from the people, processes, technologies trio: parameters related to the organisation (e.g. its mandate), human parameters (e.g. code of conduct, internal training, etc.), tools parameters (e.g. information sources list, incident tracking system) and process parameters (e.g. escalation to Governance Level, incident prevention process, reporting process). The model provides three steps of maturity depending on how developed and explicitly formulated these parameters are – basic, intermediate and advanced – and is meant to be used for self-assessment combined with peer review.[198]

Several studies have reviewed existing cybersecurity maturity models in the US and in Europe. Preliminary findings show that current models are fragmented and do not address the full extent and scale of critical infrastructure cybersecurity.[199] The experts consulted for this RAND study were divided with regards to existing standards and models. According to one interviewee, existing cybersecurity standards, if implemented correctly, would be sufficient to bring significant improvement in the following five to ten years.[200] However, several other experts noted that technological developments lead to rapid changes in cybersecurity; as a result, indicators of cybersecurity maturity are constantly changing. This entails that existing standards are under constant need for review.[201] Meanwhile, in order to be an efficient tool in designing secure critical infrastructure products, standards need to be developed with a strategic perspective that takes into account, to the extent possible, potential future technological developments.[202] For one of the experts consulted, current models consider only a minimum of potential threats.[203]

Some participants of the workshop also suggested that maturity models too often tend to focus on technical aspects of cybersecurity, when in fact these are not as important as wider procedures, management or design specifications. They suggested that addressing roles and responsibilities should be the first step of maturity models. One participant in particular highlighted that, in the Netherlands, it is crucial to rethink maturity and start with a more basic approach than is currently the case, including looking at basic steps in the procurement phase to outline roles and responsibilities.[204] At the EU level, a self-assessment tool for critical infrastructure operators is under development with the expectation that the results of these assessments can then be reported to competent authorities to provide a nationwide

[197] Knowles et al. (2015); ENISA (2019).
[198] ENISA (2019).
[199] Miron and Muita (2014); Knowles et al. (2015).
[200] INT17.
[201] INT10; INT16; INT17.
[202] INT17.
[203] INT13.
[204] RAND Europe workshop, 7 September 2020

estimate of the maturity of different sectors and different critical infrastructure operators.[205] In combination with the establishment of a baseline level of cybersecurity, this could allow governments to provide recommendations and guide critical infrastructure operators towards concrete solutions to improve cybersecurity levels. However, despite these efforts, one interviewee noted that it is unlikely that EU member states are currently able to accurately assess critical infrastructure cybersecurity maturity, primarily due to difficulties in determining and defining key performance indicators (KPIs).[206]

In addition, studies suggest there is a gap in the literature relative to the adoption of cybersecurity capability maturity models.[207] Experts consulted suggested that the lack of clear guidance on which model or standards to adopt is an obstacle for critical infrastructure providers.[208] Meanwhile, workshop findings show that several critical infrastructure providers – as well as policymakers – are not aware of the initial steps necessary to reach the first maturity level. These organisations can therefore not be audited and policymakers cannot provide guidelines on how to reach this level.

Finally, our review of the available literature suggests that there is little evidence on the effectiveness of maturity models. This was confirmed at the workshop, where experts commented on the need for robust assessment of the effectiveness of known standards, such as C2M2 or NIST. A limited understanding of which models are effective is an important obstacle to measuring cybersecurity maturity. Experts present at the workshop stressed that specific evaluations of existing models are needed, along with a comparative assessment of those currently in use in the Netherlands.[209] This would enable policymakers and organisations to make better informed decisions on which standards to adopt.

7.2. This study identified a tension between measuring maturity at a general level to favour applicability and at the sectorial level for further precision

Many of the challenges mentioned above result from the tension between pursuing general applicability of a given model and ensuring the precise measurement of maturity.

According to a few experts, the models and standards used by Dutch critical infrastructure operators tend to be too general and address only a minimum of potential threats.[210] Considering this tension, some experts suggested that cybersecurity capability maturity models should be specific to sectors.[211] Several called for the use of sector-specific indicators in measuring critical infrastructure cybersecurity maturity to allow for deeper evaluation of current capabilities. In particular, one explained that if we are to accept the premise that cybersecurity maturity is increased by relying on the regulations to respect specific standards, it is crucial that these standards are specific to each sector, their vulnerabilities and current maturity.[212]

[205] INT13.
[206] INT13.
[207] Miron and Muita (2014); CSR (2020).
[208] INT08; INT11; INT12.
[209] RAND Europe workshop, 7 September 2020.
[210] INT09; INT12.
[211] INT09; INT10.
[212] INT12.

However, the participants of the workshop brought additional nuances. On the one hand, they highlighted that critical sectors in the Netherlands already have different levels of maturity. The marine, nuclear and telecom sectors were perceived as being more advanced than sectors such as railways, prisons or the medical sector. Participants suggested that as sectors advance in silo when it comes to cybersecurity, they would benefit from relying on standards that are specific to their respective levels of maturity. On the other hand, standards require a common basis in order to ensure a minimum set of requirements and enable cross-comparisons between organisations or sectors: sector-specific standards risk limiting comparability and therefore the possibility of having an overview of maturity levels at the national policy level. They may also further inhibit cooperation between firms across sectors by removing a common basis of understanding regarding levels of cybersecurity maturity. The debate over the need for sector-specific standards links back to questions of governance, and whether critical infrastructure cybersecurity, as a horizontal issue, should be addressed with a general or sector-specific approach (see Section 2.2.3).

Some experts see this is as an area where the government could play a stronger role by providing sector-specific guidelines or indicators and ensuring these take into account risks specific to operational technology.[213] In addition, reconsidering what is being assessed may also play a role: cybersecurity maturity is assessed by sector in the Netherlands, and Europe in general, whereas it is assessed by function and operator in the US. The latter allows for identification of interdependencies at an earlier stage, which may result in more precise maturity assessments.[214]

7.3. There is a debate about the benefits of adopting a regulatory approach to cybersecurity maturity and of relying on a cooperative approach

Challenges linked to the application of existing standards and to the focus of current maturity assessments raise an underlying question regarding the policy approach to cybersecurity maturity. In terms of frameworks, two approaches can be distinguished globally: those that are regulatory (e.g. NIS Directive at EU level) and those that are cooperative and based on voluntary standards and sharing of good practices.

In a regulatory approach, the question of the assessors' knowledge and skills is important to consider. Research and consultations carried out suggest different levels of skills among assessors. According to Knowles et al. (2015), there is little guidance for assessors on evaluating compliance with standards. To measure cybersecurity, it is necessary to develop an approach for determining the available data, collecting it and defining metrics based on it.[215] Experts consulted for this RAND study also noted that some audit organisations lack key skills to understand and assess what is being measured. In particular, several experts mention that external audits tend to be carried out by IT specialists who have limited to no knowledge of operational technology.[216] In this regard, the Cyber Security Council (CSR – *Cyber Security Raad*) recommends that when conducting cybersecurity assessments of operational technology in critical

[213] INT09; INT10; INT12.
[214] INT13.
[215] Knowles et al. (2015).
[216] INT10; INT12; INT13; INT16.

systems, operational technology experts and employees who know the installation and can participate in making it more secure should be involved.[217]

Participants of the expert workshop suggested potential solutions to the challenge of assessors' skills. On the one hand, one echoed the CSR recommendation: ensuring cross-disciplinary teams that knowledge of IT and of operational technology as well as knowledge of the assets when conducting a cybersecurity assessment. On the other hand, others suggested the use of (self-)assessment frameworks that do not require specialist knowledge to implement. Among good practices highlighted in a 2019 Gartner report was the development of sector-specific frameworks with guidelines and assessment tools developed jointly between regulators and the industry. This kind of framework already exists in the Dutch nuclear and water sectors.[218] Understanding the types of skills needed to assess maturity based on the type of framework available was highlighted as a question requiring further investigation.

Discussions emerging from the workshop also suggested that some regulatory approaches could risk leading operators to assess their cybersecurity maturity as a 'checklist exercise' rather than to find solutions for risk mitigation. One expert suggested that this type of attitude is correlated with premature regulation and a lack of knowledge and understanding on the part of policymakers. Understanding motivations behind assessments and benefits linked to regulations was also identified as an area for further research. Finally, Ani et al. (2017) recommend the adoption of more stringent regulations through a risk-based approach that goes beyond compliance-based standards, and instead requires in-depth security-analysis measures based on procedures developed by operators to evaluate the risks related to their operations and service. This interactive and iterative process of risk management should be required from operators as part of normal operations, and should cover all constituent elements of cybersecurity (people, process and technologies).[219]

7.4. Including supply-chain risks and interdependencies in maturity assessments is essential to accurately assess cybersecurity maturity

In the technology industry, product complexity combined with a high number of suppliers results in a large attack surface that may have unknown interdependencies or vulnerabilities. Paulsen has described this as an 'assembly model'. In this ecosystem, malicious entities can enter the supply chain, while the product's complexity will prevent the introduced flaw to be seen immediately, creating high cybersecurity risks.[220] In the Netherlands, like elsewhere, many organisations outsource key services to third parties and rely on external suppliers, increasing the level of interdependence between processes and sectors. Consultations with experts suggest that, while the cybersecurity responsibility is on critical infrastructure operators, many cybersecurity gaps exist due to inadequate cybersecurity built into products and supply chains. According to interviewees, significant challenges to critical infrastructure cybersecurity arise partly as a result of vendors' influence; driven by economic considerations, vendors feel that products should be

[217] CSR (2020).
[218] Gartner (2019).
[219] Ani et al. (2017)
[220] Paulsen (2020).

offered at a low, competitive price and tend to sacrifice the cybersecurity of these products, which makes them unsuitable for use in critical sectors.[221]

According to the WRR, existing interdependences increase vulnerabilities and reduce the potential for back-up options or reversionary modes if an incident occurs. Additionally, there is little knowledge-sharing between organisations on the dependencies within supply chains and networks, and on the effect of takeovers, business or production-line closures, or investments in new technologies. This gap in information-sharing means there is little clarity on existing risks, and makes it difficult to identify incidents' severity and to inform relevant actors.[222] The current lack of visibility across the supply chain is an obstacle in the assessment of vulnerabilities and risks, and dependencies tend to be overlooked when measuring cybersecurity maturity.

As with other issues linked to cybersecurity maturity, critical sectors in the Netherlands do not all address the issue equally: according to one expert, the telecom sector is among the few areas that is aware of the need to assess and monitor supply-chain maturity. Overall, experts suggest a low level of awareness on the need for supply-chain cybersecurity maturity, due to the lack of visible threat.[223] Several experts consulted pointed towards the assessment of supply-chain maturity as an issue that will dominate the field of critical infrastructure security in the next decade.

In fact, regulators are starting to take this into account. At the European level, a framework for the energy sector covers supply-chain maturity, while future approaches will involve regulations and recommendations focusing on the responsibilities of the vendors.[224] This is also a focus of the US federal government, although it is still in the early stages on both sides of the Atlantic. A clear understanding of cross-border dependencies has not yet been achieved, even at the European level.[225] While this is a global issue, one expert suggested that this is of particular importance for small countries such as the Netherlands. This is because the Netherlands does not have the industrial base to manufacture all the critical infrastructure-relevant equipment, and therefore has no choice but to purchase it from abroad.[226]

A geopolitical dimension is therefore inherent to the question of critical infrastructure supply chains. Interdependencies in cross-border supply chains make it difficult for providers to have control over all the potential liabilities of the parts that are manufactured and shipped from across the world. In this sense, a good overview of each critical infrastructure operator's supply chain, along with its suppliers' own supply chain, is needed. Because of the interdependent nature of supply chains, this should be a combined effort on the part of sectors and industry, as well as international partners. Of course, there are strong commercial incentives for industry to not take part, given the complexity, cost and fact that sharing such information could erode their competitive advantage over others by exposing information on their own suppliers, not to mention eroding shareholder confidence by exposing how fragile some of the links may be. Yet, a good view and understanding of critical infrastructure operators' supply chains could also lead

[221] INT12.
[222] WRR (2019).
[223] INT12, INT13.
[224] INT13; INT14; INT15.
[225] INT13.
[226] INT12.

to identifying more secure alternative providers, which is important in managing supply-chain security.[227] This geopolitical dimension therefore brings an added layer of complexity in the need for cooperation between private and public sectors, and is crucial to consider when looking at threats from specific actors, as further explained under Section 8.4.3.

Experts consulted provided key insights into potential approaches to addressing supply-chain cybersecurity maturity. In this process, three levels need to be addressed:

1. First, operators need to understand the components of their supply chains, and of their suppliers' supply chain.
2. Second, operators need to evaluate, assess and rank the discovered vulnerabilities.
3. Third, operators need to decide how to address those vulnerabilities.[228]

Addressing the first level links back to solutions discussed under Section 6.2.1, whereby the government could adopt a role in providing clear vendor requirements in procurement guidelines. Indeed, one of the problems identified by interviewees has been the inability to assess the cybersecurity of vendors or impose cybersecurity standards in contracts with large corporations. Experts suggested that the government could create regulations around cybersecurity standards for suppliers of critical sectors, and hold suppliers accountable to respecting these roles and responsibilities.[229] Beyond the role played by governments, it is crucial for organisations that processes, roles and responsibilities of each party are clearly identified in contracts. This would already be an indicator of supply-chain cybersecurity.[230]

Regarding the second level, some experts suggest that suppliers could be involved in identifying and disclosing vulnerabilities. This could be done by providing recommendations and guidance on how best to secure the installations they have designed.[231] In addition, this also links back to the adoption of a risk-based approached discussed under Section 7.3, which would force operators to carry out holistic risk assessments. Such assessments would allow for the identification of vulnerabilities across the whole supply chain, and enable measures to be identified to tackle them through large-scale collaborations in risk-management and information-sharing. According to Knowles et al. (2015), this is only likely to happen with new regulatory developments.[232] Only then would it be possible for operators to consider the third level and decide how to address identified vulnerabilities and secure their supply chains.

[227] INT12; INT14; INT15; INT17; INT13.
[228] INT14; INT15.
[229] INT12; INT17; INT16.
[230] INT17; INT11; INT16.
[231] INT12; INT17.
[232] Knowles et al. (2015).

8. Critical infrastructure and improving cybersecurity

This chapter covers the third and fourth research question of the second research area, exploring how to improve the security of operational technology deployed in critical sectors. It consists of four sections that present potential approaches to improving cybersecurity of operational technology in critical infrastructure and preventing damage resulting from potential threats from external actors:

- **Section 8.1** presents the need for an integrated and multi-faceted approach to the cybersecurity of critical infrastructure. This section draws mainly on desk research and literature review and on some contributions from the experts consulted.
- **Section 8.2** discusses the need for information-sharing across Dutch critical sectors. This section draws mainly on desk research and a literature review, and on some contributions from the experts consulted.
- **Section 8.3** outlines the need for a change in organisational structure. This section draws mainly on desk research and a literature review, and on some contributions from the experts consulted.
- **Section 8.4** discusses the fourth research question of how to prevent damage from potential threats from actors and organised groups or networks of actors. This section draws mainly on interview and workshop contributions from the experts consulted for this study.

8.1. Critical infrastructure cybersecurity should rely on an integrated and multi-faceted approach

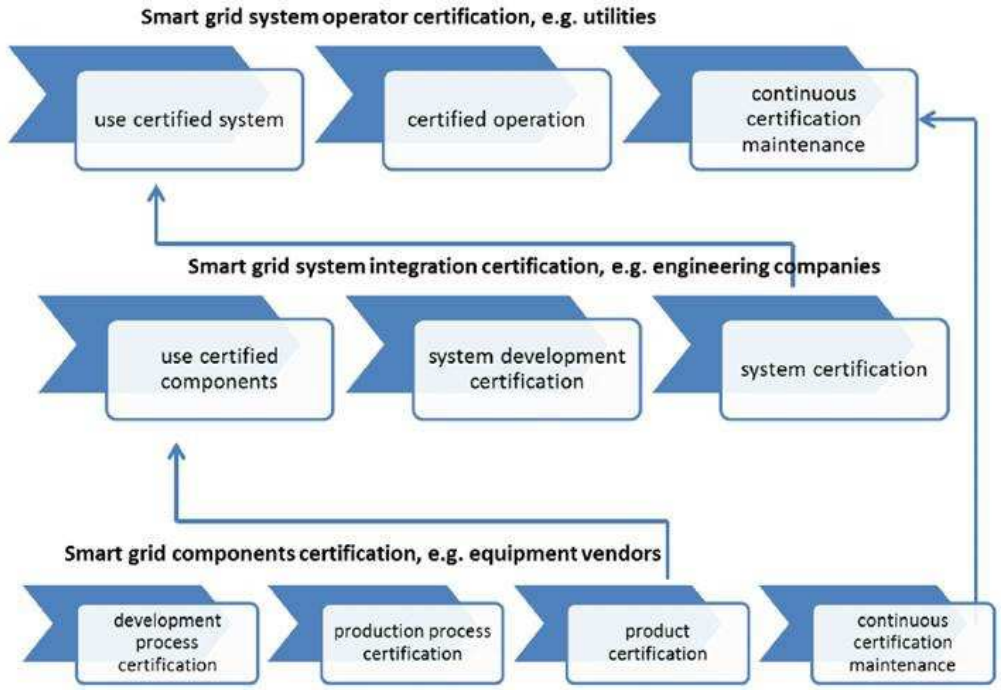
Improving the cybersecurity of critical infrastructure relies on an understanding of the interplay of legacy and new technologies (discussed in Section 6.2), and on addressing the cybersecurity triangle of people, processes and technologies. While addressing the technology may not always be an option, especially in the case of legacy operational technology, adjusting practices linked to people's attitudes and behaviours and processes in place is key. Existing research and experts consulted recommended several practices to improve the security of operational technology in critical sectors, all relying on an integrated approach to cybersecurity.

Existing measures in the Netherlands relate to standardisation and isolation, as mentioned under Sections 6.2.2 and 6.2.3. In addition to these, the Cyber Security Council also recommends the establishment of certification systems with common standards.[233] With regards to certification, one interviewee noted that

[233] CSR (2020).

in several instances, existing certification processes focus on products alone, whereas they should rely on holistic certification processes, integrated into a secure and certified environment, where people operating and maintaining the product do so in a secure, certified manner. This is also a recommendation of ENISA, in the form of smart grid certification, as illustrated in Figure 8.1.[234]

Figure 8.1 Example of a holistic certification approach for smart grid



Source: ENISA (2014).

Beyond certification, Ani et al. recommend a multifaceted approach including risk assessment, control and mitigation, trainings, systematic secured processes and technical security approach. Examples of secured processes include, for instance, implementing a 'separation of duties' whereby any complex operational task should be broken down and allocated to several persons, or a policy ensuring that users and programmes operate with only the minimum of privileges required for their function.[235] Such questions of access and control emerge as crucial to securing operational technology in critical sectors.[236] Technical security approaches rely on securing the environment through measures such as secure network architecture, an intrusion-detection system, access controls, firewalls or cryptography, to name a few. These measures were mentioned by interviewees with particular reference to shielding legacy technology and isolating operational technology from the Internet.[237] Overall, an integrated approach to cybersecurity of operational technology should not only consider what should be secured, but also different existing

[234] INT10.
[235] Ani et al. (2017).
[236] Alcaraz and Zeadally (2014); Paulsen (2020); Ceron et al. (2019); INT08.
[237] Assante and Lee (2015); Ani et al. (2017); Alcaraz and Zeadally (2014); INT17.

risks for different environments, such as Internet-connected networks, clouds and closed networks, as well as the infrastructure itself.[238]

Finally, such an approach should be coupled with ongoing research on technological developments and their associated potential and vulnerabilities. Research suggests that recognising that technology and operational trends are continuously transforming and transforming the industry, which also affects security trends, is key.[239] Paulsen (2020) notes that as automation of processes increases, the need for fast, secure risk-management solutions and security measures becomes ever more urgent, but research in this area remains limited.[240] The literature suggests that future research in this area should focus on leveraging emerging technologies. Fields that would benefit from such research include:

- **Supply-chain management**, including for instance hash-chain or cryptographic audit logs;[241]
- **Zero trust architecture**, i.e. determining how much access a user or device should have through identity- and access-management solutions integrating continuous monitoring;[242]
- **Inventory management**, an approach called for by stakeholders (see Section 6.2.1) is for automated processes and Artificial Intelligence (AI) to facilitate solutions, which could mitigate some of the risks linked to the interplay between legacy and new technologies;[243] and
- **Self-healing**, which as a research area is still in its infancy but may provide an avenue for securing operational technology in critical sectors, enabling systems to recover autonomously when required by relying on back-up copies and duplicating functionalities.[244]

8.2. Cross-sectoral information-sharing is crucial for improving security of Dutch critical infrastructure

Information-sharing and coordination between critical sectors are crucial to help improving operational technology cybersecurity, and are areas where the government could have a role to play. This includes sharing knowledge related to operational technology among operators, sharing vulnerabilities and involving suppliers in the conversation.

At the European level, ENISA recommends establishing schemes for incident reports.[245] In fact, according to several experts, the Netherlands is amongst the most advanced countries in Europe with regards to information-sharing in cybersecurity, and in particular in critical infrastructure. This results from the *Polder* model of governance (see Section 2.1) and the associated Dutch approach to collaboration, which has led industries to ignore competition considerations over cybersecurity and instead cooperate to achieve

[238] INT08.
[239] Ani et al. (2017)
[240] Paulsen (2020).
[241] Paulsen (2020).
[242] Paulsen (2020); Alcaraz and Zeadally (2014).
[243] Paulsen (2020); Alcaraz and Zeadally (2014).
[244] For an overview of existing research in this area, see Alcaraz and Zeadally (2014).
[245] ENISA (2015).

common security by sharing information about possible threats and incidents.[246] Indeed, cybersecurity in the Netherlands relies on several information-sharing communities, including the Electronic Crimes Task Force (ECTF), Financial Intelligence Unit NL (FIU-NL), *Beveiliging en Publieke Veiligheid Schiphol* (BPVS) and Information Sharing and Analysis Centres (ISACs). ISACs are sector-specific platforms that include representatives from the General Intelligence and Security Service, the national High Tech Crime Unit, the NCSC (which hosts those platforms), and the Dutch National Detection Network (NDN), through which organisations can exchange good practices and lessons learned as well as incidents, vulnerabilities and potential threats.[247]

Information-sharing, however, still suffers from established challenges linked to issues of trust and confidentiality in the sector. Luiijf identifies lack of trust as a significant obstacle to security improvement of operational technology. This issue was also highlighted by an interviewee who noted that lack of trust within and between critical sectors and with the government leads to challenges in deploying and applying tailored advice in case of cyberattacks.[248] According to Luiijf, defining the environment for information-sharing is crucial if this obstacle is to be addressed; this includes both the physical environment as well as the format of meetings, and the stakeholders involved.[249] Several interviewees saw this as an area where the government, and in particular the NCSC, can play a role, by providing a platform to facilitate discussions, information-sharing and knowledge exchange. They also saw a role for the government in promoting collaborative behaviour by sponsoring the time that mature actors can donate to share lessons learned with less mature actors, which is already happening in a few sectors. It should be noted that interviews – as well as the expert workshop – suggest that the government should adopt a role of facilitator only. Therefore, public-private partnerships – such as those that already exist in the form of organisations like the ISACs – are the preferred approach by experts, rather than a stronger regulatory approach.

However, existing organisations, including the ISACs, do not allow for information-sharing between critical sectors, which is crucial due to the interdependencies that exist. This need for greater information-sharing and coordination between critical sectors is among the Cyber Security Council recommendations, and was raised by several interviewees and in the workshop.[250] Workshop participants suggested a need for a platform that offers greater accessibility than the ISACs, and to more stakeholders, which would facilitate cooperation between the public and private sectors. This might include suppliers, who could bring an additional dimension to a community of information-sharing on the security of operational technology in critical sectors. In particular, moving the focus of information-sharing centres from sectoral to thematic was seen as necessary to allow for cross-sectoral cooperation. The possibility of creating an ISAC specific to operational technology (or OT-ISAC) was discussed, where stakeholders across the supply chain would address issues and threats specific to their operational technology. This approach is already under exploration by TNO and the NCSC as a potential solution to this need. Workshop discussion suggested that such an OT-ISAC may also provide a platform for sharing vulnerabilities without making them public, and therefore ensuring that all those who need to know about them across

[246] INT09; INT11; INT13.
[247] ENISA (2019); Luiijf (2016).
[248] INT09.
[249] Luiijf (2016).
[250] INT11; INT14; INT15; INT16; INT17

the supply chain are made aware without informing actors who may use the information illegally or maliciously. In addition, one expert suggested that cross-sectoral information-sharing should also not be limited to critical sectors. The current COVID-19 public health and economic crisis has shown that more sectors are more important than previously considered, despite them not being labelled as critical infrastructure.[251]

Regarding the type of information to share across sectors, cross-sector exercises and vulnerability disclosure appear as the main area that would benefit from accrued cooperation.[252] Conducting joint cross-sector cyber exercises is also essential as part of a broader effort to establish risk analysis based on modelling and simulations, as discussed in more detail in Section 4.3.6.[253] According to discussions in the workshop, some critical sectors in the Netherlands are already evolving in this direction, through a shift from individual to collective horizon-scanning and cyber exercises. This deepening of the approach toward identifying vulnerabilities is essential to better understand potential damages across critical sectors. In addition, workshop discussions suggested that existing vulnerability disclosure programmes are well established in the IT environment, but there is little knowledge regarding how these can be applied to the environment of OT. It emerged that to understand how best to share vulnerabilities and address them across sectors, further research is necessary into how the community working on operational technology could use similar programmes.

8.3. Change in organisational structure towards multi-disciplinary teams would help improve security and understand risks and vulnerabilities

As previously addressed (see Section 6.21.1), improving cybersecurity relies on better skills and awareness from people working in critical sectors. This is especially true with regards to OT, where two important gaps exist with regards to specific skills and to cybersecurity awareness among specialists. This issue needs to be addressed through multiple approaches, ranging from education to division of resources within organisations.[254] Implementing a change in organisational culture towards the development of multi-disciplinary teams is among the key solutions to bridge this gap. This evolution relies on increasing knowledge and skills within teams as well as changes from a business strategy perspective.

Several experts noted the need to educate operational technology experts on IT and IT experts on operational technology. In critical infrastructure, IT and operational technology can essentially be viewed as two different cultures that need to merge into one so as to work effectively towards the same goal.[255] This is seen as key in ensuring that all employees involved with operational technology in critical sectors understand why certain norms and practices are relevant and important in order to maintain system security. Staff awareness is crucial, particularly because in many cyberattacks – such as ransomware or phishing – social engineering plays the biggest role; while IT experts are aware and careful around

[251] INT10.
[252] CSR (2020).
[253] Luiijf (2020); Alcaraz and Zeadally (2014).
[254] Radvanovsky (2018).
[255] INT10; INT11; INT13; INT14; INT15.

malware-related messages and know how to avoid them, the same cannot be expected from operational technology experts. This understanding is also essential at the high management level, which needs to implement the necessary changes that are conducive to increase staff awareness and education, as well as to provide the necessary resources, both financial and human.[256] It is therefore important to develop multidisciplinary teams within organisations, to include operational technology experts, IT experts and contract lawyers. With their expert knowledge of the systems' maintenance processes, the specific cybersecurity threat, and the language in which provisions need to be spelled out in order to be enforceable with suppliers or contractors, these teams could then address any potential issues in a more comprehensive manner.[257]

In the US, NICE provides education and support for the development of a workforce equipped with the necessary knowledge and skills in cybersecurity (see Section 3.3.2 for further detail on their workforce strategy). NICE recommends cybersecurity workforce planning as a key component of organisations and suggests good practices towards achieving necessary cyber awareness among teams. One practice includes ensuring a link between business strategy and cybersecurity workforce requirements.[258] This was echoed by an interviewee who noted that, in terms of manpower resources, it is essential for high management to understand the need to have employees whose job is dedicated solely to ensuring the security of critical infrastructure systems, from both a traditional and a cybersecurity perspective. This is because ensuring security is a day-to-day job, not limited to the security review processes undertaken a couple of times a year.[259] Similarly, another interviewee suggested that incorporating cybersecurity skills-needs into a written multiyear strategy can ensure that they remain a priority.[260] This requires cultural and structural changes within organisations, relying on a better understanding of cybersecurity at several levels. In this context, the Dutch government may be able to provide support in a similar format as the US's NICE.

8.4. This study explored approaches to prevent damage to vital infrastructure resulting from potential threats from actors and organised groups or networks of actors

There is little research and evidence available on the protection of critical infrastructure from the angle of existing threats from actors and organised groups. This is because much of the research on critical infrastructure is relatively actor-agnostic. However, consultations with experts and discussions resulting from the expert workshop provided some insights on the topic, as outlined in this section.

8.4.1. The current priority should be on tackling immediate threats

According to several interviewees, cybersecurity is not sufficiently mature in the Netherlands to approach critical infrastructure protection from the angle of threats from actors and organised groups. Instead, the priority should be on threats that may seem lesser but are more immediate. On the one hand threats such

[256] INT09; INT10; INT12; INT13; INT16.
[257] INT11; INT13.
[258] DHS (2014).
[259] INT12.
[260] INT10.

as ransomware may be less disruptive, but they are more prominent, even if they are often not targeted specifically at critical infrastructure.[261] In addition, some threats are non-intentional, such as physical threats (e.g. disruption or damaging of physical cables, antennas etc.), and are rarely taken into account in risk management.[262] One expert also suggested that without adequate situational awareness of an operator's assets, equipment misconfigurations or malfunctions can sometimes be mistaken for attacks.[263] While protecting against these threats requires basic cybersecurity hygiene and awareness, so should easily be mitigated, this is not always the case in critical sectors.

Advanced Persistent Threats (APTs), on the other hand, are more difficult to defend against. This is because, in being politically motivated, the actors carrying them out usually study the critical infrastructure environment they will be attacking and tailor their actions to observed vulnerabilities. Assante and Lee (2015) describe this process as an 'operation campaign' relying on two stages: an intelligence-gathering operation to understand system weaknesses and overcome protection mechanisms, and a second stage using this knowledge to carry out an attack.[264] Considering the time and capabilities required for such an attack, they are less likely to occur frequently. Given the current levels of cybersecurity maturity, experts therefore felt that critical sectors should focus primarily on the first category of threats.[265]

8.4.2. A better definition of roles and responsibilities between the government and private sector is necessary

Defining responsibilities around the identification of external threats to critical infrastructure was highlighted as a critical issue over the course of interviews for this study. Indeed, some understood this as an issue beyond cybersecurity, which focuses on defending an attack regardless of the actor, while others felt this was an area that requires collaboration across private and public sectors, as well as beyond cybersecurity alone.

According to several experts, understanding the threat landscape is not the responsibility of the critical infrastructure operator, but of law enforcement. They felt that government actors should especially take on more responsibility when it comes to preventing threats from state actors. For example, this could be done by means of more information-sharing between intelligence services and critical infrastructure operators regarding the state actors in the threat landscape, which could help critical infrastructure operators to construct more accurate and comprehensive risk assessments. The critical infrastructure operator's role is then to defend against these threats. Since the same measures can protect against multiple actions from multiple actors, knowing the motivation, intention or identity of the actors is irrelevant to the critical infrastructure operator.[266]

In addition, some experts noted that effective protection and response in the case of attacks on critical infrastructure requires national, interagency cooperation, since a nation's response to a cyberattack on

[261] INT10; INT11; INT17.
[262] INT10; INT11.
[263] INT16.
[264] Assante and Lee (2015).
[265] INT10; INT12; INT17.
[266] INT08; INT10.

critical infrastructure may not always lie in the cyber realm itself.[267] This is an area where cooperation between the government and the private sector can help to prevent damage from attacks. In the US – and also relevant for the Dutch context – deterrence is seen as an issue that necessitates alignment between government critical infrastructure operators by:

1. Encouraging the private sector to improve policies, procedures and coordination; and
2. Being proactive in pre-empting the threat by identifying risks and actors, in partnership with the private sector.

In the Netherlands, the NCSC is currently working on agreements with several private operators, such as Siemens, to ensure that any security breaches are disclosed in advance so that the NCSC can prepare a response and recommendations to other sectors before the breach is made public.[268] However, consultations as well as the expert workshop highlighted that knowledge of operational technology is currently too low among government actors, while it should be an essential premise for effective collaboration on these issues. In particular, this prevents the government from being able to provide valuable guidelines specific to preventing damage to the critical infrastructure.[269]

This was extensively discussed during the study workshop, where it emerged that there is a lack of clarity on expected roles and responsibilities when it comes to protecting critical infrastructure from external threats. On the one hand, the lack of expertise on operational technology among government actors prevents them from taking a leading technical role, and on the other hand critical infrastructure operators should not be expected to have the geopolitical and criminological expertise required for protecting themselves against external threats and identifying actors responsible for a given attack. The Department of Homeland Security (DHS) in the US and the *Bundesamt für Sicherheit in der Informationstechnik* (BSI) in Germany have forensics teams that provide guidance and evaluation services to critical infrastructure operators as trusted partners. Understanding the roles adopted by government bodies, critical infrastructure operators and other potential actors in preventing and investigating attacks to critical infrastructure in different countries – and investigating what would work in the Netherlands – emerged as a key area for research.[270]

8.4.3. As a geopolitical issue, this question requires a geopolitical approach

As outlined above, protecting critical infrastructure from APTs emerged as a geopolitical issue that should therefore be approached from a geopolitical point of view, alongside identification of external threats, adoption of a geopolitical strategy and cooperation with like-minded nations.

When it comes to state actors, interviewees felt that there has been too much of a focus on the technical aspects of the possible actions that they could carry out in cyberspace that could damage critical infrastructure. It was felt that focusing on the actors themselves would be a more efficient strategy. Because state actors exist within a geopolitical landscape, and attacking critical infrastructure is equal to

[267] INT14; INT15.
[268] INT09.
[269] INT09; RAND Europe workshop, 7 September 2020.
[270] RAND Europe workshop, 7 September 2020.

attacking the safety and well-being of citizens, this is a political problem that requires a political solution.[271] When considering potential approaches to protect critical infrastructure from APTs, some of the literature suggests the creation of a classification of actors by level of threat and possible prevention as a way forward. Indeed, a 2019 Gartner report suggests that for attacks that are uncommon and technically advanced (i.e. from professional criminals and terrorists), it is best to focus on early detection and quick response. Meanwhile, very advanced attacks, which are difficult to predict as attack patterns may not be known, require a focus on recovery options (e.g. options for manual operation and quick recovery). These recommendations can be built into a framework focused on actors and the level of threat they represent.[272] To do this, risk management should look at actors' intent and capabilities.

This was also noted by some interviewees, who highlighted the complexity of the APT threat landscape given the interconnected nature of state actors, criminal organisations acting as state proxies, and private criminal organisations being offered safe haven by some states.[273] Because of the breadth and the constantly changing nature of the threat landscape, organisations often find it difficult to match their existing and known vulnerabilities with information about the potential threats, as filtering what is relevant to their specific circumstances is a complicated and time-consuming undertaking.[274] The expert workshop also led to similar considerations, linking this to the ongoing global discussion on the adoption of 5G and the role of Chinese suppliers. Foreign state-owned enterprises interwoven into the supply chain of a critical infrastructure system may be able to gather intelligence and ultimately weaponise it.[275]

Considering the constant evolution of the geopolitical situation, interviewees also referred to states whose internal situations and foreign aspirations are changing quickly, making it increasingly difficult to anticipate external threats.[276] Some suggested that understanding the individual interplay between intentions and capabilities is key to a successful deterrence and defence strategy. In fact, according to them, countries that are most successful when it comes to cybersecurity are those who integrate cyber capabilities and cyber protection in an overall, multi-layered defence strategy, alongside the rest of their military and security defence capabilities.[277]

To this end, some of the literature suggests that international guidelines and standards may provide a helpful basis to tackling these issues. In particular, Haber and Zarsky (2017) note that strategies for compliance with international standards should be developed in combination with global information-sharing platforms.[278] This was echoed by one interviewee who called for the establishment of international guidelines in the form of policies and accepted norms akin to the Tallinn Manual, clearly designating critical infrastructure as a non-acceptable target in international law.[279]

[271] INT11.
[272] Gartner (2019).
[273] INT14; INT15.
[274] INT10.
[275] Cilluffo (2020).
[276] RAND Europe workshop, 7 September 2020.
[277] INT14; INT15.
[278] Haber and Zarsky (2017).
[279] INT11.

9. Recommendations for the NCTV to improve critical infrastructure protection and cybersecurity

Given the myriad of challenges related to the protection of critical infrastructure, this chapter presents recommendations emerging from this second phase of the cybersecurity state-of-the-art study. A set of priority recommendations for the NCTV has been identified, with a focus on two cross-cutting issues of key importance to ensure and improve the protection of critical infrastructure:

1. The current skills gap in critical infrastructure; and
2. The lack of visibility across the critical infrastructure supply-chain.

In addition, secondary recommendations for tackling specific areas of critical infrastructure protection are also listed below.

The NCTV should work with responsible ministries and other organisations to encourage and support skills development in cybersecurity and engineering, which remain a high priority for the protection of Dutch critical sectors in the immediate term

As outlined in previous sections, the current skills and knowledge gap in critical infrastructure results in significant challenges, ranging from undermining the cybersecurity of assets themselves to limiting the ability of assessors to provide valuable insights into the cybersecurity maturity of an organisation. This translates into risks at all levels and is a potential enabler for external attacks.

As discussed in a previous RAND Europe report, current skills gaps in engineering, digital and highly specialised skills risk jeopardising the sustainable functioning of Dutch critical infrastructure.[280] As outlined in Section 6.2.3, these gaps are further reinforced by the teaching, learning and implementation of the operational technology and IT disciplines as independent from one another. While the issue is already acknowledged within the EU and in the Netherlands, it was emphasised by all experts consulted over the course of this study as remaining the priority area for the protection of Dutch critical sectors.[281] There is currently an ongoing effort at the European level to assess digital skills of EU citizens and future needs.[282] However, findings from this study show that immediate-term measures are needed to address the skills gap and to bridge the current OT–IT divide. The NCTV should therefore work with the responsible ministries to:

[280] Retter et al. (2020).
[281] European Centre for the Development of Vocational Training (2016); Nederland Digital (2019).
[282] European Commission (2020).

- Invest in research and awareness on operational technology within the government to ensure that dedicated bodies – such as the NCSC – can provide appropriate recommendations and guidelines, especially in cases of malicious attacks. This would also build trust and benefit collaboration between the government and industries.[283]
- Create synergies between academia, vocational training (*Hoger beroepsonderwijs* – HBO), industry, regulators and the government by implementing measures such as job rotations in critical sectors, secondments for public servants, compulsory internships for students and guest lectures from stakeholders across the industry supply-chain, and with regulators.[284]
- Integrate elements of operational technology and IT academic curricula to build shared understanding across both disciplines and further collaboration at both academic and industry levels.[285]
- Increase cybersecurity awareness among specialists of operational technology by teaching elements of cybersecurity to students of engineering, as well as providing cybersecurity trainings to specialists of operational technology working in critical sectors.[286]

The NCTV should support the development of tools to understand and address the risks linked to the critical infrastructure supply-chain

As mentioned in Section 7.4, supply-chain cybersecurity maturity is expected to be one of the key issues dominating the field of cybersecurity in the next decade. However, it is still in its infancy as a research area. In addition, gaining visibility across the supply chain of critical infrastructure remains a challenge due to the complex interdependencies interwoven in it. This challenge affects the security of critical infrastructure in several ways, from further complicating liability issues in case of accidents or attacks to potentially enabling malicious actors by having a state-owned or -backed supplier operating maliciously from within the supply chain of a critical sector. Understanding vulnerabilities and risks linked to the critical infrastructure supply-chain is therefore essential to the protection of Dutch critical sectors. Areas for further research and action include:

- Broadening existing risk-mapping models to encompass the whole critical infrastructure supply-chain, including externalities. Experts suggest that existing risk models provide a solid basis to expand to the whole critical infrastructure supply-chain. This could rely on supply-chain management, by leveraging new technologies (as outlined in Section 8.1). In addition, this could rely on assessing risks based on service delivery and service continuation, rather than on operators, in order to better identify interdependencies. For instance, this would require including cloud operators and telecommunications operators when assessing risks to smart-grid service delivery.[287]

[283] INT09; RAND Europe workshop, 7 September 2020.
[284] RAND Europe workshop, 7 September 2020.
[285] RAND Europe workshop, 7 September 2020.
[286] INT10; INT12; INT13; INT14; INT15; INT17; RAND Europe workshop, 7 September 2020.
[287] INT13; RAND Europe workshop, 7 September 2020.

- Investigating potential avenues for international cooperation on addressing critical infrastructure supply-chain vulnerabilities and developing geopolitical alliances and European or alliance-based approaches to tackle uncertainties linked to international supply-chains, e.g. to inform risk-mapping models to include externalities and tackle foreign threats. In the EU, this requires further collaboration on mapping interdependencies. At national level, this would also require a discussion at the policy level on how to tackle technologies and components supplied from countries like China or Russia.[288]
- Enabling information- and knowledge-sharing specific to operational technology in order to gain better understanding and visibility of operational technology products' supply-chain and associated risks, through initiatives such as the development of an information-sharing platform specific to operational technology, or an OT-ISAC – a project currently under discussion between the NCSC and TNO.[289] A feasibility study of this endeavour would be a beneficial first step. In addition, applied research for vulnerability programmes specific to operational technology also emerged as a necessary step to better understand specific risks to the operational technology supply-chain.

Additional recommendations for improving the protection of critical infrastructure

In addition to the cross-cutting recommendations outlined above, this study has identified additional secondary recommendations to improve the protection of Dutch critical infrastructure. These are specific to issues discussed in Chapters 7-8, namely:

- The lack of research on existing cybersecurity models;
- The debate on adopting a regulatory or voluntary approach to cybersecurity maturity;
- The need for a change in organisational structure; and
- The lack of framework for tackling APTs.

To address these challenges, the study has identified a set of recommendations:

- Developing the evidence base on cybersecurity maturity models by conducting robust and independent evaluations of the effectiveness of maturity models, and by comparing existing models. Further research should also focus on whether existing models require specialist assessors.[290]
- Developing the evidence base on current approaches to cybersecurity regulations in critical infrastructure by investigating differences between general and sector-specific standards and their impact on the cybersecurity of critical infrastructure. In addition, conducting behavioural research on the impact of regulatory approaches as opposed to voluntary standards may also help identify the adequate type of approach for the current needs of Dutch critical sectors.[291]

[288] INT12l INT14; RAND Europe workshop, 7 September 2020.
[289] INT13; RAND Europe workshop, 7 September 2020.
[290] RAND Europe workshop, 7 September 2020.
[291] RAND Europe workshop, 7 September 2020.

Encouraging organisational changes within critical infrastructure providers is also important, and could include focusing on more intensive coordination and cooperation between teams responsible for operations, security and management. Furthermore, organisations should introduce multi-disciplinary teams including experts in OT, operational technology and legal requirements in order to better secure their assets and overall operations. This is an area where the NCTV can play a supporting role by providing recommendations or workforce planning frameworks.[292]

- Developing government capability for tackling APTs through the development of a forensics function within the Dutch government. Experts suggest investigating the distribution of forensics responsibilities with regards to critical infrastructure in the Netherlands and in other countries in order to inform these decisions. This would help define responsibilities and ensure that law enforcement plays an appropriate role in tackling APTs. In particular, this would support deterrence efforts by sending the message that malicious attacks are likely to be attributed, including to state actors.[293]

[292] INT11; INT12; INT13.
[293] INT11; RAND Europe workshop, 7 September 2020.

10. Summary and conclusions

This chapter summarises the key findings and recommendations of the study and presents some overall conclusions.

10.1. This study has several key findings across the two research areas

As shown in Table 10.1, this study sought to answer a set of research questions related to each of the two topics investigated: cybersecurity governance from a national security perspective and critical information security.

Table 10.1 Overview of Phase 2 research questions

Overarching research areas	Research questions (RQs)
1. Cybersecurity governance from a national security perspective	1.1 How can the current model of governance and current cybersecurity initiatives in the Netherlands be aligned and improved?
	1.2 How can system responsibility for cybersecurity be set up?
	1.3 What lessons can be identified through international comparisons of different national cybersecurity governance models?
	1.4 How can capabilities and skills required across stakeholders and functions to ensure national cybersecurity be identified and managed?
	1.5 How could efficiency and effectiveness be measured for cybersecurity policymaking?
2. Critical infrastructure security and protection	2.1 What are the risks and challenges resulting from the interplay between legacy critical infrastructure technologies and new technologies?
	2.2 How can current levels of cybersecurity maturity within the critical infrastructure sector be measured and understood?
	2.3 What can be done to improve security of operational technology deployed in critical sectors?
	2.4 What can be done with a view to potential threats from actors and organised groups or networks of actors in order to prevent damage to the vital infrastructure?

The following sections summarise the key findings across the two research areas and their associated research questions.

10.1.1. Cybersecurity governance from a national security perspective

Governance can be understood as the approaches used by multiple stakeholders to identify, frame and coordinate the response to a collective problem. Cybersecurity governance from a national security perspective can, therefore, be seen as the approaches used by multiple stakeholders to identify, frame and coordinate proactive and reactive responses to potential national security risks that stem from the cyber domain.

Cybersecurity governance in the Netherlands

This study explored how the current model of governance and current cybersecurity initiatives in the Netherlands could be aligned and improved, and how system responsibility for cybersecurity could be set up. The study found that the governance of cybersecurity is a prominent area of discussion in the Netherlands, and that there are several ongoing initiatives exploring how the governance of cybersecurity in the Netherlands is working and how it could be improved in the future.

The current cybersecurity governance model in the Netherlands is anchored in the *Polder* model of consensus-driven decision making. In practice, this means that the Dutch governance structure is a network governance model with several organisations working to ensure national cybersecurity, whereby each organisation is responsible for cybersecurity within their mandate and area of responsibility. Within this context, this study identified a series of challenges to the current governance of cybersecurity from a national perspective in the Netherlands:

- **Unclear roles and responsibilities within the cybersecurity governance structure and a lack of agility and proactiveness in cybersecurity policy making.** The study identified that the distributed governance model may make it difficult to have clear roles and responsibilities across the entire system. The study also highlighted that there may be a mismatch of resources and efforts placed on crisis management and reactive response, rather than proactively building and improving the resilience of digital society in the Netherlands.
- **Information-sharing challenges.** Adequate and productive information-sharing is fundamental to both the prevention and response phases of addressing cybersecurity threats. This study found two information-sharing areas as potential areas for improvement: information-sharing and knowledge relating to the state of cybersecurity within the national government, and information-sharing between organisations with a cybersecurity responsibility.
- **Challenges related to a lack of or duplicated regulations and standards may add complexity within the governance system.** The current governance structure may lead to a lack of coherence in regulation, with competing or contradicting requirements that could potentially undermine efforts to strengthen cybersecurity. Within this context, more proactive and enforceable minimum cybersecurity standards may, therefore, help harmonise the cybersecurity arrangements and help address varying maturity levels across government.
- **The distinction of vital and non-vital infrastructure.** This distinction plays a pivotal role in the Dutch governance structure, in which critical infrastructure operators are subject to additional legislation and regulation, have mandatory incident-reporting requirements, and are part of the NCSC information-sharing structure. This may mean that non-critical providers and services are

subject to less stringent security requirements and may miss out on important security advice, whilst still being vital to societal resilience or national security.

- **Challenges of oversight and evaluation.** This study found that there is currently not an enforceable government-wide cybersecurity standard and each government organisation maintains its own cybersecurity arrangements. Additionally, the NCSC primarily works in an advisory capacity. This makes it challenging to enforce, evaluate and assure the cybersecurity arrangements across the various actors in the Dutch ecosystem.

The study also explored potential lessons for the Netherlands from different national cybersecurity governance models. To help answer this question, the study team developed five case-study country profiles of national governance approaches in Estonia, Germany, Sweden, the United Kingdom and the United States. However, these international case studies can only offer limited lessons for the Dutch governance system. One of the overarching challenges when comparing national governance approaches is the lack of evaluation and performance metrics of cybersecurity governance, which makes it difficult to understand how well each respective governance system is functioning. In other words, case-study analysis can illustrate how different countries have approached their governance structure but cannot fully answer what makes them work (or not work) within their national structures, or how each nation's performance compares to other approaches.

Managing cybersecurity capabilities and skills required for national security

This study also explored how to identify and manage the capabilities and skills required to ensure national cybersecurity. The Dutch government has emphasised the importance of having appropriate and sufficient depth of capabilities and skills in place to ensure a digitally secure Netherlands, particularly from a national security perspective – and several initiatives are already implemented and underway. Within this context, the study however identified three overarching challenges in relation to cybersecurity skills from a national security perspective:

- **The distributed responsibility for workforce management issues**, which may make it challenging to coordinate the cybersecurity workforce across different government organisations and agencies.
- **The lack of commonly accepted and shared language**. Within the Dutch context, there is not a single, commonly agreed and widely used taxonomy for cybersecurity skills or professions, which makes it challenging to understand the current capacity and skills in the Netherlands and how to best improve them.
- **Recruitment and retention issues**. Recruitment and retention challenges are well-known and prevalent in cybersecurity. In such a competitive labour market, government organisations may face challenges in recruiting cybersecurity professionals and ensuring access to the right skills for national security, especially in-house but also through outsourcing and partnership arrangements with the private cybersecurity industry.

This study identified several approaches and interventions that may help address the three challenges outlined above, including the use of:

- An easily accessible knowledge base to foster a shared understanding of the cybersecurity field;

- Workforce strategies to help align cybersecurity skills efforts across government;
- Competency frameworks and career paths to streamline workforce management, skills development and sustainment; and
- Training-needs analysis to help identify the required skills across functions and stakeholders from a national security perspective.

Measuring performance for cybersecurity policymaking

The study also sought to explore how the efficiency and effectiveness of national cybersecurity could be measured or evaluated to better inform policy- and decision-making. The study identified several approaches to measuring performance, including:

- Frameworks for thinking about the evidence needed for cybersecurity policymaking;
- Approaches that have previously been used for evaluation in the cyber domain; and
- Approaches from other sectors that could be used for evaluation in the cyber domain.

The various approaches presented have different uses, potential strengths and benefits and it is, therefore, useful to consider some fundamental evaluation questions when reviewing them (i.e. *why* we need to measure performance, *what* we need to measure, and *how* we should measure it). Table 10.2 presents an overview of the identified approaches and where they may add the most value.

Table 10.2 Overview of approaches to improve the measurement of cybersecurity performance and policymaking

Approach or framework	Use case and added value
Evidence model for cybersecurity policymaking	To assess and improve the evidence used for cybersecurity policymaking.
Post-incident and lessons-learned analysis	To analyse, assess and improve the response mechanisms to incidents or attacks, including the governance of cybersecurity, both within the overall system and within crisis management or incident response structures.
Self-assessments of cybersecurity maturity	To assess and help improve the cybersecurity maturity of organisations.
Programme evaluation	To evaluate the impact of specific programmes or interventions within national cybersecurity.
Performance auditing and Value for Money	To evaluate the wider performance-specific programmes or the overall national approach to cybersecurity (e.g. its economy, efficiency and effectiveness).
Exercises and games	To explore poorly understood areas of cybersecurity and develop better evidence for policymaking. To exercise, test and assess governance structures and plans, particularly in relation to incident response and crisis management.
Measuring the value of national cybersecurity	To define and measure the overall contribution and value of the national cybersecurity system.

Decision making under deep uncertainty methods	To assess and refine future polices and improvements to national cybersecurity.

10.1.2. Critical infrastructure and security

Critical infrastructure encompasses those services deemed necessary for the functioning of society (e.g. power plants, water supply systems, transport infrastructure, democratic institutions and government processes, etc.). Ensuring the security of critical processes outlined above is perceived as one of the pillars of national cybersecurity, and is also of particular concern due to its geopolitical importance. Recent trends to Internet-enable parts of critical infrastructure and the adoption of emerging technologies or solutions present new challenges linked to the cybersecurity of critical infrastructure, and have led governments to investigate how best to secure them.

Critical infrastructure and technology

In relation to critical infrastructure and technology, the study particularly explored the risks and challenges resulting from the interplay between legacy critical infrastructure technologies and new technologies. The study team found that the interplay between legacy and new technologies is well understood among Dutch experts, but that risks and challenges are not always addressed or adequately managed. These risks are linked to:

- **Liability and obsolescence** of some parts of critical assets, which risk enabling system failure or malicious exploitation. These challenges should be addressed through better understanding of the assets concerned and of the interplay between suppliers and buyers, for instance through asset management and clearly defined security agreements between suppliers and buyers.
- **The connectivity of operational technologies** and the resulting cascading effects, which increase potential platform attacks and multiply potential damage. The implementation of the NIS directive partly addresses this risk through the identification of essential providers who are dependent on ICT, but it is necessary to better map the risks linked to cascading effects.
- **The gap between OT and IT** remains an obstacle to tackling already identified risks. As this interplay increases, so does the urgency of bridging this gap through education, awareness, trainings and cooperation between experts of IT and of operational technologies.

Critical infrastructure and cybersecurity maturity

The study further explored how current levels of cybersecurity maturity within the critical infrastructure sector could be measured and understood. The study identified several approaches and models that are used to assess cybersecurity maturity in critical infrastructure. A maturity model can be understood as a benchmark for organisations to assess their capability in a given field against a set of indicators. These establish a baseline for consistent evaluation and allow organisations to set goals and priorities for improvement, based on their maturity level.

However, the study also identified several challenges linked to measuring cybersecurity:

- **Existing models for measuring maturity in the critical infrastructure sector come with several challenges**, including the difficulty in defining useful and measurable indicators and the constant evolution of the cybersecurity field, which requires constant actualisation of standards and models.
- **The tension between measuring maturity at a general level and measuring it at the sectorial level** was underlined as a trade-off between general applicability and further precision. Experts suggested the government should provide sectorial recommendations and guidelines on this issue.
- **The debate about the benefits of adopting a regulatory approach to cybersecurity maturity and of relying on a cooperative approach** suggests there may be a risk that measuring cybersecurity maturity becomes a 'checklist exercise'. Understanding the motivation behind assessments and the benefits linked to regulation was therefore identified as an area for further research.
- **Including supply-chain risks and interdependencies in maturity assessments** emerged as essential to accurate measurement of cybersecurity maturity and to a better and more comprehensive understanding of risks.

Critical infrastructure and improving cybersecurity

Lastly, the study explored what can be done to improve security of operational technology deployed in critical sectors and to protect against potential threats from actors and organised groups or networks of actors. Improving the security of operation technology in critical sectors relies on addressing the cybersecurity triangle of people, processes and technologies, and is linked to challenges discussed under previous research questions. The study identified the following essential areas of action for improving the security of operational technology:

- **Critical infrastructure security should rely on an integrated and multi-faceted approach**, considering assets as well as their environment. Such an approach may benefit from future technological developments such as supply-chain management that relies on hash-chain or cryptographic audit logs, zero-trust architecture, inventory management that uses automated processes and AI, and self-healing.
- **Cross-sectorial information-sharing emerged as crucial to improving the security of Dutch critical infrastructure**. This was identified as an area where the government could play a role of coordinator to help overcome challenges linked to trust and confidentiality.
- **Changes in organisation structures**, especially towards multi-disciplinary teams and better coordination between operations, security, management and legal teams, would both help improve security and gain a better understanding of existing risks.

This study found little evidence available on the protection of critical infrastructure from the angle of existing threats from actors and organised groups. Consultations with experts, however, did provide valuable insights on the issue:

- **The current priority should be on tackling immediate threats**, which may be less disruptive than APTs but are more common due to current low maturity levels of several critical infrastructure providers.

- **Providing a clear definition of roles and responsibilities between the government and private sector** appeared as necessary to ensure prevention against APTs and better reaction and investigation of such attacks.
- **This question was identified as a geopolitical issue, which therefore requires a geopolitical approach from the government**, including by relying on international cooperation to identify and tackle external threats.

10.2. This study offers the NCTV a set of recommendations to help improve cybersecurity in the Netherlands

As highlighted in the final report for Phase 1 of this state-of-the-art study, the field of cybersecurity suffers from its complexity, poor definition and inadequate or missing data and methods to perform research. From a policy perspective, these challenges translate into potential risks for society. This second phase of the study has also demonstrated that the two themes investigated – cybersecurity governance from a national security perspective and critical information security – face similar challenges that are critical to national cybersecurity in the Netherlands. First, a lack of information-sharing was identified as a key obstacle to effective governance of cybersecurity, as well as to ensuring and improving the security of critical infrastructure. Second, challenges of oversight and evaluation affecting the governance of cybersecurity also emerged as problematic in measuring the cybersecurity of critical infrastructure. Third, the distinction between critical and non-critical infrastructure, sectors and processes emerged as potentially ill-suited to the cybersecurity ecosystem, including existing interdependencies between and across sectors, processes and infrastructure as well as measures to assess and implement security requirements. Finally, while skills gaps and workforce challenges are not new, this study identified these issues as remaining key obstacles to securing critical infrastructure and ensuring effective governance of cybersecurity, and therefore to overall digital resilience at the national level.

In order to address the overarching challenges identified, this study identified a set of priority recommendations for the NCTV to consider:

1. Further explore and examine the distinction between critical and non-critical infrastructure within the Dutch governance model.
2. Further investigate and invest in proactive approaches to national cybersecurity.
3. Further explore the role of minimum security standards and potential needs for further authority to ensure compliance.
4. Invest in skills development to bridge the OT–IT gap and develop synergies between academia, industry, regulators and the government.
5. Develop tools to understand and address risks linked to the critical infrastructure supply-chain, both nationally and across international borders.

In addition to these recommendations, this second phase of the study also identified additional areas requiring the attention of the NCTV. Some of these areas are already the subject of existing efforts to develop new capability. In these cases, the NCTV should seek to:

- Continue its work with the Ministry of Education and other responsible ministries to address challenges related to skills gaps, training requirement and workforce management.
- Continue working with *CIO RIJK* and *CISO Rijk* to develop a comprehensive overview and understanding of the state of cybersecurity within the national government.
- Continue working with the Ministry of the Interior and Kingdom Relations and other relevant stakeholders to assist in ongoing efforts to harmonise cybersecurity legislation and regulation in the Netherlands.

On the other hand, additional recommendations also focused on areas where there is little to no existing effort. In particular, the NCT should adopt a leading role in:

- Developing the evidence base on cybersecurity maturity models;
- Developing the evidence base on current approaches to cybersecurity regulations in critical infrastructure; and
- Developing government capability for tackling APTs.

Beyond this state-of-the-art study, there are several ongoing efforts being carried out simultaneously to further develop the necessary evidence for the Netherlands' cybersecurity, and to address these risks. Challenges and recommendations identified in this study should therefore be considered alongside results of other past and ongoing research efforts. As mentioned in the Phase 1 report, some of these challenges may be addressed by additional research, while others may perhaps be better addressed outside a research agenda.[294] It may be the case that there is an understanding of what needs to be done, but perhaps not the political will, funding or operational ability to adequately implement these measures. These issues nevertheless warrant the attention of the NCTV. Similarly, areas where existing efforts are already underway may still require or benefit from the support of the NCTV.

[294] Silfversten et al. (2019).

References

Adams, Samantha A., Marlou Brokx, Lorenzo Dalla Corte, Masa Galic, Kaspar Kala, Bert-Jaap Koops, Ronald Leenes, Maurice Schellekens, Karine e Silva and Ivan Skorvanek. 2015. 'The Governance of Cybersecurity: A comparative quick scan of approaches in Canada, Estonia, Germany, the Netherlands, and the UK.' *Tillburg University.* As of 13 October 2020: https://www.wodc.nl/binaries/2484-volledige-tekst_tcm28-73672.pdf

Alcaraz, Cristina and Sherali Zeadally. 2014. 'Critical infrastructure protection: Requirements and challenges for the 21st century.' *International Journal of Critical Infrastructure Protection* 8, 53–66.

Algemene Rekenkamer. 2019. 'Strengthening the digital defences: the cyber security and critical water structures.' Rekenkamer.nl. As of 13 October 2020: https://english.rekenkamer.nl/publications/reports/2019/03/28/strengthening-the-digital-defences-the-cyber-security-of-critical-water-structures

Ani, Uchenna P. Daniel, Hongmei (Mary) He & Ashutosh Tiwari. 2017. 'Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective.' *Journal of Cyber Security Technology* 1:1, 32–74. As of 16 October 2020: https://doi.org/10.1080/23742917.2016.1252211

Assante, Michael J. and Robert M. Lee. 2015. 'The Industrial Control System Cyber Kill Chain.' SANS Institute: Information Security Reading Room. As of 18 November 2020: https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297

Association of Netherlands Municipalities (VNG). 2018. 'Local Government in the Netherlands.' VNG. As of 13 October 2020: https://www.publieksdiensten.nl/wp-content/uploads/2018/04/DENMARK-4-Local-Government-in-the-Netherlands.pdf

Barnett, Chris, Julian Barr, Angela Christie, Belinda Duff and Shaun Hext. 2010. 'Measuring the Impact and Value for Money of Governance & Conflict Programmes.' ITAD. As of 13 October 2020: https://assets.publishing.service.gov.uk/media/57a08b1eed915d3cfd000b44/60797_ITAD-VFM-Report-Dec10.pdf

Bayerische Staatskanzlei. 2015. 'Law on electronic administration in Bavaria.' 22 December 2015. As of 10 October 2020: https://www.gesetze-bayern.de/Content/Document/BayEGovG-10

Bobowska, B., M. Choras & M. Wozniak. 2018. 'Advanced Analysis of Data Streams for Critical Infrastructures Protection and Cybersecurity.' *Journal of Universal Computer Science* 24(5): 622–33.

Boeke, Sergei. 2016. 'First Responder or Last Resort? The role of the Ministry of Defence in national cyber crisis management in four European countries.' Universiteit Leiden. As of 13 October 2020: https://openaccess.leidenuniv.nl/bitstream/handle/1887/46615/Boeke%28September2016%29FirstRespondersorLastResort.pdf?sequence=1

———. 2017. 'National cyber crisis management: Different European approaches.' *Governance* 31(3): 449–464. As of 13 October 2020: https://onlinelibrary.wiley.com/doi/full/10.1111/gove.12309

Boyson, Sandor. 2014. 'Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems.' *Technovation* 34, 342–353.

Bundesamt für Sicherheit in der Informationstechnik (BSI). N.d. 'Cyber Defence Center.' BSI.bund.de. As of 10 October 2020: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/Cyber-Abwehrzentrum/cyberabwehrzentrum_node.html

Bundesminister des Innern. N.d. [Homepage]. BMI.bund.de. As of 10 October 2020: https://www.bmi.bund.de/DE/startseite/startseite-node.html

———. 2005. 'National Plan for the Protection of Information Infrastructures.' As of 10 October 2020: https://www.bsi-fuer-buerger.de/SharedDocs/Downloads/EN/BSI/Kritis/National_Plan_for_Information_Infrastructure_Protection.pdf?__blob=publicationFile

———. 2011. 'Cyber Security Strategy for Germany.' As of 10 October 2020: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany/@@download_version/bca1e34aca9b411eb3d382b5d220482a/file_en

———. 2016. 'Cyber Security Strategy for Germany.' As of 10 October 2020: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany/@@download_version/8adc42e23e194488b2981ce41d9de93e/file_native

Bundesnachrichtendienst. N.d. [Homepage]. As of 10 October 2020: https://www.bnd.bund.de/EN/Home/home_node.html

Bundestag. 1990. 'BSI-Errichtungsgesetz.' Bgbl.de, 17 December 1990. As of 10 October 2020: https://www.bgbl.de/xaver/bgbl/start.xav?start=%2F%2F*%5B%40attr_id%3D%27bgbl190s2834.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl190s2834.pdf%27%5D__1594656311572

———. 2009. 'Act on the Federal Office for Information Security.' As of 10 October 2020: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/BSI/BSI_Act_BSIG.pdf?__blob=publicationFile&v=4

———. 2015. 'IT-Sicherheitsgesetz.' Bgbl.de, 24 July 2015. As of 10 October 2020: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*%255B@attr_id=%27bgbl115s1324.pdf%27%255D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s1324.pdf%27%5D__1593012627909

Bundeswehr. N.d. 'Das Zentrum Cyber-Operationen.' Bundeswehr.de. As of 10 October 2020: https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-strategische-aufklaerung/das-zentrum-cyber-operationen

Cabinet Office. 2009. 'Cyber Security Strategy of the United Kingdom: safety, security, and resilience in cyber space.' Cabinet Office. As of 20 October 2020: https://www.gov.uk/government/publications/cyber-security-strategy-of-the-united-kingdom

Calder, J. 2013. *Programme Evaluation and Quality: A Comprehensive Guide to Setting Up an Evaluation System*. Routledge.

Center for Cyber and Homeland Security. 2019. 'Strengthening Defense Mission Assurance Against Emerging Threats.' Center for Cyber and Homeland Security.

Ceron, J.M., J.J. Chromik, J.J.C. Santanna and A. Pras. 2019. 'Online Discoverability and Vulnerabilities of the ICS/SCADA Devices in the Netherlands.' University of Twente.

Chappelle, Wayne, Kent McDonalds, James Christensen, Lilian Prince, Tanya Goodman, William Thompson and William Hayes. 2013. 'Sources of Occupational Stress and Prevalence of Burnout and Clinical Distress among US Air Force Cyber Warfare Operators.' School of Aerospace Medicine Wright Patterson AFB Ohio. As of 13 October 2020: https://apps.dtic.mil/dtic/tr/fulltext/u2/a584653.pdf

Chromik, Justyna. 2020. 'Exposed, Vulnerable, and (Safety) Critical. Now What?' Applied Risk. As of 13 October 2020: https://applied-risk.com/resources/discoverability-ot-systems-exposure

Cilluffo, Frank J. 2020. 'Testimony of Frank J. Cilluffo, Before the United States Senate Committee on Banking, Housing, and Urban Affairs.' Auburn University McCrary Institute for Cyber and Critical Infrastructure Security.

Cimpanu, Catalin. 2020. 'A hacker is patching Citrix servers to maintain exclusive access.' Zero Day. As of 20 October 2020: https://www.zdnet.com/article/a-hacker-is-patching-citrix-servers-to-maintain-exclusive-access/

Claver, Alexander. 2018. 'Governance of cyber warfare in the Netherlands: an exploratory investigation.' *The International Journal of Intelligence, Security, and Public Affairs*, 20(2), 155–180. As of 13 October 2020: https://www.tandfonline.com/doi/full/10.1080/23800992.2018.1484235

Congressional Research Service (CRS). 2018. 'DHS's Cybersecurity mission: An overview.' As of 16 June 2020: https://fas.org/sgp/crs/homesec/IF10683.pdf

Cyber Security and Infrastructure Security Agency (CISA). 2014. 'Federal Information Security Modernization Act.' As of 20 October 2020: https://www.cisa.gov/federal-information-security-modernization-act

———. 2020a. [Homepage]. As of 16 June 2020: https://www.cisa.gov/

———. 2020b. 'National Risk Management Center (NRMC).' As of 16 June 2020: https://www.cisa.gov/national-risk-management

———. 2020c. 'National Cybersecurity Protection System.' As of 16 June 2020: https://www.cisa.gov/national-cybersecurity-protection-system-ncps

Cyber Security Council – Cyber Security Raad (CSR). 2020. 'Recommendation on the digital security of Industrial Automation & Control Systems (IACS) in the critical national infrastructure of the Netherlands.' CSR.

Cyber Seek. N.d.a. [Homepage]. Cyberseek.org. As of 13 October 2020: https://www.cyberseek.org/

———. N.d.b. 'Cybersecurity Supply/Demand Heat Map.' Cyberseek.org/heatmap. As of 13 October 2020: https://www.cyberseek.org/heatmap.html

———. N.d.c. 'Cybersecurity Career Pathway.' Cyberseek.org/pathway. As of 13 October 2020: https://www.cyberseek.org/pathway.html

CyBOK. N.d. [Homepage]. Cybok.org. As of 13 October 2020: https://www.cybok.org/

Dcypher. N.d. [Homepage]. Dcypher.nl. As of 13 October 2020: https://www.dcypher.nl/en

Department for Business, Innovation & Skills (BIS), David Cameron and Mark Prisk. 2011. 'Protecting and promoting the UK in a digital world.' Gov.uk. As of 20 October 2020: https://www.gov.uk/government/news/protecting-and-promoting-the-uk-in-a-digital-world--2

Department of Energy. 2014. 'Cybersecurity Capability Maturity Model (C2M2). Version 1.1.' As of 19 October 2020: https://www.energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf

Department of Homeland Security. 2014. 'Cybersecurity Capability Maturity Model White Paper. Version 1.0.' As of 19 October 2020: https://www.hsdl.org/?abstract&did=798503

Dutch Research Council (NWO). 2020. 'Dutch Research Agenda – Theme: Cybersecurity – Towards a secure and trustful digital domain.' NWO. As of 13 October 2020: https://www.nwo.nl/en/funding/our-funding-instruments/nwa/dutch-research-agenda---cybersecurity/dutch-research-agenda---cybersecurity.html

Dutch Safety Board. N.d.a. 'Dutch Safety Board.' Onderzoeksraad.nl. As of 13 October 2020: https://www.onderzoeksraad.nl/en/page/12263/dutch-safety-board

———. N.d.b. 'Security leak Citrix.' Onderzoeksraad.nl. As of 13 October 2020: https://www.onderzoeksraad.nl/en/page/17171/security-leak-citrix

———. 2012. 'The DigiNotar incident.' Onderzoeksraad.nl. As of 13 October 2020: https://www.onderzoeksraad.nl/en/page/1730/the-diginotar-incident

Estonian Centre of Registers and Information Systems. 2020. [Homepage]. As of 10 October 2020: https://www.rik.ee/en

Estonian Data Protection Inspectorate. 2020. [Homepage]. As of 10 October 2020: https://www.aki.ee/en

Estonian Defence League. 2020. 'Estonian Defence League's Cyber Unit.' As of 10 October 2020: https://www.kaitseliit.ee/en/cyber-unit

Estonian Information System Authority. 2020. 'Cyber Security in Estonia 2020.' As of 10 October 2020: https://www.ria.ee/sites/default/files/content-editors/RIA/cyber_security_in_estonia_2020_0.pdf

Estonian Internal Security Service. 2020. [Homepage]. As of 10 October 2020: https://www.kapo.ee/

Estonian Minister of Economic Affairs and Communication. 2011. 'Statutes of the Information System Authority.' As of 10 October 2020: https://www.ria.ee/sites/default/files/content-editors/RIA/statutes_of_the_information_system_authority.docx

Estonian Ministry of Defence. 2008. 'Cyber Security Strategy.' As of 10 October 2020: https://www.valitsus.ee/sites/default/files/content-editors/arengukavad/kuberjulgeoleku_strateegia_2008-2013.pdf

———. 2018. 'Statutes of the Cyber Command.' As of 10 October 2020: https://mil.ee/wp-content/uploads/2020/01/K%C3%BCberv%C3%A4ejuhatuse-p%C3%B5him%C3%A4%C3%A4rus.pdf

———. 2020. 'Cyber Command.' As of 10 October 2020: https://mil.ee/en/landforces/cyber-command/#t-cyber-and-information-operations-center

Estonian Ministry of Economic Affairs and Communication. 2014. '2014-2017 Cyber Security Strategy.' As of 10 October 2020: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf

———. 2018. '2019-2022 Cybersecurity Strategy.' As of 10 October 2020: https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

European Centre for the Development of Vocational Training. 2016. 'Skill Shortage and Surplus Occupations in Europe.' As of 16 October 2020: https://ec.europa.eu/epale/sites/epale/files/skill_shortage_and_surplus_occupations_in_europe.pdf

European Commission. 2019. 'Migration and Home Affairs: Critical infrastructure.' As of 13 October 2020: https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/criticalinfrastructure_en

———. 2020. 'Digital Competence Framework for citizens.' Ec.europa.eu. As of 16 October 2020: https://ec.europa.eu/jrc/en/digcomp

European e-Competence Framework. N.d. 'The what, how and why guide to the e-CF.' As of 18 November 2020: https://www.ecompetences.eu/

European Parliament and the Council of the EU. 2016. 'Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union.' As of 10 October 2020: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148

European Union Agency for Network and Information Security (ENISA). 2014. 'Smart grid security certification in Europe.' ENISA.

———. 2015. 'Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors.' ENISA.

———. 2019. 'ENISA Maturity Evaluation Methodology for CSIRTs.' ENISA.

Evaluating Cyber Security Evidence for Policy Advice (ECSEPA). N.d. [Homepage]. Ecsepa.coventry.ac.uk. As of 13 October 2020: http://ecsepa.coventry.ac.uk/

Executive Office of the President. 2016. 'Memorandum for Heads of Executive Departments and Agencies.' Whitehouse.gov. As of 13 October 2020: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-15.pdf

Federal Ministry of Justice and Consumer Protection. 1990. 'German Federal Constitutional Protection Act.' As of 10 October 2020: https://www.gesetze-im-internet.de/bverfschg/BJNR029700990.html#:~:text=der%20Web%2DSite-,Gesetz%20%C3%BCber%20die%20Zusammenarbeit%20des%20Bundes%20und%20der%20L%C3%A4nder%20in,f%C3%BCr%20Verfassungsschutz%20(Bundesverfassungsschutzgesetz%20%2D%20BVerfSchG)

———. 2005. 'Law on Parliamentary Participation in the Decision on the Use of Armed Forces Abroad. 2005.' As of 10 October 2020: https://www.gesetze-im-internet.de/parlbg/BJNR077500005.html

———. 2017. 'Section 4 (1) 5 of the 2017 Federal Criminal Police Act.' As of 10 October 2020: https://www.gesetze-im-internet.de/bkag_2018/BJNR135410017.html

———. 2019. 'Basic Law for the Federal Republic of Germany as last amended by Article 1 of the Act of 28 March 2019.' As of 10 October 2020: http://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html#p0451

FragDenStaat. 2016. 'Cooperation Agreements on the National Cyber Defence Center.' Fragdenstaat.de, 8 June 2016. As of 10 October 2020: https://fragdenstaat.de/anfrage/kooperationsvereinbarungen-zum-nationalen-cyber-abwehrzentrum/

Fraunhofer CIPedia. N.d. 'Operator of Essential Services.' As of 13 November 2020: https://websites.fraunhofer.de/CIPedia/index.php/Operator_of_Essential_Services

Fox, J., van den Brink, P. and van Schie, T. 2019. 'Success factors for digitally safe Operational Technology.' TNO.

Gartner. 2019. 'Cyber Security for Industrial Automation and Control Systems – A report for the Ministry of Justice and Safety.' Gartner.

German Federal Criminal Police Office. 'Our mandate.' Bka.de. As of 10 October 2020: https://www.bka.de/EN/TheBKA/OurMandate/ourmandate_node.html

German Federal Ministry of Defence. N.d. 'CyberSecurity Council.' Bmvg.de. As of 10 October 2020: https://www.bmvg.de/de/themen/cybersicherheit/partnerschaften-zur-cybersicherheit/cyber-sicherheitsrat

———. 2018. 'Die Konzeption der Bundeswehr Ausgewählte Grundlinien der Gesamtkonzeption.' April 2018. As of 10 October 2020: https://www.bmvg.de/resource/blob/26546/befaf450b146faa515e19328e659fa1e/20180731-broschuere-konzeption-der-bundeswehr-data.pdf

Government of Republic of Estonia. 2018. 'Statutes of the Defence Forces.' As of 10 October 2020: https://www.riigiteataja.ee/akt/128062018008

Government of Sweden. 2018. 'Kompletteringar till den nya säkerhetsskyddslagen.' As of 20 October 2020: https://www.regeringen.se/48d97d/contentassets/b152429991334d788c59a12d8d10d0f3/sammanfattning-pa-svenska-och-engelska-av-sou-2018-82.pdf

Haasnoot, Marjolijn, Jan H. Kwakkel, Warren E. Walker and Judith ter Maat. 2013. 'Dynamic adaptive policy pathways: A method for crafting robust decisions for a deeply uncertain world.' *Global Environmental Change* 23(2), 485–498.

Haber, Eldar and Tal Zarsky. 2017. 'Cybersecurity for Infrastructure: A Critical Analysis.' Florida State University Law Review 44(2). As of 16 October 2020: https://ir.law.fsu.edu/lr/vol44/iss2/3

Hannigan, Robert. 2019. 'Organising a Government for Cyber: The Creation of the UK's National Cyber Security Centre.' Royal United Services Institute for Defence and Security Studies (RUSI). As of 20 October 2020: https://rusi.org/sites/default/files/20190227_hannigan_final_web.pdf

Hathaway, Melissa and Francesca Spidalieri. 2017. 'The Netherlands Cyber Readiness at a Glance.' Potomac Institute for Policy Studies. As of 13 October 2020: https://www.potomacinstitute.org/images/CRI/FinalCRI20NetherlandsWeb.pdf

Helderman, Jan-Kees, Gwen Bevan and George France. 2012. 'The rise of the regulatory state in healthcare: a comparative analysis of the Netherlands, England, and Italy.' *Health Economics, Policy, and Law* 7: 103–124.

Herpig, Sven & Clara Bredenbrock. 2019. 'Cybersicherheitspolitik in Deutschland.' Stiftung Neue Verantwortung, April 2019. As of 10 October 2020: https://www.stiftung-nv.de/sites/default/files/cybersicherheitspolitik_in_deutschland.pdf

Herpig, Sven and Beigel, Rebecca. 2020. 'Akteure und Zuständigkeiten in der deutschen Cybersicherheitspolitik.' As of 10 October 2020: https://www.stiftung-nv.de/sites/default/files/snv_papier_cybersicherheitsarchitektur_final.pdf

HM Government. 2016. 'National Cyber Security Strategy 2016–2021.' HM Government. As of 20 October 2020: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

HM Treasury. 2019. 'The Public Value Framework: with supplementary guidance.' As of 13 October 2020: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785553/public_value_framework_and_supplementary_guidance_web.pdf

House of Commons Committee of Public Accounts. 2019. 'Cyber Security in the UK: Ninety-Ninth Report of Session 2017–19.' As of 20 October 2020: https://publications.parliament.uk/pa/cm201719/cmselect/cmpubacc/1745/1745.pdf

Hussain, Atif, Siraj Ahmed Shaikh, Alex Chung, Sneha Dawd, and Madeline Carr. 2018. 'An Evidence Quality Assessment Model for Cybersecurity Policymaking.' As of 13 October 2020: https://discovery.ucl.ac.uk/id/eprint/10052318/1/EQAM.pdf

Information Commissioner's Office (ICO). 2020. 'The role of the National Cyber Security Centre (NCSC).' ICO. As of 20 October 2020: https://ico.org.uk/for-organisations/the-guide-to-nis/the-role-of-the-national-cyber-security-centre-ncsc/

Information System Authority. 2020. 'RFC 2350 Description for CERT-EE.' As of 10 October 2020: https://www.ria.ee/sites/default/files/content-editors/kuberturve/rfc_2350_description_for_cert.pdf

Innenminister Konferenz. N.d. 'Permanent conference of the interior ministers and senators of the countries: Tasks and working methods.' Innenministerkonferenz. As of 10 October 2020: https://www.innenministerkonferenz.de/IMK/DE/aufgaben/aufgaben-node.html

Julnes, George. 2019. 'Supporting Transitions to Sustainability: Evaluation for Managing Processes in the Public Interest.' *New Directions for Evaluation* 162. As of 13 October 2020: https://onlinelibrary.wiley.com/doi/full/10.1002/ev.20366

Kick, Jason. 2014. 'Cyber Exercise Playbook.' MITRE Corporation. As of 13 October 2020: https://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf

Knowles, William, Daniel Prince, David Hutchinson, Jules Ferdinand Pagna Disso and Kevin Jones. 2015. 'A Survey of cyber security management in industrial control systems.' *International Journal of Critical Infrastructure Protection* 9, 52–80.

Landesamt für Sicherheit in der Informationstechnik. N.d. [*Homepage*]. As of 12 October 2020: https://www.lsi.bayern.de/lsi/index.html

Lempert, Robert J., Steven W. Pooper and Steven C. Bankes. 2003. 'Shaping the Next One Hundred Years: New Methods for Quantitative, Long-Term Policy Analysis.' RAND Corporation. As of 13 October 2020: https://www.rand.org/pubs/monograph_reports/MR1626.html

Ling, Tom and Lidia Villalba van Dijk. 2009. 'Performance Audit Handbook.' RAND Corporation. As of 13 October 2020: https://www.rand.org/pubs/technical_reports/TR788.html

Local Government Association. N.d. 'Cyber Security Self Assessment tool.' Local.gov.uk. As of 13 October 2020: https://www.local.gov.uk/our-support/efficiency-and-income-generation/cyber-security/cyber-security-self-assessment-tool

Luiijf, E., H. Burger & M. Klaver. 2003. 'Bescherming Vitale Infrastructuu: Quick-scan naar vitale producten en diensten.' TNO rapport FEL-03-C001, 2003.

Luiijf, Eric and Allard Kernkamp. 2015. 'Sharing Cyber Security Information: Good Practice Stemming from the Dutch Public-Private-Participation Approach.' Global Conference on Cyber Space (GCCS) 2015.

Luiijf, Eric, Tom van Schie and Theo van Ruijven. 2017. 'Companion Document to the GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers.' Global Forum on Cyber Expertiese (GFCE).

Lyon, Vivian. 2020. 'Exploring Strategies for Recruiting and Retaining Cybersecurity Professionals.' *Walden University: Walden Dissertations and Doctoral Studies.* As of 13 October 2020: https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=9579&context=dissertations

Marchau, Vincent A. W. J., Warren E. Walker, Pieter J. T. M. Bloemen and Steven W. Pooper. 2019. 'Introduction.' In *Decision Making under Deep Uncertainty,* edited by Marchau, Vincent A. W. J., Warren E. Walker, Pieter J. T. M. Bloemen and Steven W. Pooper. Springer, Cham. As of 13 October 2020: https://link.springer.com/chapter/10.1007/978-3-030-05252-2_1

Martin, Andrew, Awais Rashid, Howard Chivers, George Danezis, Steve Schneider and Emil Lupu. 2019. 'Introduction to CyBOK Issue 1.0.' The National Cyber Security Centre. As of 20 October 2020: https://www.cybok.org/media/downloads/Introduction_to_CyBOK.pdf

McPhee, Ian. 2006. 'Evaluation and Performance Audit: Close cousins – or distant relatives?' Canberra Evaluation Forum. As of 13 October 2020: https://www.anao.gov.au/sites/default/files/McPhee_evaluation_and_performance_audit_2006.pdf

Mikolic-Torreira, Igor, Ryan Henry, Don Snyder, Sina Beaghley, Stacie L. Pettyjohn, Sarah Harting, Emma Westerman, David A. Shlapak, Megan Bishop, Jenny Oberholtzer, Lauren Skrabala and Cortney Weinbaum. 2016. 'A Framework for Exploring Cybersecurity Policy Options.' RAND Corporation. As of 13 October 2020: https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1700/RAND_RR1700.pdf

Ministry of Economic Affairs and Climate Policy. 2018. 'Digital Trust Center (DTC).' Ministry of Economic Affairs and Climate Policy. As of 13 October 2020: https://www.digitaltrustcenter.nl/sites/default/files/2019-12/Factsheet%20DTC%20English%20version.pdf

Ministry of Economic Affairs and Communication. 2020. [Homepage]. As of 18 June 2020: https://mkm.ee/en

Ministry of Justice and Security. 2019. 'National Security Strategy.' NCTV. As of 13 October 2020: https://english.nctv.nl/binaries/nctv-en/documents/publications/2019/09/19/national-security-strategy/National+Security+Strategy_2019.pdf

Ministerie van Justitie en Veiligheid. 2018. 'Staatsblad van het Koninkrijk der Nederlanden.' As of 13 November 2020: https://zoek.officielebekendmakingen.nl/stb-2018-388.html

Miron, Walter and Kevin Muita. 2014. 'Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure.' *Technology Innovation Management Review*. As of 18 November 2020: https://timreview.ca/sites/default/files/article_PDF/MironMuita_TIMReview_October2014.pdf

National Archives. N.d. 'Open Government Licence for public sector information.' As of 18 November 2020: http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/

National Audit Office (NAO). N.d.a. 'Assessing value for money.' nao.org.uk. As of 13 October 2020: https://www.nao.org.uk/successful-commissioning/general-principles/value-for-money/assessing-value-for-money/

———. N.d.b. 'Successful commissioning.' Nao.org.uk. As of 20 October 2020: https://www.nao.org.uk/successful-commissioning/wp-content/uploads/sites/4/2013/02/commission_flow_chart_large-1.jpg

———. 2013. 'Evaluation in government.' NAO. As of 13 October 2020: https://www.nao.org.uk/wp-content/uploads/2013/12/10331-001-Evaluation-in-government_NEW.pdf

———. 2019. 'Progress of the 2016–2021 National Cyber Security Programme.' As of 20 October 2020: https://www.nao.org.uk/wp-content/uploads/2019/03/Progress-of-the-2016-2021-National-Cyber-Security-Programme-Summary.pdf

National Coordinator for Security and Counterterrorism – Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). N.d.a1 'Critical Infrastructure (protection).' Nctv.nl. As of 13 October 2020: https://english.nctv.nl/topics/critical-infrastructure-protection

———. N.d.b. 'Overzicht vitale processen.' Nctv.nl. As of 13 October 2020: https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen

———. 2020. 'Nationaal Crisisplan Digitaal.' NCTV. As of 13 October 2020: https://www.rijksoverheid.nl/documenten/rapporten/2020/02/21/tk-bijlage-1-nationaal-crisisplan-digitaal

National Cybersecurity and Communications Integration Center. 2020. [Homepage]. As of 16 June 2020: https://www.us-cert.gov/nccic

National Cyber Security Centre Netherlands (NCSC-NL). N.d. 'Wbni-melding.' Ncsc.nl. As of 13 October 2020: https://www.ncsc.nl/contact/wbni-melding-doen

———. 2018. 'National Cybersecurity Agenda.' NCSC-NL. As of 13 October 2020: https://english.ncsc.nl/topics/national-cybersecurity-agenda/documents/publications/2019/juni/01/national-cyber-security-agenda

———. 2019a. 'Operational Framework NCSC-NL.' NCSC-NL. As of 13 October 2020: https://english.ncsc.nl/publications/publications/2019/juli/02/operational-framework-and-rfc2350

———. 2019b. 'NCSRA III.' NCSC-NL. As of 13 October 2020: https://english.ncsc.nl/research/publications/publications/2019/juli/1/ncsra-iii

———. 2020. 'UPDATE: Schakel Citrix-systemen uit waar dat kan of tref aanvullende maatregelen.' NCSC-NL. As of 20 October 2020: https://www.ncsc.nl/actueel/nieuws/2020/januari/16/door-citrix-geadviseerde-mitigerende-maatregelen-niet-altijd-effectief

National Cyber Security Centre (NCSC-UK). N.d.a. 'What we do.' Ncsc.gov.uk. As of 20 October 2020: https://www.ncsc.gov.uk/section/about-ncsc/what-we-do

———. N.d.b. 'Products & Services.' Ncsc.gov.uk. As of 20 October 2020: https://www.ncsc.gov.uk/section/products-services/Introduction

———. N.d.c. 'CiSP.' Ncsc.gov.uk. As of 20 October 2020: https://www.ncsc.gov.uk/section/keep-up-to-date/cisp

———. N.d.d. 'Active Cyber Defence (ACD).' Ncsc.gov.uk. As of 20 October 2020: https://www.ncsc.gov.uk/section/products-services/active-cyber-defence

———. 2019. 'Active Cyber Defence (ACD) – The Second Year.' As of 20 October 2020: https://www.ncsc.gov.uk/report/active-cyber-defence-report-2019

National Institute of Standards and Technology (NIST). N.d.a. 'NICE Framework Resource Center: Current Version.' Nist.gov. As of 13 October 2020: https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/current-version

———. N.d.b. 'NICE Framework Resource Center: About.' Nist.gov. As of 18 November 2020: https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/about

———. 2017. 'National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework: NIST Special Publication 800-181.' NIST. As of 13 October 2020: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

———. 2020. 'NICE Presentation.' NIST. As of 13 October 2020: https://www.nist.gov/document/niceframework101ppt-presentationstandardpptx

Nederland Digital. 2019. 'Dutch Digitalisation Strategy. Getting the Netherlands ready for the digital future.' As of 16 October 2020: https://www.nederlanddigitaal.nl/binaries/nederlanddigitaal-nl/documenten/publicaties/2019/09/30/english-version-of-the-dutch-digitalisation-strategy/Nederlandse_Digitaliseringsstrategie_ENG.pdf

Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO). 2019. 'Succesfactoren van het inbedden van Operationele Technologie Security.' Tno.nl. As of 13 October 2020: https://www.tno.nl/nl/over-tno/nieuws/2019/11/operationele-technologie-security-rapport/

Netherlands Scientific Council for Government Policy (WRR). 2019. 'Voorbereiden op digitale ontwrichting.' WRR. As of 13 October 2020: https://www.wrr.nl/publicaties/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting

Organisation for Economic Development (OECD). 2010. 'Glossary of Key Terms in Evaluation and Results Based Management.' OECD. As of 13 October 2020: http://www.oecd.org/development/evaluation/2754804.pdf

———. 2018. 'Review of Digital Transformation: Going Digital in Sweden.' As of 20 October 2020: https://www.oecd-ilibrary.org/docserver/9789264302259-6-en.pdf

Pardee RAND Graduate School. N.d. 'Our Focus: Analytic Games We Create.' Prgs.edu. As of 13 October 2020: https://www.prgs.edu/research/methods-centers/gaming/about.html

Parlementaire Monitor. 2020. 'Inbreng verslag schriftelijk overleg over o.a. overzicht op hoofdlijnen Citrix-kwetsbaarheden (26643-660) - Informatie- en communicatietechnologie (ICT).' As of 3 October 2020: https://www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vl7wn7izyzym

Parliament of Estonia. 2000. 'Security Authorities Act.' As of 10 October 2020: https://www.riigiteataja.ee/en/eli/ee/514112013020/consolide

———. 2013. 'Estonian Defence League Act.' As of 10 October 2020: https://www.riigiteataja.ee/en/eli/525112013006

———. 2018. 'Cybersecurity Act.' As of 10 October 2020: https://www.riigiteataja.ee/en/eli/523052018003/consolide

Paulsen, Celia. 2020. 'The Future of IT Operational Technology Supply Chains.' IEEE Computer Society.

Pernik, Piret. 2018. 'Preparing for Cyber Conflict Case Studies of Cyber Command.' As of 10 October 2020: https://icds.ee/wp-content/uploads/2018/12/ICDS_Report_Preparing_for_Cyber_Conflict_Piret_Pernik_December_2018-1.pdf

Radvanovsky, Robert. 2018. 'Critical Infrastructure Security Paradigm and Modern Protection Policies.' In *Cyber Security Policies and Critical Infrastructure Protection*, edited by Guido Gluschke, Prof. Dr. Mesut Hakki Casin, and Merco Macori. Institute for Security and Safety GmbH.

Retter, Lucia, Erik J. Frinking, Stijn Hoorens, Alice Lynch, Fook Nederveen and William D. Phillips. 2020. 'Relationships between the economy and national security: Analysis and considerations for economic security policy in the Netherlands.' RAND Europe. As of 13 October 2020: https://www.rand.org/pubs/research_reports/RR4287.html

Rijksoverheid. 2020. 'Aart Jochem eerste CISO Rijk.' Rijksoverheid.nl. As of 13 October 2020: https://www.rijksoverheid.nl/actueel/nieuws/2020/09/18/aart-jochem-eerste-ciso-rijk

Rowe, Andy. 2019. 'Sustainability-Ready Evaluation: A Call to Action.' *New Directions for Evaluation* 162, 29–48. As of 13 October 2020: https://onlinelibrary.wiley.com/doi/10.1002/ev.20365

Schallbruch, Martin and Skierka, Isabel Marie. 2018. 'The Organisation of Cybersecurity in Germany.' Digital Society Institute, ESMT Berlin. As of 10 October 2020: https://www.researchgate.net/publication/326509095_The_Organisation_of_Cybersecurity_in_Germany

Serna, Fermin J. 2020. 'Citrix provides update on Citrix ADC, Citrix Gateway vulnerability.' Citrix Blog. As of 20 October 2020: https://www.citrix.com/blogs/2020/01/11/citrix-provides-update-on-citrix-adc-citrix-gateway-vulnerability/

Silfversten, Erik, Erik Frinking, Nathan Ryan and Marina Favaro. 2019. 'Cybersecurity: A State-of-the-art Review.' RAND Europe. Prepared for the WODC. As of 13 October 2020: https://www.wodc.nl/onderzoeksdatabase/2956-state-of-the-art-cybersecurity.aspx

Swedish Civil Contingencies Agency. N.d. 'Myndigeter med ansvar.' As of 20 October 2020: https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/systematiskt-informationssakerhetsarbete/informationssakerhet-i-samhallet/myndigheter-med-ansvar/

———. 2015. 'Samverkansgruppen för informationssäkerhet.' As of 20 October 2020: https://www.informationssakerhet.se/om-informationssakerhet2/samverkansgruppen-for-informationssakerhet/

———. 2019. 'Comprehensive Cyber Security Action Plan.' As of 20 October 2020: https://rib.msb.se/filer/pdf/28898.pdf

———. 2020. 'Samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022: redovisning 2020.' As of 20 October 2020: https://www.msb.se/sv/publikationer/samlad-informations--och-cybersakerhetshandlingsplan-for-aren-20192022--redovisning-2020/

Swedish Government Offices. 2018. 'Förordning om informationssäkerhet för samhällsviktiga och digitala tjänster.' As of 20 October 2020: https://www.svenskforfattningssamling.se/doc/20181175.html

Swedish Ministry of Defence. 2019. 'Uppdrag inför inrättandet av ett nationellt cybersäkerhetscenter.' As of 20 October 2020: https://www.regeringen.se/4ada4c/globalassets/regeringen/dokument/forsvarsdepartementet/regeringsbeslut/uppdrag-infor-inrattandet-av-ett-nationellt-cybersakerhetscenter.pdf

Swedish Ministry of Justice. 2017. 'A National Cyber Security Strategy.' As of 20 October 2020: https://www.government.se/4ada5d/contentassets/d87287e088834d9e8c08f28d0b9dda5b/a-national-cyber-security-strategy-skr.-201617213

Swedish National Audit Office (NAO). 2016. 'Informationssäkerhetsarbete på nio myndigheter (RiR 2016:8).' As of 20 October 2020: https://www.riksrevisionen.se/rapporter/granskningsrapporter/2016/informationssakerhetsarbete-pa-nio-myndigheter.html

Swedish Security Police. 2019. 'Svar på uppdrag (Fö2019/01000/SUND) inför inrättandet av ett nationellt cybersäkerhetscenter.' As of 20 October 2020: https://www.sakerhetspolisen.se/download/18.a5cd4be16dfd84e1711fc/1576501963916/Svar_pa_uppdrag_infor_inrattandet_av_ett_nationellt_cybersakerhetscenter.pdf

Taylor, J.M. & H.R. Sharif. 2017. 'Security challenges and methods for protecting critical infrastructure cyber-physical systems.' 2017 International Conference on Selected Topics in Mobile and Wireless Networking, MoWNeT 2017. Institute of Electrical and Electronics Engineers Inc. As of 13 October 2020: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85032911530&doi=10.1109%2fMoWNet.2017.8045959&partnerID=40&md5=374bf4aafa71a27eb1d2be9eebb17dea

The German Federal Government. 2016. 'White Paper on German Security Policy and the future of the Bundeswehr.' As of 10 October 2020: https://www.gmfus.org/file/8970/download

The White House. 2013. 'Presidential Policy Directive – Critical Infrastructure Security and Resilience.' Obamawhitehouse.archives.gov. As of 20 October 2020: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

———. 2016. 'Presidential Policy Directive – United States Cyber Incident Coordination.' Obamawhitehouse.archives.gov. As of 20 October 2020: https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

———. 2017. 'National Security Strategy of the United States of America.' As of 16 June 2020: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

———. 2018. 'National Cyber Strategy of the United States of America.' As of 16 June 2020: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

UK National Cyber Security Centre (NCSC-UK). N.d. 'Active Cyber Defence (ACD).' Ncsc.gov.uk. As of 13 October 2020: https://www.ncsc.gov.uk/section/products-services/active-cyber-defence

———. 2019. 'Active Cyber Defence (ACD) – The Second Year.' NCSC-UK. As of 13 October 2020: https://www.ncsc.gov.uk/report/active-cyber-defence-report-2019

US Congress. 1986. 'Computer Fraud and Abuse Act of 1986.' As of 16 June 2020: https://www.congress.gov/bill/99th-congress/house-bill/4718

———. 1999. 'Gramm-Leach-Bliley Act.' As of 16 June 2020: https://www.congress.gov/bill/106th-congress/senate-bill/900

———. 2002. 'Federal Information Security Management Act of 2002.' As of 16 June 2020: https://www.congress.gov/bill/107th-congress/house-bill/3844

———. 2014a. 'National Cybersecurity Protection Act of 2014.' As of 16 June 2020: https://www.congress.gov/bill/113th-congress/senate-bill/2519#:~:text=National%20Cybersecurity%20Protection%20Act%20of%202014%20%2D%20(Sec.&text=Requires%20the%20center%20to%20be,federal%20and%20non%2Dfederal%20entities.

———. 2014b. 'Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015.' As of 20 October 2020: https://www.congress.gov/bill/113th-congress/house-bill/3979

———. 2015. 'To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.' As of 16 June 2020: https://www.congress.gov/bill/114th-congress/senate-bill/754

———. 2018. 'Cybersecurity and Infrastructure Security Agency Act of 2018.' As of 16 June 2020: https://www.congress.gov/bill/115th-congress/house-bill/3359

US Department of Defense. 2018a. 'National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge.' As of 16 June 2020: https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf?mod=article_inline

———. 2018b. 'Summary: Department of Defense Cyber Strategy'. As of 16 June 2020: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

US Department of Homeland Security (DHS). 2014. 'Cybersecurity Capability Maturity Model White Paper.' DHS.

———. 2016. 'National Cyber Incident Response Plan'. As of 16 June 2020: https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

———. 2018. 'U.S Department of Homeland Security - Cybersecurity Strategy' As of 16 June 2020: https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf

———. 2019. 'Critical Infrastructure Sectors.' As of 13 October 2020: https://www.dhs.gov/cisa/critical-infrastructure-sectors

———. 2020. 'Cybersecurity.' As of 16 June 2020: https://www.dhs.gov/topic/cybersecurity

US Cyberspace Solarium Commission. 2020. [Homepage]. As of 20 October 2020: https://www.solarium.gov/

US Government Accountability Office (GAO). 2004. 'Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism.' As of 20 October 2020: https://www.gao.gov/products/GAO-04-408T

———. 2011. 'Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination.' GAO. As of 13 October 2020: https://www.gao.gov/assets/590/586494.pdf

———. 2017. 'Cybersecurity: Federal Efforts Are Under Way That May Address Workforce Challenges.' GAO. As of 13 October 2020: https://www.gao.gov/assets/690/683923.pdf

———. 2020. 'Cybersecurity: Clarity of Leadership Urgently Needed to Fully Implement the National Strategy.' GAO. As of 20 October 2020: https://www.gao.gov/assets/710/709555.pdf

US Senate. 2019. 'Federal Cybersecurity: America's Data at Risk.' Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs. As of 20 October 2020: https://www.hsgac.senate.gov/imo/media/doc/2019-06-25%20PSI%20Staff%20Report%20-%20Federal%20Cybersecurity%20Updated.pdf

Van Asselt, Marjolein and Ortwin Renn. 2011. 'Risk governance.' *Journal of Risk Research* 14: 431–449.

Voigt, Paul. 2018. 'Information Security Considerations (Germany).' Practical Law of Thomson Reuters. As of 10 October 2020: https://www.taylorwessing.com/-/media/taylor-wessing/files/germany/2019/06/information-security-considerations-germany-2019.pdf

Zedler, Dominika. 2017. 'Zur strategischen Planung von cyber security in Deutschland.' Außen Sicherheitspolit, 30 January 2017. As of 10 October 2020: https://link.springer.com/content/pdf/10.1007/s12399-016-0606-9.pdf

Walker, W.E., Rahman S.A., Cave, J. 2001. 'Adaptive policies, policy analysis, and policymaking.' *European Journal of Operations Research* 128, 282–289.

Walker, Warren E., Robert J. Lempert, Jan H. Kwakkel. 2016. 'Deep Uncertainty.' In *Encyclopedia of Operations Research and Management Science*, edited by Saul I. Gass and Michael C. Fu. As of 13 October 2020: https://link.springer.com/referenceworkentry/10.1007%2F978-1-4419-1153-7_1140

Wilhelmson, Nina and Thomas Svensson. 2011. 'Handbook for planning, running, and evaluating information technology and cyber security exercises.' Center for Asymmetric Threat Studies (CATS). As of 13 October 2020: https://www.diva-portal.org/smash/get/diva2:1235949/FULLTEXT01.pdf

World Health Association (WHO). N.d. 'How to Evaluate the Programme.' In *Drinking and Driving: A Road Safety Manual for Decision-Makers and Practitioners*. As of 13 October 2020: https://www.who.int/roadsafety/projects/manuals/alcohol/4-How%20to.pdf?ua=1

Annex A. Methodology

This chapter outlines the methodology employed by the study team to conduct Phase 2 of the study. The purpose of this phase is to examine in detail the two research areas (RAs) prioritised by the NCTV in Phase 1, namely:

1. **Cybersecurity governance from a national security perspective**, which is concerned with the rising use and adoption of, and potential disruption to ICTs, which has led governments to question how best to govern cybersecurity issues that relate to national security.
2. **Critical infrastructure protection and security**, which is concerned with how recent trends to Internet-enable certain components of critical infrastructure and of adopting new or emerging technologies or solutions are presenting novel and significant security challenges to services deemed critical to the functioning of society.

The two RAs and RQs are listed in Table A.1 below.

Table A.1 Overview of research areas and research questions

Overarching research area	Research questions (RQs)
1. Cybersecurity governance from a national security perspective	1.1 How can the current model of governance and current cybersecurity initiatives in the Netherlands be aligned and improved?
	1.2 How can system responsibility for cybersecurity be set up?
	1.3 What lessons can be identified through international comparisons of different national cybersecurity governance models?
	1.4 How can capabilities and skills required across stakeholders and functions to ensure national cybersecurity be identified and managed?
	1.5 How could efficiency and effectiveness be measured for cybersecurity policymaking?
2. Critical infrastructure protection and security	2.1 What are the risks and challenges resulting from the interplay between legacy critical infrastructure technologies and new technologies?
	2.2 How can current levels of cybersecurity maturity within the critical infrastructure sector be measured and understood?
	2.3 What can be done to improve security of operational technology deployed in critical sectors?
	2.4 What can be done with a view to potential threats from actors and organised groups or networks of actors in order to prevent damage to the vital infrastructure?

The study team used a combination of desk research and literature review, case studies, key informant interviews and expert workshops.

Specifically, the methodological activities were broken down into four main tasks:

Task 1: RA1 evidence synthesis

Task 2: RA2 evidence synthesis

Task 3: Expert workshops

Task 4: Analysis

The corresponding steps are outlined in detail in the following sections.

A.1. Task 1: RA1 evidence synthesis

The synthesis of available evidence on RA1 involved a mixed-methods approach of desk research and document review, case studies and key informant interviews. Table A.2 provides an indication of how each methodological approach mapped onto the sub-questions.

Table A.2 Overview of RA1 methodological approaches mapped onto sub-questions

RQs	Approach
1.1 How can the current model of governance and current cybersecurity initiatives in the Netherlands be aligned and improved?	Desk research and literature review Key informant interviews with Dutch stakeholders Expert workshop
1.2 How can system responsibility for cybersecurity be set up?	Key informant interviews with Dutch stakeholders Expert workshop
1.3 What lessons can be identified through international comparisons of different national cybersecurity governance models?	Case studies
1.4 How can capabilities and skills required across stakeholders and functions to ensure national cybersecurity be identified and managed?	Case studies Desk research and literature review Key informant interviews with Dutch stakeholders Expert workshop
1.5 How could efficiency and effectiveness be measured for cybersecurity policymaking?	Desk research and literature review Case studies and interviews as part of case studies

A.1.1. Desk research and document review

The desk research and document review explored the evidence base on the topic of cybersecurity governance from a national security perspective. It determined how thoroughly this topic is investigated in the existing literature and examined the quality of the data and methods used as part of existing studies.

The research was conducted in both English and in Dutch, and included, to the greatest extent possible, literature with a geographic focus on the Netherlands. The type of documents reviewed included:

- Dutch government publications and strategy documents, to contextualise the national governance of cybersecurity in the Netherlands;
- Academic and grey literature: journal articles, working papers, conference proceedings, white papers, and blogs on the topic of national governance of cybersecurity; and
- Outputs of previous Dutch and European research efforts on the topic of national governance of cybersecurity.

The document search was conducted through:

- Pre-existing RAND Europe knowledge of key policy documents;
- A structured keyword search conducted both in Dutch and in English through Google Scholar, using terms linked to the RQs;
- A snowballing approach to identify other relevant documents in report bibliographies or citations; and
- Recommendations given by interviewees.

A.1.2. Case studies

The case studies were pursued to identify different governance approaches pursued by other countries and explore what lessons could be identified through a comparison of different cybersecurity national governance models. The case study countries were selected in conjunction with the WODC and the project SAC, and comprised Estonia, Germany, Sweden, the United Kingdom and the United States.

The development of the case study country profiles focused on:

- Producing a brief overview of the national governance structure; and
- Identifying any evaluations of the national governance structure to highlight potential lessons for the Netherlands.

The case studies were predominantly developed through review of publicly available government strategies and policies, reports on national governance structures and evaluations or other efforts that assessed or evaluated the national governance approaches.

A.1.3. Stakeholder interviews

Key informant interviews were used to capture views from different stakeholders and to test assumptions and evidence emerging from the document review. The interviews were conducted with Dutch or international cybersecurity subject-matter experts in the area of cybersecurity governance, as detailed in Annex B. The interviewees were identified through a combination of:

- Pre-existing RAND Europe knowledge and contacts; and
- Recommendations given by the WODC and the SAC.

The interviews were semi-structured and designed to elicit responses about national cybersecurity governance structures, best practices, and knowledge and research gaps. Box 6 provides an overview of the key interview questions for RQ1 and the list of interviews can be found in Annex B.

Box 6 Sample of RA1 interview questions

- What are your thoughts on the current Dutch governance structure?
- How do you ensure you have the right capabilities and skills required across stakeholders and across functions (e.g. intelligence, operations, coordination, command and control, training, etc.) to ensure national cybersecurity?
- Are there capabilities and skills that you would say are crucial for national cybersecurity?
- How can the current model of governance and current cybersecurity initiatives (e.g. strategies, research agendas, roadmaps, etc.) in the Netherlands be aligned and improved?
- How can system responsibility for cybersecurity be set up?

A.2. Task 2: RA2 evidence synthesis

As was the case with RA1, the synthesis of available evidence on RA2 involved a mixed-methods approach. Table A.3 provides an indication of how each methodological approach mapped onto the sub-questions.

Table A.3 Overview of RA2 methodological approaches mapped onto sub-questions

RQs	Approach
2.1 What are the risks and challenges resulting from the interplay between legacy critical infrastructure technologies and new technologies?	Desk research and literature review Interviews Expert workshop
2.2 How can current levels of cybersecurity maturity within the critical infrastructure sector be measured and understood?	Desk research and literature review Interviews Expert workshop
2.3 What can be done to improve security of operational technology deployed in critical sectors?	Desk research and literature review Interviews Expert workshop
2.4 What can be done with a view to potential threats from actors and organised groups or networks of actors in order to prevent damage to the vital infrastructure?	Desk research and literature review Interviews Expert workshop

A.2.1. Desk research and literature review

The desk research and document review explored the evidence base on the topic of cybersecurity governance from a national security perspective. It determined how thoroughly this topic is investigated in the existing literature and examined the quality of the data and methods used as part of existing studies. The research was conducted in both English and in Dutch, and included, to the greatest extent possible, literature with a geographic focus on the Netherlands. The type of documents reviewed included:

- Dutch government publications and strategy documents, to contextualise critical infrastructure security in the Netherlands;
- Academic and grey literature: journal articles, working papers, conference proceedings, white papers, and blogs on the subject of critical infrastructure security, particularly in consideration of cybersecurity arrangements and national approaches to operationalisation and management; and
- Outputs of previous Dutch and European research efforts on the topic of critical infrastructure security, including European Union research framework outputs and publications from ENISA.

The document search was conducted through:

- Pre-existing RAND Europe knowledge of key policy documents;
- A structured keyword search conducted both in Dutch and in English through Google Scholar, using terms such as 'critical infrastructure cybersecurity', 'cybersecurity of operational technology', 'critical infrastructure cybersecurity maturity', or 'supply chain cybersecurity maturity';
- A snowballing approach to identify other relevant documents in report bibliographies or citations; and
- Recommendations given by interviewees.

A.2.2. Stakeholder interviews

Key informant interviews were used to capture views from different stakeholders and to test assumptions and evidence emerging from the document review. The interviews were conducted with Dutch or international cybersecurity subject-matter experts in the area of critical infrastructure protection. The interviewees were identified through a combination of:

- Pre-existing RAND Europe knowledge and contacts;
- Recommendations given by the WODC and SAC;
- Desk research and document review, which revealed subject-matter experts; and
- Recommendations given by other interviewees.

The interviews were semi-structured and designed to elicit responses about national cybersecurity governance structures, best practices, and knowledge and research gaps. Box 7 provides an overview of the key interview questions for RQ2 and the list of interviews can be found in Annex B.

Box 7 Sample of RA2 interview questions

- What is the interplay between legacy critical infrastructure technologies and new technologies?
- What can be done to improve security of OT deployed in critical sectors?
- What can be done with a view to potential threats from actors and organised groups or networks of actors in order to prevent damage to the vital infrastructure?
- How can current levels of cybersecurity maturity within the critical infrastructure sector be measured and understood?
    - How do you understand supply-chain cybersecurity maturity?

A.3. Task 3: Workshops

Once the first two tasks concluded – which completed the mapping of the existing knowledge and research on the two research areas – the study team conducted two half-day workshops, one dedicated to each respective RA:

- **Expert workshop 1** focused on cybersecurity governance from a national security perspective; and
- **Expert workshop 2** focused on critical infrastructure security.

The main purpose of these workshops was two-fold:

- Firstly, the workshops presented an opportunity to share the emerging findings from the data-synthesis activities (including desk research and document review, case studies and interviews) so that participants could discuss, challenge, validate and ensure that the findings are relevant to the specific Dutch context; and
- Secondly, the workshops facilitated a structured discussion meant to identify possible next steps or actionable recommendations to the NCTV in relation to the RQs, as well as prioritise sub-questions in order to identify priority areas for the Netherlands so as to inform the future NCTV research agenda.

The outputs of the two workshops were then analysed as part of Task 4. The list of workshop participants can be found in Annex B.

A.4. Task 4: Analysis

Once the first three tasks were completed, the findings and outputs were consolidated. The evidence base was mapped out against the research questions and the findings were analysed. On the basis of the conclusions drawn, relevant policy inputs were developed. In order to validate the final findings and recommendations, the study team organised a series of internal workshops that also contributed to the development of the study's recommendations for the NCTV.

Annex B. List of interviewees and workshop participants

This annex lists the interviewees and workshop participants that took part in the study.

Table B.1 List of interviewees

Reference	Name and role	Organisation
INT01	Advisor	Netherlands Ministry of the Interior and Kingdom Relations Directorate for Public Administration (DGOO)
INT01	Advisor	Netherlands Ministry of the Interior and Kingdom Relations Directorate for Public Administration (DGOO)
INT02	Raul Rikk, National Cyber Security Policy Director	Government CIO Office, Estonia Ministry of Economic Affairs and Communications
INT03	Jeoren van der Ham, Senior Researcher	Netherlands National Cyber Security Centre
INT03	George Middeldorp, Strategic advisor	Netherlands National Cyber Security Centre
INT04	Lourens Visser, CIO Rijk	Netherlands Ministry of the Interior and Kingdom Relations
INT05	Patricia Zorko, Deputy National Coordinator for Security and Counterterrorism, Director, Cybersecurity Department	Netherlands National Coordinator for Security and Counterterrorism
INT06	Jos de Groot, Director, Digital Economy	Netherlands Ministry of Economic Affairs
INT07	Policy Officer Cyber	Netherlands Ministry of Defence
INT08	Jair Satanna	University of Twente
INT09	Anonymous	Anonymous
INT10	Tom van Schie	TNO
INT11	Jeroen Gaiser	*Rijkswaterstaat*
INT12	Xander van der Voort	VanderVoort Cybersecurity
INT13	Anonymous	Anonymous
INT14	Anonymous	Auburn University
INT15	Shannon Cardash	Auburn University
INT16	Justyna Chromik	Applied Risk
INT17	Ragnar Schierholz	ABB

The study involved two workshops held remotely:

- 7 September 2020 – workshop focusing on critical infrastructure; and
- 8 September 2020 – workshop focusing on cybersecurity governance.

Table B.2 List of workshop participants

Workshop date	Name	Organisation
7 September 2020	Tom van Schie	TNO
7 September 2020	Jeroen Gaiser	*Rijkswaterstaat*
7 September 2020	Ragnar Schierholz	ABB
8 September 2020	Frank Heijligers	Netherlands Ministry of the Interior
8 September 2020	Jeroen van der Ham	Netherlands National Cyber Security Centre
8 September 2020	Nicolas Castellon	Capgemini
8 September 2020	Pieter Bindt	Associate Board Member, Dutch Safety Board
8 September 2020	Pieter Van Den Berg	
8 September 2020	Michiel Steltman	
8 September 2020	Jan-Piet Barthel	
8 September 2020	Matthijs Koot	Secura
8 September 2020	Anonymous	-

Annex C. Case-study country profiles

This annex contains four case studies of national governance systems in Estonia, Germany, Sweden, the United Kingdom and the United States, which collectively provide a point of comparison and potential lessons for governance of the cybersecurity ecosystem in the Netherlands.

C.1. Estonia

C.1.1. Background

Overall, Estonia has undertaken a comprehensive approach to e-governance and national cybersecurity, perceived as a key pillar of national security. In continuation of the two previous strategies of 2008–2013[295] and 2014–2018,[296] the 2019–2022 Cybersecurity Strategy establishes Estonia's policy direction with regards to its long-run vision, aims and priorities.[297] The national strategy is accompanied by the 2018 Cybersecurity Act, which represents the major general regulation of cybersecurity in Estonia and is the national implementation of the European network and information security directive (NIS directive).[298]

The Estonian Cybersecurity Strategy builds on several challenges identified in 2018, mapped against four overarching objectives, as seen in Table C.1 below.

[295] Estonian MOD (2008).
[296] Estonian Ministry of Economic Affairs and Communication (2014).
[297] Estonian Ministry of Economic Affairs and Communication (2018).
[298] Parliament of Estonia (2018).

Table C.1.1 Overview of Estonia's national cybersecurity challenges, strategy objectives and means

Challenge (2018)	Ends (2022)	Means
• Weak strategic integral management, insufficient cross-institutional situational awareness and fragmented organisation of information systems security • Insufficient consideration of security aspects during the development phase of information systems and services • Insufficient understanding of the impact of cyber threats, incidents and infrastructure interdependencies	**Objective 1: A sustainable digital society** Estonia is a sustainable digital society relying on strong technological resilience and emergency preparedness.	• Developing technological resilience • Ensuring cyber incident and crisis prevention, preparedness and resolution • Fostering comprehensive governance and development of a cohesive cybersecurity community
• Scarcity of Estonian enterprises successfully offering their cybersecurity products and services on the international market • Insufficient investments into R&D investment	**Objective 2: Cybersecurity industry, research and development** Estonian cybersecurity industry is strong, innovative, research-oriented and globally competitive, covering all key competences for Estonia.	• Supporting and promoting Estonian cybersecurity R&D and research-driven industry
• Retaining Estonia's reputation as a highly reliable international partner	**Objective 3: A leading international contributor** Estonia is a credible and capable partner in the international arena.	• Advancing substantial cooperation on cyber issues with strategic international partners • Promoting sustainable cybersecurity capacity-building across the globe
• Low cybersecurity awareness and deficient sense of ownership in risk management • Lack of specialists and insufficient supply of new talent	**Objective 4: A cyber-literate society** Estonia is a cyber-literate society and ensures sufficient and forward-looking talent supply	• Advancing substantial cooperation on cyber issues with strategic international partners • Promoting sustainable cybersecurity capacity-building across the globe

Source: Estonian Ministry of Economic Affairs and Communication (2018).

C.1.2. Overview of governance approach

The Cyber Security Council of the Security Committee of the Estonian Government is responsible for the Cybersecurity Strategy at the strategic and policy level, whereas the Ministry of Economic Affairs and Communications (MEAC) is the main implementation and coordination body for national cybersecurity.[299]

Various other ministries and agencies support the MEAC in the implementation of the Cybersecurity Strategy, as discussed in further detail.

[299] Ministry of Economic Affairs and Communication (2020).

Roles and responsibilities

Similar to the Dutch system, the Estonian cybersecurity governance model follows the constitutional governance model that applies to government overall. Estonia uses a decentralised and distributed model of governance, with a relatively weak Prime Minister function and significant authority delegated to individual ministers and ministries.[300] This means that policy areas are led by a 'lead ministry', which is responsible for regulation and implementation of regulation within the policy area in question.[301]

Civilian architecture for cybersecurity

At the strategic level, the Security Committee coordinates the activities of security authorities at the ministerial level. The Security Committee is composed of the Prime Minister, the Minister of Justice, the Minister of Defence, the Minister of Finance, the Minister of the Interior and the Minister of Foreign Affairs. Its responsibilities include:

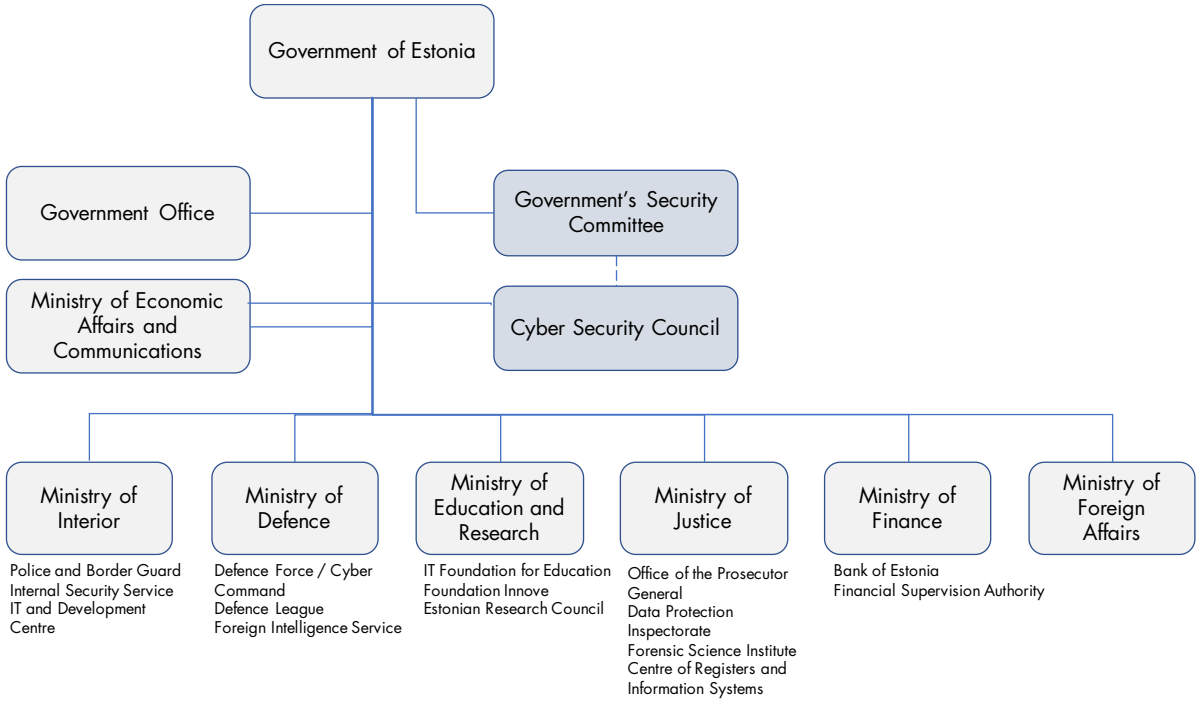
- Conducting analysis and assessment of the national security situation;
- Articulating Estonia's need for security-related information; and
- Performing other functions imposed on the Security Committee as directed by the Government of the Republic and other legislative acts.[302]

The Cyber Security Council, which was created as a subcommittee of the Security Committee in 2009, is responsible for facilitating strategic-level inter-agency collaboration and tracking the policy implementation of the Cybersecurity Strategy objectives.[303] The Council is chaired by the Secretary General of the MEAC, as the lead ministry for cybersecurity, and gathers the permanent secretaries of all relevant ministries and heads of relevant agencies.

The decision to place cybersecurity under the MEAC was primarily driven by a desire to align the Estonian digitisation effort with its national cybersecurity effort, thereby closing the gap between ICT development policy and cybersecurity risk management.[304] An Estonian government official interviewed for this study noted that this choice has been one of the key enablers for the Estonian national cybersecurity effort. As cybersecurity was already an integral part of the discussion at the early stages of digitalisation of Estonian society and e-government, it was much easier to close the gaps between an increasingly digital Estonia and its changing security requirements.[305] Nonetheless, there are also several other ministries that feed into Estonian national cybersecurity, as shown in Figure C.1.

[300] INT02.
[301] INT02.
[302] Parliament of Estonia (2000).
[303] Estonian Information System Authority (2020).
[304] INT02.
[305] INT02.

Figure C.1.1 Overview of cybersecurity organisations in Estonia



Source: RAND Europe based on Estonian Ministry of Economic Affairs and Communication (2014).

Within the MEAC, the State Information System Authority (RIA) is the main authority for cybersecurity coordination.[306] In this sphere, the RIA:

- Organises the protection of critical information infrastructure;
- Organises the development of the system of security measures for information systems and coordinates the implementation of information security measures;
- Performs the duties of a single point of contact for the purposes of section 5 of the Cybersecurity Act and of a Computer Emergency Response Team (CERT), and coordinates the prevention and resolution of cybersecurity incidents;
- Organises the monitoring and analysis of risks to cybersecurity and notification of the public regarding the threats;
- Manages external projects within the framework of the competence of the Authority; and
- Performs administrative and state supervision and implementation of administrative coercion, and carries out extrajudicial proceedings of misdemeanours pursuant to legislation.[307]

The RIA consists of several structural units, including the Cyber Security Branch, the State Information System Branch and the Information Security Department. The former's main duties are:

- Fulfilment of CERT tasks at the national level, including handling security incidents in Estonian computer networks;

[306] Estonian Information System Authority (2020).
[307] Estonian Ministry of Economic Affairs and Communication (2014).

- Coordination of ensuring cybersecurity and preventing and solving cyber incidents, increasing overall cyber awareness for the prevention of cyber incidents and responding to them;
- Preparation of reports on cyber incidents and the spread of malware in Estonian computer networks;
- Carrying out observation of the domains in the Estonian IP address space and domains with an Estonian country reference, analysing the risks posing a threat to the security of network and information systems and their impact, and forwarding warnings;
- Participating in the development of legislation, strategies, development plans, indicative programmes and budgets related to cybersecurity and exercising state and administrative supervision, the proceeding of misdemeanours, and processing the applications for activity licences for the provision of qualified trust services;
- Giving advice for the due implementation of measures aimed at ensuring the security of network and information systems; and
- Organising and coordinating research and development activities and cooperating with the research and scientific institutions of the area of cybersecurity;

Considering its role and breadth of activities, the RIA is similar to other nations' own national cybersecurity centres (e.g. those in the Netherlands or UK).[308] The RIA also hosts the Estonian Computer Emergency Response Team (CERT-EE), which is in charge of potential security incidents for networks in the country. Its main purposes are to promote secure networking, deal with computer security incidents and cooperate with internationally recognised information-technology security-incident prevention institutions (e.g. teams, CSIRTs, CERTs).[309] CERT-EE thus centres on the operational level while the Cyber Security Branch commands the strategic layer by mapping vulnerabilities, steering risk assessment and overseeing the implementation of measures.[310] In case of serious cyberattacks, RIA monitors the coordination of national responses, the prevention and measures to thwart incidents. On demand, it can be assisted by the Cyber Defence Unit (CDU) of the Estonian Defence League, which is permitted to support civilian authorities in the cybersecurity sphere.[311]

Other organisations that support the MEAC and RIA in national cybersecurity include the Estonian Internal Security Service, which contributes to national defence by identifying and attempting to thwart in advance cyber threats related to intelligence, terrorism and sabotage, while the Ministry of Justice is also involved in cybersecurity policy through legal proceedings and violence-prevention activities.[312] It also includes agencies that undertake supervision of rights and personal data protection, such as the Data

[308] INT02.
[309] Estonian Information System Authority (2020).
[310] Boeke (2017).
[311] Estonian Defence League (2020).
[312] Estonian Internal Security Service (2020).

Protection Inspectorate and those who are in charge of developing and managing registers and information systems , such as the Centre of Registers and Information Systems.[313]

Defence aspects of national cybersecurity

The Ministry of Defence (MOD) organises Estonian national defence to deter cyberattacks and guarantee the country's ability to shield against external threats. To this end, the Estonian MOD collaborates with the Foreign Intelligence Service, Defence Forces Cyber Command (Cyber Command) and the Defence League's Cyber CDU.[314]

Within the MOD, the Cyber Command was created in 2018 as a wartime unit under the direct authority of the Commander of the Defence Forces.[315] Its establishment was meant to enhance the strategic and operational understanding of cyberspace operations in a kinetic conflict as well as raising awareness with regards to cyber threats upon military activities.[316] The Cyber Command main functions are to:

- Organise command support and cyber defence in the area of government of the MOD;
- Organise information and cyber operations; and
- Organise the development and operation of information and communication technology in the area of government of the MOD.[317]

Additionally, it guarantees cyber defence and provides information and communication technology infrastructure and services along to supply headquarters support for the military's Joint Headquarters[318]. Since 2019, the Cyber Command and RIA have a cooperation agreement to practise both inter-agency cooperation – as well as with other civilian entities – in diverse exercises and to foster the exchange of information.[319] However, it is uncertain whether the Cyber Command supports civilian authorities should serious cyberattacks occur in their jurisdiction.[320]

The CDU of the Estonian Defence League is a voluntary, military-organised entity contributing to the protection of national cyberspace. During crisis, it can be used to support civil structures and defend critical infrastructures. [321] The 2013 Estonian Defence League Act (EDLA) incorporated the CDU into the national defence system, detailing its mandate, structure and functioning.[322] The Defence League is managed by the Commander of the Defence League, who is directly subordinated to the Commander of the Defence Forces.[323] Where necessary, the Defence League can also be invited to ensure cybersecurity under the supervision of other authorities, such as the RIA. As established in the EDLA, Defence League's scope of responsibilities in the realm of cyber include to:

---

[313] Estonian Data Protection Inspectorate (2020); Estonian Centre of Registers and Information Systems (2020).
[314] Estonian Ministry of Defence (2020).
[315] Estonian Ministry of Defence (2018).
[316] Pernik (2018).
[317] Government of Republic of Estonia (2018).
[318] Estonian Ministry of Defence (2020).
[319] Estonian Information System Authority (2020).
[320] Pernik (2018).
[321] Estonian Information System Authority (2020).
[322] Estonian Information System Authority (2020).
[323] Parliament of Estonia (2013).

- Prepare the national defence capability of the state;
- Participate in enhancing and ensuring security of Estonian residents;
- Provide and organise military training to active members; and
- Provide and organise other training and education.

The Defence League may also be invited to contribute:

- In resolving an emergency, in rescue work and ensuring the safety in the procedure provided for in the Emergency Act;
- In resolving a state of emergency in the procedure provided for in the State of Emergency Act;
- In ensuring cybersecurity under the direction of a competent authority; and
- In police activity in the procedure provided for in the Police and Border Guard Act.

C.1.3. Evaluation and performance

The 2018–2020 Cybersecurity Strategy contains two key impact indicators for the strategy:

1. No cyber incident causes significant disruptive social and economic effect on Estonian society or forces its residents to abandon the digital solutions they are accustomed to using; and
2. Estonian residents feel secure online and trust digital public services.

The Strategy highlights the achievement of the first indicator, noting that since 2007, no cyber incident has substantively disrupted Estonia's information society or forced Estonia to abandon its digital solutions.[324] For the second indicator, the Strategy uses two metrics:

1. The percentage of residents who forgo electronic communication with public sector or private service providers in order to avoid security risks – the ambition is that this will remain at the same level by 2020 (i.e. 3.1 per cent).
2. The percentage of secure digital identity users among all digital identity holders – the ambition is that this will increase to ≥65 per cent by 2020 (up from 57.6 per cent in 2017).[325]

Beyond the above, this case study review did not identify any publicly available evaluation of Estonia's governance model or its national cybersecurity performance. However, the case study interviewee highlighted that the Estonian government continuously gathers opinion on the performance of national cybersecurity work to improve the strategy and its implementation. The interviewee also noted that there has been a study of the governance structure in cooperation with an Estonian technical university, but that it has not been made public.[326]

[324] Estonian Ministry of Economic Affairs and Communication (2018).
[325] Estonian Ministry of Economic Affairs and Communication (2018).
[326] INT02.

C.2. Germany

C.2.1. Background

The first national cybersecurity-related strategy was adopted in 2005 through the National Plan for the Protection of Information Infrastructures.[327] The 2011 Cybersecurity Strategy for Germany broadened the scope of the 2005 strategy from a technical, infrastructure-centred approach toward a whole-society issue incorporating the strategic, social and economic perspectives.[328] It further established two federal bodies to monitor the cybersecurity of information and infrastructure in Germany. Since then, the National Cyber Security Council has ensured the implementation of the National Cyber Security Strategy. The National Cyber Response Centre (as part of the BSI) analyses cybersecurity incidents and recommends measures for action to the National Cyber Security Council. In response to an increased number of threats on governmental institutions, vital services, the private sector and individuals, the strategy was updated in 2016.[329] Reflecting on these challenges, the 2016 strategy describes four strategic national cybersecurity priorities for Germany:

- Safe and self-determined action in a digitised environment;
- Joint efforts from the Federal Government and the private sector;
- Efficient and sustainable cybersecurity architecture; and
- Active positioning of Germany in European and international cybersecurity policy.[330]

Following the 2016 Cyber Security Strategy for Germany, the federal government unveiled its White Paper on German Security Policy and the future of the Bundeswehr (German Armed Forces), with specific emphasis given on the security challenges arising from the Cyber and Information realms.[331]

Germany's cybersecurity strategy is also supported by legislation. In 2009, the Act to Strengthen the Security of Federal Information Technology established the BSI as the central institution to deal with cybersecurity at the federal level.[332] In order to strengthen the protection of critical infrastructure, the 2015 IT Security Act amended the Act of 2009 with new measures.[333] The 2015 IT Security Act was then updated in 2017 to bring German law in line with the NIS Directive requirements.[334] It further commands online, telecommunication services, electricity supply networks and diverse entities to equip their IT systems and infrastructures with sufficient safeguards.[335] Overall, these regulations implement minimum IT security requirements – in particular for critical infrastructures in several sectors (transportation, energy, insurance, water and food, health, ICT, finance) – and require service providers to report significant cybersecurity incidents to the BSI.

---

[327] Bundesminister des Innern (2005).
[328] Bundesminister des Innern (2011).
[329] Bundesminister des Innern (2016).
[330] Bundesminister des Innern (2016).
[331] Bundeswehr (n.d.).
[332] Bundestag (2009).
[333] Bundestag (2015).
[334] European Parliament and the Council of the EU (2016).
[335] Voigt (2018).

C.2.2. Overview of governance approach

Roles and responsibilities

Germany's political governance system is based on a federal approach where power is shared between the central state (i.e. federal level) and the federal regional state (i.e. the 16 *Länder).* Each of the 16 states has its own government and minister president who, collectively, are represented on the German Federal Council (*Bundesrat*).[336] Although cybersecurity is predominantly a national (i.e. federal) issue in Germany, each state typically has some structures in place for IT administration and cybersecurity.[337]

Beyond cybersecurity, the German internal security architecture is also distinguished by the institutional separation between the federal and state governments. In addition, the 1949 Basic Law of the Federal Republic of Germany (FRG), resulting from the negotiations with Allied governments after the Second World War, enshrined a separation between police and intelligence powers.[338] While police functions are mostly held by the *Länders*, intelligence powers are divided between the local and federal levels. Domestic intelligence services of the *Länders* have, however, more modest scope of responsibilities and capabilities.[339] As a result, the responsibility of domestic security is thus primarily shared amongst the Ministries of Home Affairs, both from the federal and *Länders* governments.[340] The Federal Ministry of the Interior, Building and Homeland Affairs (BMI) is responsible, among other things, for civil security in cyberspace.[341] The BMI coordinates the implementation of the cybersecurity strategy through the Federal Commissioner for Information Technology, who is also Chairman of the Cyber Security Council.

With regards to cybersecurity, the BSI has become over time the national cybersecurity authority as part of the BMI. Originally created in 1991 with the mission to guarantee the security of information technology through licences and certifications for IT systems, its mission subsequently extended as a result of multiple amendments in 2009, 2015 and 2017.[342] Most notably, the 2011 Cybersecurity Strategy for Germany has tailored the BSI to be at the centre of Germany's cybersecurity architecture and remain connected with all the cybersecurity authorities in the country.[343]

The Act on the Federal Office for Information Security (BSI Act) describes the extensive list of the BSI's missions, which are included at the end of this case study. Its responsibilities encompass several principal functions. The BSI is responsible for the certification and accreditation of information technology systems whose derived missions entail testing and evaluating security systems. As the competent authority for cybersecurity, the BSI also supervises the implementation of cybersecurity measures in Germany, notably from operators of critical infrastructures according to the 2015 IT security law (which amended the BSI Act). Therefore, these must take 'appropriate technical and organisational measures which comply with the state of the art against digital threats to protect their information technology systems, components and

[336] Schallbruch & Skierka (2018).
[337] Schallbruch & Skierka (2018).
[338] Federal Ministry of Justice and Consumer Protection (2019).
[339] Schallbruch & Skierka (2018).
[340] Schallbruch & Skierka (2018).
[341] Bundesminister des Innern (2020).
[342] Bundestag (1990).
[343] Bundesminister des Innern (2016).

processes.'[344] Unless they are able to prove to BSI they have taken sufficient measures in order to guarantee the cybersecurity of their systems, the BSI has the power to issue fines and complaints. Since the 2009 BSI Act, the BSI has also been responsible for the operational aspect of Germany's cybersecurity across the federal bodies to thwart nefarious actions against their networks. The resulting new missions for the BSI are to manage federal networks, probe into incidents and employ defensive action. With regards to operations, the BSI's jurisdiction has its boundaries within the federal network and is therefore not allowed to act beyond; in this realm, cooperation with *Länders*' police forces and enforcement authorities is required.[345] In light of the BSI Act, the BSI can also provide support for cyber defence to operators of critical infrastructures if they so demand.[346]

The Federal CERT is the emergency team and contact point for all German federal authorities in the event of a security-related IT incident. The Citizens CERT represents a warning and information service for private individuals who are informed about current security vulnerabilities. The Federal CERT is attached to the BSI and cooperates with the CERTs of the *Länders* within the framework of the CERT Network. The latter is a platform for the mutual exchange of information between the Federal CERT and the *Länders* CERT to strengthen IT crisis prevention and response of the public administration across all of Germany.[347]

As the main proponents of police functions, each of the 16 *Länders* has jurisdiction for prosecution of cybercrimes. The Federal Criminal Police Office (BKA) is the central body for German police at the national scale to gather and handle information.[348] In the realm of cyber, should attacks be directed towards federal government or critical infrastructure, the BKA is responsible to lead investigations.[349] It is not however mandated to forestall attacks.[350] Due to its counterintelligence purpose, the Federal Office for the protection of the Constitution (BfV) is also entitled to gather information on cyberattacks and can additionally support cyber defence.[351] Specifically, the BfV investigates on use of IT by extremists, terrorists or foreign intelligence services, for example, to carry out espionage, political disinformation or computer sabotage in Germany.[352] For defensive purposes, the BfV tries to thwart cyberattacks on state and private institutions, but in light of the aforementioned separation between intelligence and police functions, it does not hold any police powers and cannot apprehend attackers. Additionally, the Federal Intelligence Service (BND) is the foreign intelligence service of the Federal Republic of Germany and acts on behalf of the Federal Government.[353] The BND records attacks intended to serve cyber espionage or sabotage in Germany and warns affected actors so that defence mechanisms can be initiated.

[344] Section 8a of the 2009 Act on the Federal Office for Information Security.
[345] Schallbruch & Skierka (2018).
[346] Section 5a of the 2009 Act on the Federal Office for Information Security.
[347] Herpig & Beigel (2020).
[348] German Federal Criminal Police Office (n.d.).
[349] Federal Ministry of Justice and Consumer Protection (2017).
[350] Schallbruch & Skierka (2018).
[351] Federal Ministry of Justice and Consumer Protection (1990).
[352] Herpig & Bredenbrock (2019).
[353] Bundesnachrichtendienst (n.d.).

Cyber defence in Germany

Until 2014–2015, the German Armed Forces (Bundeswehr) had not developed its own cybersecurity policy, preferring instead to bring a defence contribution to cybersecurity policy developed by civilian authorities.[354] With the cyber domain becoming central in military activities and following the call for more cyber skills in the 2016 National Cyber Security Strategy, the Federal Ministry of Defence (BMVg) has fully integrated this aspect of security in its portfolio. Nowadays, the BMVg monitors the military defence of German cyberspace. As presented in its 2018 concept, the Bundeswehr[355]:

- Is in charge of the defence aspects of state-wide cybersecurity. The concept mentions large-scale asymmetric attacks, massive cyberattacks and complex cyberattacks. The Bundeswehr provides a military contribution with immediately reactive forces for cyber/IT situation management and crisis management in the event of attacks from cyberspace.
- Contributes to the state-of-the-art situation in cyber and information both at the national, multinational level, for example by providing skills for homeland security, national risk and crisis management as well as the development of national key technologies.
- Guarantees cybersecurity of the Bundeswehr's networks.

Within the Bundeswehr, the Cyber and Information Space (CIR) was established in April 2017 to integrate the necessary forces for operation management in cyberspace within a single unified organisational entity. In addition to the Army, Air Force and Navy, the new branch is responsible for the defence of the Cyber and Information Space in Germany. The Bundeswehr Cyber-Operations Centre (ZCO) represents the operational arm of the CIR, gathering all capabilities for the planning, preparation, conduct and execution of both defensive and offensive military cyber operations.[356]

In general, the German constitution distinguishes two regimes of action for the Bundeswehr. An intervention under the threshold of deployment, such as defensive measures to guarantee the cybersecurity of the Bundeswehr or the provision of assistance to the BSI, does not demand the approval of the German parliament beforehand.[357] On the other hand, cyber operations going beyond the Bundeswehr's network and impacting third parties, through coercion for example, are understood as deployment of military force and therefore require prior parliamentary approval.[358]

Interplay between cybersecurity authorities

The combined involvement of the federal and state level of German public administration – including civilian and military authorities in cyberspace – makes it often difficult to identify the relevant body responsible for specific cyber issues. In order to address this situation, two bodies were established by the 2011 German National Cyber Security Strategy: The National Cyber Security Council (Cyber SR) and the National Cyber Defence Centre (NCAZ).

[354] Schallbruch & Skierka (2018).

[356] Bundeswehr (n.d.).
[357] Schallbruch & Skierka (2018).
[358] Federal Ministry of Justice and Consumer Protection (2005).

The Cyber SR was created as a cross-institutional body where the different ministries, the Federal Chancellery and the *Länders* are represented to bring federal–state harmonisation in the cyber realm.[359] It ensures the coordination of the preventative tools and the multidisciplinary approaches for cybersecurity amongst the public authorities and with private stakeholders. The 2016 Strategy has further extended the mission of the Council to identify the long-term need for action and trends, strengthen cybersecurity and adopt the federal architecture for cybersecurity in Germany. Some studies suggest that the Cyber SR may be struggling to present itself as the federal–state coordinator in light of the functional overlap with the conference of interior ministers' cybersecurity working group[360] and its prominence.[361] Coordination between public authorities can also be hardened by the heterogeneity of *Länders*' own organisational structures, which vary from one to another. Additionally, while some states have cooperation agreements with the BSI on cybersecurity, others have created their own regional cybersecurity authority. For example, in 2017 Bavaria established its Office for Information Security[362] (LSI), which is competent to provide defence against threats to the state's IT network and systems.[363, 364] Overlapping with the BSI's functions, the LSI can also upon request, advise and support state and local authorities, public companies, operators of critical infrastructures and other facilities.[365]

With the aim of bringing more clarity into the complex distribution of power and responsibilities among authorities at the operational level, the NCAZ was created within the BSI as a joint information and exchange platform.[366] The NCAZ is designed to optimise operational cooperation between public authorities, as well as to coordinate appropriate protection and defence countermeasures to address incidents.

In case of an attack, the NCAZ presents the separation of powers and collaboration between authorities as the following:

- The BSI evaluates the attack from an information-technology perspective;[367]
- The BfV, the Military Counter-Intelligence Service (MAD) and the BND rate it from an intelligence perspective, while the BKA, the Customs Investigation Bureau (ZKA) and the Federal Police assess it from a police perspective;[368] and
- The BBK evaluates disaster preparedness and critical-infrastructure issues.[369]

However, literature has reported that in an unpublished report of 2014, the Federal Audit Office heavily criticised the NCAZ by expressing doubts on its ability to fulfil its missions.[370] The Federal Audit Office

[359] German Federal Ministry of Defence (n.d.).
[360] Innenminister Konferenz (n.d.).
[361] Schallbruch & Skierka (2018).
[362] Landesamt für Sicherheit in der Informationstechnik (n.d.).
[363] Bayerische Staatskanzlei (2015).
[364] See Article 10 (1) of the Law on electronic administration in Bavaria.
[365] See Article 10 (2) of the Law on electronic administration in Bavaria.
[366] Schallbruch & Skierka (2018).
[367] Bundesamt für Sicherheit in der Informationstechnik (BSI) (n.d.).
[368] Bundesamt für Sicherheit in der Informationstechnik (BSI) (n.d.)
[369] Schallbruch & Skierka (2018).
[370] Schallbruch & Skierka (2018).

in particular emphasised a lack of expertise and clear division of responsibilities, and questioned the result of cooperation amongst authorities in the NCAZ.[371] A more recent study in 2017, based on interviews with security representatives, presents the limited fulfilment by NCAZ of its missions as a weakness for cybersecurity in Germany.[372] It is also worth noting the puzzling absence of cooperation of NCAZ with private and critical infrastructure operators and the lack of linkages with the *Länders*.

C.2.3. Evaluation and performance

This case study did not identify any publicly available evaluation of the German cybersecurity system or its governance, nor how this compares to the Dutch equivalent's performance. However, a report from the European School of Management and Technology (ESMT) on the organisation of cybersecurity in Germany concluded that German cybersecurity policy suffers from several gaps that 'become apparent in international comparison and contrast with German officials' own claims that Germany's cybersecurity policy is strategically comprehensive'. Whereas the BSI has developed a strong position within the German cybersecurity ecosystem with its engineering-focused approach to national cybersecurity, unclear roles and responsibilities for other organisations often lead to their engagement into turf wars and an overall lack of progress.[373]

According to the ESMT report, German policymakers continue to predominantly view cybersecurity as preventive matter focused on securing IT. As a result, the authors highlight that the current German system focuses on the:

- Development of secure technologies;
- Dissemination of technical know-how;
- Technical and organisational security of critical systems;
- Legal obligation to and enforcement of protective measures; and
- Development of defensive capabilities and increased criminal prosecution in the field of cybercrime.

As such, the authors conclude that current German cybersecurity policy suffers from six key gaps or weaknesses:

1. A lack of clarity in the overarching institutional architecture for national cybersecurity, particularly in relation to the responsibilities, coordination and cooperation of the various security authorities.
2. The German approach does not clearly define the goal, scope and legal framework of 'active cyber defence' measures.
3. A lack of maturity in how to approach national IT security vulnerabilities.

[371] Herpig & Bredenbrock (2019).
[372] Zedler (2017).
[373] Schallbruch & Skierka (2018).

4. A lack of practical implementation concepts as to how to keep software manufacturers liable for vulnerabilities in their products.
5. A missing national industrial policy on cybersecurity to assist 'national sovereignty'.
6. A lacking role for Germany in international efforts to maintain peace and stability in cyberspace.[374]

Box 8 Mandate of the Federal Office for Information Security

(1) The Federal Office shall promote the security of information technology. To do so, it shall perform the following tasks:

1. Preventing threats to the security of federal information technology;
2. Gathering and analysing information on security risks and security precautions and providing the results to other authorities as needed for them to fulfil their tasks, and to third parties as needed for them to preserve their security interests;
3. Studying security risks involved in the use of information technology, and developing security precautions, especially information technology processes and devices for information technology security (IT security products) as needed by the Federation to fulfil its tasks, including research as part of its legally mandated tasks;
4. Developing criteria, procedures and tools to test and evaluate the security of information technology systems or components and to test and evaluate compliance with IT security standards;
5. Testing and evaluating the security of information technology systems or components and issuing security certificates;
6. Testing information technology systems and components and confirming compliance with IT security standards defined in the Federal Office's technical guidelines;
7. Testing, evaluating and approving information technology systems or components to be used in processing or transmitting official confidential information in accordance with Section 4 of the Security Clearance Check Act (SÜG) in the federal area or by companies in the context of federal contracts;
8. Producing key data and operating cryptography and security management systems for federal information security systems used to protect official confidentiality or in other areas at the request of the authorities concerned;
9. Providing support and advice on organizational and technical security measures and carrying out technical tests to protect confidential official information in accordance with Section 4 of the Security Clearance Check Act against unauthorised access;
10. Developing technical security standards for federal information technology and for the suitability of information technology contractors in special need of protection;
11. Making IT security products available to federal bodies;
12. Providing support for the federal bodies responsible for the security of information technology, especially where these bodies undertake advisory or supervisory tasks; support for the Federal Commissioner for Data Protection and Freedom of Information shall take priority and shall be

[374] Schallbruch & Skierka (2018).

provided in line with the autonomy granted the Federal Commissioner in carrying out his/her tasks;

13. Providing support for:

- The police and prosecution authorities in carrying out their legally mandated tasks.
- The authorities for the prosecution of the Constitution and the Military Counterintelligence Service in analysing and evaluating information derived from surveillance of terrorist activities or from intelligence activities as authorized by federal and state law and the Law on the Military Counterintelligence Service.
- The Federal Intelligence Service in carrying out its legally mandated tasks.

This support may be provided only where necessary to prevent or investigate activities directed against the security of information technology or activities carried out using information technology. The Federal Office shall keep a record of requests for support;

13a. Upon request of the competent *Länder* bodies, supporting these bodies in connection with the prevention of threats to the security of information technology; upon request of the competent *Länder* bodies, supporting these bodies in connection with the prevention of threats to the security of information technology;

14. Advising and warning federal and *Länder* bodies as well as producers, distributors and users with regard to the security of information technology, keeping in mind the possible consequences of the lack of security precautions or of inadequate security precautions;

15. Creating appropriate communications structures to recognize crises at an early stage, respond and manage crises and to coordinate efforts to protect the security of information technology of critical infrastructures in cooperation with private industry;

16. Tasks as central body for the security of information technology with regard to the cooperation with foreign competent bodies, without prejudice to special competences of other bodies;

17. Tasks in accordance with Sections 8a to 8c as central body for the security of information technology of critical infrastructures and digital services;

18. Providing support in the restoration of the security or functionality of information technology systems in outstanding cases pursuant to Section 5a.

(2) The Federal Office may assist the *Länder* in securing their information technology upon request.

(3) The Federal Office may advise and support operators of critical infrastructures in securing their information technology upon their request or refer them to qualified providers of security services.

Source: Bundestag (2009).

C.3. Sweden

C.3.1. Background

Sweden unveiled its first national cybersecurity strategy in 2017 in an effort to establish a roadmap for its long-term cybersecurity efforts. The document presents the Swedish government's overarching priority

areas and associated objectives, as well as further guidance to achieve these priority areas.[375] The strategy contains six overarching strategic priorities[376]:

1. Securing a systematic and comprehensive approach in cybersecurity efforts;
2. Enhancing network, product and system security;
3. Enhancing the capability to prevent, detect and manage cyberattacks and other IT incidents;
4. Increasing the possibility of preventing and combating cybercrime;
5. Increasing knowledge and promoting expertise; and
6. Enhancing international cooperation.

The strategy is also accompanied by an implementation plan, which is discussed in more detail below.[377]

Within a legislative context, key legislation in relation to cybersecurity includes the Protective Security Act and the implementation of the EU NIS Directive. The Protective Security Act, originally implemented in 1996 and updated in 2018, sets multiple provisions dedicated to protective security, notably with regards to espionage, sabotage, terrorism and other crimes that might endanger national security.[378] Law 2018:1174 'Information Security regarding Providers of Critical Infrastructure and Digital Services' implemented the NIS Directive within Swedish law, and seeks to achieve a higher common level of security of network and information systems in compliance with EU regulation.[379]

C.3.2. Overview of governance approach

This section provides an overview of the governance approach, the main cybersecurity organisations and their roles and responsibilities. Sweden's cybersecurity governance has its foundation in its crisis-management structure, and was historically seen as a non-military aspect of national defence and security.[380] As such, the Ministry of Justice (MOJ – *Justitiedepartementet*) and the Civil Contingencies Agency (MSB) are the most important governmental entities responsible for cybersecurity.

Within the cybersecurity context, the MOJ is responsible for developing cybersecurity policy and regulation to guarantee the security and well-functioning of Swedish society. The MOJ also coordinated the development of the National Cyber Security Strategy and has an overall 'catch-all' role for digital security in Sweden.[381] The MOJ oversees multiple agencies with cybersecurity responsibilities, including the MSB, the Swedish police authority (in charge of cybercrime law enforcement investigations); the Swedish Security Service (SÄPO) (responsible for identifying and thwarting offences against national security, the fight against terrorism and guaranteeing the central government's protection); and the Swedish Data Protection Agency.[382] However, the Swedish governance model is decentralised and

[375] Swedish Ministry of Justice (2017).
[376] Swedish Ministry of Justice (2017).
[377] Swedish Civil Contingencies Agency (2019).
[378] Government of Sweden (2018).
[379] Swedish Government Offices (2018).
[380] OECD (2018).
[381] OECD (2018).
[382] OECD (2018).

distributed with individual 'lead' ministries primarily in charge of a particular policy area. Within this model, there is also a significant amount of delegated power to the operational government agencies and authorities, which are responsible for carrying out government policy. As such, the MOJ works in a cooperative and collaborative manner given that it cannot command a government agency in the jurisdiction of another ministry. There are therefore cybersecurity responsibilities distributed across several ministries, departments and organisations, as highlighted below.

From a societal perspective, the MSB is the main coordinator of national cybersecurity. The MSB's roles and responsibilities cover a spectrum of activities, including crisis management, public safety and civil defence. In relation to cybersecurity, the MSB is responsible for crisis and incident response, the provision of information and guidance, and other cybersecurity services, including the Swedish national Computer Security Incident Response Team (CSIRT) CERT-SE. It is worth noting that the MSB holds operational capacity only through CERT-SE and apart from that, its role is limited to an advisory and coordinating capacity.

In summary, the main government organisations with cybersecurity responsibilities include[383]:

- **The Civil Contingencies Agency** (MSB)*:* The MSB's overarching responsibility is the coordination of national cybersecurity efforts. It also maps and examines society's cybersecurity efforts, for instance within Swedish municipalities and regions.
- **The Swedish Post and Telecom Authority** (PTS): The PTS monitors the areas of electronic communication and mail in Sweden. The authority's tasks include promoting access to secure and efficient electronic communications, which include telecommunications, Internet and radio. The PTS also engages with the private sector through multiple activities dedicated to cybersecurity to bolster network security robustness.
- **The Agency for Digital Government** (DIGG)*:* DIGG's mission is to coordinate and support the digitalisation of public administration to make public administration more efficient and effective.
- **The Swedish Data Protection Authority**: The Swedish Data Protection Authority is the regulatory authority responsible for data integrity and protection.
- **The Swedish Armed Forces**: The Swedish Armed Forces have tasks in the area of cyber defence and information security in support of national security in relation to secure cryptographic functions, security protection and signal protection.
- **The Swedish Defence Materiel Administration** (FMV)*:* FMV has carried out evaluations of IT products and systems since the end of the 1980s within its own organisation, and has long been actively involved in international standardisation work on information security.
- **The National Defence Radio Establishment** (FRA): FRA has two core areas of responsibility – information security and signal intelligence services.

In light of the multidisciplinary nature and development of cybersecurity, the Swedish government established the Cooperation Group for Information Security (SAMFI) to fuel effective collaboration

[383] Swedish Civil Contingencies Agency (n.d.).

between government authorities. To this end, SAMFI gathers the MSB, FMV, FRA, Swedish Armed Forces, Swedish Police Authority, PTS and Swedish Security Service.[384] SAMFI deals with a range of cybersecurity issues, including:

- Strategy, action plan and regulations;
- Technical issues and standardisation issues;
- National and international development in the field of information security;
- Information activities;
- Exercises and training; and
- Management and prevention of IT incidents.

The MSB allocates resources for a SAMFI office and other SAMFI authorities contribute resources when needed and according to ability.[385]

In addition to SAMFI, the National Cooperative Council against Serious IT Threats (NSIT), a collaborative platform set up in 2014, is responsible for analysing and evaluating threats and vulnerabilities in the light of serious cyberattacks against Sweden's security-sensitive national interests. The NSIT is composed of the Swedish Security Service, FRA and Swedish Armed Forces through its Military Intelligence and Security Service (MUST).[386]

Implementation of the National Cyber Security Strategy

The 2017 National Cyber Security Strategy contains the government's overarching priorities and aims to provide a platform for Sweden's continued development within cybersecurity, as well as to help create the long-term conditions for all stakeholders in society to work efficiently (i.e. central government authorities, municipalities and county councils, companies, organisations and private individuals).

The strategy was followed up with specific instructions to relevant government agencies to ensure the implementation of the strategic priorities. The implementation of the strategy aligns with Sweden's distributed governance model, in which each agency is responsible for implementation within their area of responsibility. Similarly, the overall implementation is coordinated by SAMFI, rather than led by a single or central organisation. The overarching logic is that continued in-depth collaboration between the SAMFI authorities is a prerequisite for strengthening Sweden's ability to protect against cyberattacks and other serious IT incidents.

As noted above, the strategy implementation process is coordinated through a joint action plan developed by the SAMFI organisations.[387] The plan comprises more specific implementation actions that fall within the scope of the responsibilities and mandates of each of the agencies involved. The action plan provides the government with evidence to be able to analyse and assess whether current measures are sufficient to

[384] Swedish Civil Contingencies Agency (2015).
[385] Swedish Civil Contingencies Agency (2015).
[386] Swedish Ministry of Justice (2017).
[387] Swedish Civil Contingencies Agency (2019).

achieve the objectives of the national strategy and what further measures the government may need to take.[388]

However, the action plan should not be seen as a complete account of all the measures that the various authorities intend to implement in relation to cybersecurity (i.e. there may be additional work outside the action plan). All measures in the action plan connect to one or some of the six strategic priorities. with most of the measures relating to[389]:

1. Securing a systematic and comprehensive approach in cybersecurity efforts;
2. Enhancing network, product and system security; and
3. Enhancing capability to prevent, detect and manage cyberattacks and other IT incidents.

The action plan shows which authority is responsible for each measure, who participates in the work and what the measure covers. The measures are typically implemented within a given financial framework, either individually by one of the SAMFI organisations or in joint projects.[390] The implementation of the national strategy is therefore a clear example of the decentralised and distributed governance model in action, in which multiple agencies coordinate and cooperate within their remits and available financial frameworks.

The development of a Swedish national cybersecurity centre

Building on the National Cyber Security Strategy, the government further tasked the MSB, FRA, Swedish Armed Forces and Security Police to develop a plan to set up a national cybersecurity centre in 2020. The government recognised that cyber threats against Sweden and Swedish interests are extensive and that additional steps must be taken to ensure Sweden's security, going beyond the organisational structures that were then in place.[391]

In response to this request, the four agencies published a draft concept and implementation plan for a national cybersecurity centre in December 2019. The draft plan for the national cybersecurity centre articulated the envisioned objectives for the centre to[392]:

- Provide coordination of abilities to prevent, detect and manage cyberattacks and other IT incidents to make Sweden safer within the cyber domain;
- Ensure that authorities can act seamlessly, increasing the operational capacity of each agency to effectively support public and private actors; and
- Strengthen Swedish cyber defence overall.

One of the main perceived benefits of the national cybersecurity centre is to enable the sharing of information and knowledge between government organisations so that each authority can fulfil its task in a more efficient way. This means that the national cybersecurity centre is not intended to assume the

[388] Swedish Civil Contingencies Agency (2020).
[389] Swedish Civil Contingencies Agency (2020).
[390] Swedish Civil Contingencies Agency (2020).
[391] Swedish Ministry of Defence (2019).
[392] Swedish Security Police (2019).

tasks, mandate or capacity of the constituent authorities. Rather, joint work through the centre will help to unify the national cybersecurity effort, thereby reducing current fragmentation.[393]

The work of the centre at full operating capability (FOC) is expected to lead to:

- Shorter lead times from detection to action;
- Better analysis of results, with a greater exchange of information;
- Increased clarity in messages and recommendations;
- Increased accessibility to the participating authorities for both private and public target groups;
- Strengthened private–public collaboration;
- Unified national cybersecurity work and harmonisation of regulation and protective measures; and
- More efficient use of government resources.

At FOC, the target audience for the centre is expected to be:

- Government organisations;
- Municipalities and county councils;
- Regional organisations, such as Sweden's Municipalities and Regions (SKR); and
- Private-sector organisations in priority sectors (e.g. critical infrastructure sectors, defence, etc.).

However, the centre is not expected to provide all the above services to all constituents at the initial operating capability (IOC). At the IOC stage, the centre will focus on compiling and analysing information relating to threats, vulnerabilities and risks; disseminating information between participating authorities and other actors; and coordinating the incident-response work.

As the overarching logic of the national cybersecurity centre is that the work of the centre will strengthen the authorities' ability to better deliver their respective tasks, each authority is expected to contribute to the centre's activities according to its own ability and budget.[394] The initial governance and set-up of the centre has been developed as part of the concept plan, but the constituent authorities acknowledge that the full organisational and governance structure should be developed following an in-depth study.

At this stage, it is envisioned that the centre will be governed on three levels:

1. A strategic steering group consisting of the highest manager, or the person appointed by the manager, for the authorities that contribute personnel resources (i.e. the MSB, FRA, Swedish Armed Forces and Security Police) will provide strategic direction for the long-term development of the centre.
2. Short- and medium-term management will be the responsibility of an operational steering group consisting of representatives from departments affected by the centre's activities, from the respective authorities.

[393] Swedish Security Police (2019).
[394] Swedish Security Police (2019).

3. Day-to-day operations will be led by a manager and a deputy manager. The manager shall be appointed by the strategic steering group for a time-limited appointment, and both positions should ideally be filled by candidates from the participating authorities.

For support, the strategic and operational steering groups will each have a council consisting of representatives from the public and private sectors. In the short term, the centre is expected to host up to 20–30 people, mostly seconded from the participating authorities. At FOC, the centre is expected to host around 250 people. The joint working to set up the national centre was expected to begin in early 2020, at one of the MSB's premises in Stockholm.[395]

C.3.3. Evaluation and performance

There is not yet any publicly available evaluation of the current cybersecurity effort in Sweden, not least as the national cybersecurity strategy is still in implementation and the national cybersecurity centre is still to be set up. However, the recent revamp of the national cybersecurity effort was to a degree undertaken in response to deficiencies identified by past inquiries and reviews of Swedish cybersecurity and government cybersecurity arrangements. These reviews particularly included reports by the Swedish National Audit Office (NAO) of cybersecurity arrangements in public administration, the latest of which was published in 2016. The findings of the 2016 review are summarised below.

The purpose of the 2016 audit was primarily to investigate and assess the cybersecurity arrangements in nine public sector agencies. The nine agencies were chosen as they conduct critical infrastructure activities, handle large amounts of money, are strongly IT-dependent and handle sensitive information that requires protection. The secondary objective of the audit was to examine whether the Swedish government efficiently supports and ensures that the agencies have effective internal control for cybersecurity. The audit included the Public Employment Service, the Migration Agency, the National Grid, the Social Insurance Agency, the Companies Registration Office, the Maritime Administration, the Land Registry, the National Government Employee Pensions Board and the PTS.[396]

The overall audit conclusion by the NAO was that the cybersecurity arrangements of the nine agencies fell considerably short of being adequate. Several underlying causes for this were identified, including[397]:

- **The importance of adequate cybersecurity arrangements was in general far too limited**, which resulted in cybersecurity not being prioritised adequately in relation to the risks posed. The NAO emphasised that this applied both to the government, which was found not to emphasise sufficiently the importance of cybersecurity, and to the agencies' management, who did not give priority to cybersecurity to the extent required.
- **There was a general lack of systematic cybersecurity** work in line with the requirements of the Civil Contingencies Agency's regulations on government agencies' cybersecurity. The emphasis on systematic cybersecurity efforts has since been developed into an integral part of the national cybersecurity effort and the national strategy.

[395] Swedish Security Police (2019).
[396] Swedish National Audit Office (2016).
[397] Swedish National Audit Office (2016).

- **There was a lack of senior management support and issues with delegated responsibilities**. The audit identified that senior managers often did not give adequate support to cybersecurity efforts or delegated the responsibilities to individuals that may not have an adequate mandate within the organisation, or sufficient resources, to carry out those tasks.
- **There was a lack of follow-up and detailed knowledge**. Several agencies were found to have cybersecurity policies, guidelines or manuals, but overall, the audit found that awareness of the contents and purpose of these resources was low among employees and managers. The audit also noted that developing a coherent picture of the cybersecurity arrangements was challenging, as there was often no structured follow-up of the cybersecurity management system and its impact.
- **There was heterogeneity in the cybersecurity effort**. Lastly, the NAO noted that the cybersecurity work across the audited agencies was conducted in many different ways, despite the fact that significant components of this work should have been generic by nature. The audit thus showed a greater need for harmonisation of approaches taken by the agencies.

Given the nature of the audit findings, the NAO concluded that it is likely that the weaknesses identified in the nine agencies audited would also apply to most other public administration agencies in Sweden. Within this context, the NAO concluded that stronger governance was required from the government so that necessary cybersecurity measures are actually implemented, monitored and evaluated. According to the NAO, the audit clearly showed that simply developing a regulatory framework or structure is not sufficient to help public administration agencies achieve cybersecurity.[398]

Lastly, the NAO noted the difficulties in determining whether or not decisions taken on cybersecurity are well-informed and well-founded. The NAO found that reviewers would need a more coherent view of the threats, risks and suitable measures and the size of the annual budget spent on cybersecurity to be able to assess the costs and benefits of national cybersecurity. According to the NAO, it is not possible to achieve an optimum level of cybersecurity in central government as a whole without these components.[399]

C.4. United Kingdom

C.4.1. Background

The United Kingdom adopted its first national strategy in 2009, the *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space*,[400] followed by a second strategy for the period 2011–2015, *The UK Cyber Security Strategy – Protecting and Promoting the UK in a Digital World*.[401] However, the third strategy launched in 2016 marked a landmark shift in the UK's cybersecurity policy, and also forms the current framework detailing the UK's objectives for its national cybersecurity policy. The *National Cyber Security Strategy 2016–2021* set out the government's vision for the UK to be secure

[398] Swedish National Audit Office (2016).
[399] Swedish National Audit Office (2016).
[400] Cabinet Office (2009).
[401] BIS et al. (2011).

and resilient to cyber threats, and prosperous and confident in the digital world.[402] The vision is accompanied by three overarching objectives:

1. **Defend**: Achieving the means to defend the UK against evolving cyber threats, respond to incidents and ensure the resilience and protection of UK networks, data and systems. This objective also encompasses the ability for citizens, businesses and the public sector to defend themselves.
2. **Deter**: Ensuring that the UK is resilient to all forms of aggression in cyberspace by achieving the ability to detect, understand, investigate and disrupt hostile action, along with pursuing and prosecuting offenders and thereby holding offenders accountable. This objective also includes the ability to employ offensive capabilities in cyberspace.
3. **Develop**: Investing in sustainable development and retainment of skills in the public and private sectors, and encouraging innovation in the cybersecurity industry underpinned by world-leading scientific research and development, which will help to meet and overcome future threats and challenges.[403]

These overarching objectives are further supported by an underpinning ambition for international action to exert the UK's influence and invest in partnerships that help the UK to shape the global evolution of cyberspace aligned with the UK's economic and security interests.[404] The 2016–2021 national strategy was predominantly an interventionist strategy with a key role for central government, seeking to simplify the UK government's approach to cybersecurity and promote national and global partnerships. The strategy was accompanied by an implementation programme (the National Cyber Security Programme) and a total investment of £1.9 billion across the strategy period.

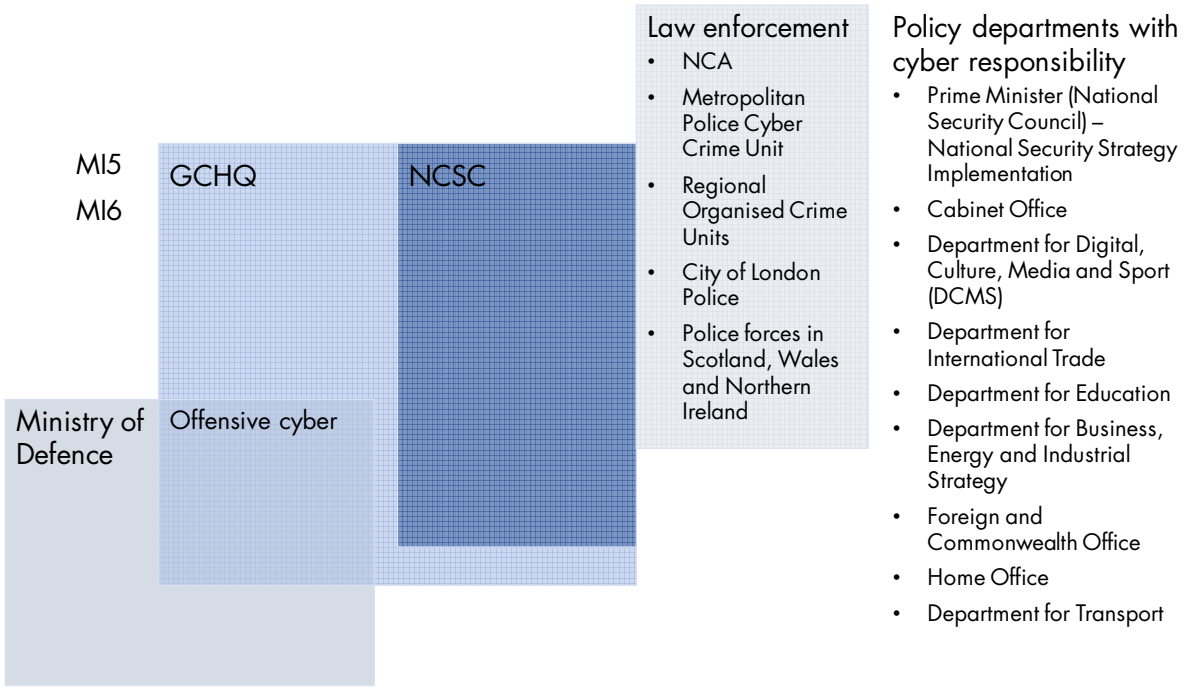
C.4.2. Overview of governance approach

Several organisations in the UK have some degree of cybersecurity responsibility (as seen in Figure C.4.1), which can largely be structured around three tenets:

- **Policy coordination, development and implementation**, which largely rests with the Cabinet Office;
- **National security and intelligence**, which largely rests with the Government Communications Headquarters (GCHQ) and the UK NCSC; and
- **Cyber defence**, which is led by the MOD.

[402] HM Government (2016).
[403] HM Government (2016).
[404] HM Government (2016).

Figure C.4.1 Overview of the UK cybersecurity ecosystem



Source: RAND Europe based on Hannigan (2019).

The main cybersecurity responsibility from a national security perspective lies with the UK NCSC, which was set up as a single body to act as national cybersecurity authority through the *National Cyber Security Strategy 2016–2021*. Since its establishment, it is responsible for monitoring national cyber incidents, sharing knowledge through practical guidance and tackling systematic vulnerabilities. The following section presents a brief history of how the UK NCSC came to be and illustrates the underlying rationale for the UK's centralised governance structure.

The journey to the UK NCSC

As part of the first UK national cybersecurity strategy in 2009, the UK government established an Office for Cyber Security (OCS) in the Cabinet Office to take overall ownership of strategy implementation and provide strategic leadership for cybersecurity across central government. Additionally, the government established a Cyber Security Operations Centre (CSOC) at GCHQ, building on the expertise found in its information assurance department, the Communication-Electronics Security Group (CESG). The objective was to provide situational awareness and technical response to cyber incidents.[405] These first steps towards establishing a governance structure for national cybersecurity highlighted several problems common to many countries, particularly the large number of government organisations with some degree of cybersecurity responsibility. Within the UK, some 15 central government departments and security agencies saw themselves as having a key role within cybersecurity. These organisations sought to provide advice and assistance to government, business and individual citizens; however, few of them had adequate

[405] Cabinet Office (2009).

technical expertise to do so effectively. Additionally, it was still unclear which organisation was ultimately responsible for responding to any given cybersecurity incident.[406]

These concerns formed part of the original rationale for centralisation and led to the development of a potential central authority on cybersecurity, which was first recommended in 2014–2015. In the meantime, several other cybersecurity organisations had been established during this period, including:

- The cyber missions of the Centre for the Protection of National Infrastructure (CPNI);
- The Centre for Cyber Assessment (CCA), formerly responsible for drawing cyber threat assessments to the attention of UK governmental departments;
- The Cyber Security Information Sharing Partnership (CiSP); and
- The Computer Security Incident Response Team in the UK (CERT-UK).[407].

The election of a new government in 2015 and an increasing recognition that the current approach was not producing sufficient results for national cybersecurity culminated in discussions for the next phase of UK national cybersecurity. These discussions were centred around two core tenets: a single source of expert national advice (including major-incident response and handling and threat information-sharing) and practical measures to strengthen UK cybersecurity. The latter part was formative in developing the UK NCSC's Active Defence Programme, which is discussed in further detail below.[408]

The original discussions also included the possibility to create a coordination body, while leaving the overall control with each responsible ministry (similar to the Dutch governance model), but this was ultimately abandoned as it was perceived as not being able to meet the stated ambition.[409] Instead, the decision was taken to set up a national centre under GCHQ that would subsume CERT-UK, the CCA, the CPNI cyber team and other functions.[410] The only exception to this centralisation was law enforcement, as shown in Box 9, which serves as a useful example of how cyber governance approaches emerge from pre-existing governance structures.

[406] Hannigan (2019).
[407] ICO (2020).
[408] Hannigan (2019).
[409] Hannigan (2019).
[410] Hannigan (2019).

Box 9 UK NCSC and law enforcement as an example of cyber governance emerging from pre-existing governance structures

Policing and prosecuting authorities are independent in the UK, and it was therefore acknowledged that it would be impossible and inappropriate to place law enforcement within the UK NCSC. However, there was also a recognition that most cyberattacks are a crime of some sort, with significant involvement of organised criminals, so completely excluding law enforcement from the UK NCSC made little sense.

Instead, the National Crime Agency (NCA), the Metropolitan Police and other law enforcement organisations invested in their own cybercrime structures. The UK NCSC and NCA then worked to set up a mutually reinforcing relationship that led to a close link between the NCA and UK NCSC, without placing the NCA under the UK NCSC11111 command structure.[411]

The role of the UK NCSC

The UK NCSC is the authority responsible for cyber incidents at the national level, and for ensuring a coordinated response to threats. At present, the UK NCSC works to:

- Understand cybersecurity and distil this knowledge into practical and openly available guidance;
- Respond to cybersecurity incidents to reduce the harm they cause to organisations and the wider UK;
- Use industry and academic expertise to develop the UK's cybersecurity capability; and
- Reduce risks to the UK by securing public and private sector networks.[412]

In the light of these missions, the UK NCSC has become an authoritative voice and centre of expertise on cybersecurity that delivers tailored support and advice to public sector organisations and businesses. The UK NCSC also plays the role of a single point of contact for European countries as the UK's CSIRT.

The UK NCSC is also responsible for several cybersecurity products and services, including:

- **Cybersecurity skills and education**, consisting of working with industry, government and academia to support the next generation of UK cybersecurity researchers, students and cybersecurity professionals.
- **Cybersecurity standards**, including Cyber Essentials, a cybersecurity scheme to help governmental organisations to select suppliers that meet minimum cybersecurity requirements.
- **Certification services**, where the UK NCSC provides certification for private-sector consultancy and professionals, and skills development through certified training. The UK NCSC also offers certification of commercial products through certified product assurance.
- **Security assessment services**, including the UK NCSC CHECK penetration testing, tailored assurance schemes, and cyber-incident response and recovery facilitation.[413]
- **Information-sharing services**, including the Cyber Security Information Sharing Partnership (CiSP), which is a joint industry and government initiative for real-time exchange of cyber threat information.[414]

[411] Hannigan (2019).
[412] NCSC-UK (n.d.a).
[413] NCSC-UK (n.d.b).

Although the UK NCSC has a wide range of roles and responsibilities, the original plans for setting up the centre tried to resist attempts to add certain responsibilities, particularly in relation to education and skills, and cybersecurity regulation. While the UK NCSC has an active role in developing skills within the UK, the national policy leadership was judged to be best placed at the relevant ministry, which in this case was the Department for Digital, Culture, Media and Sport (DCMS). Similarly, regulation was also left outside the UK NCSC, as it was perceived to be best suited for sectoral bodies with an understanding of the appropriate domain. There were also concerns that if the UK NCSC had a regulatory role, industry would be less willing to engage with the UK NCSC and share information, which was contradictive to the centre's main mission.[415]

In addition to the work outlined above, the UK NCSC also works proactively to strengthen technical cybersecurity through the Active Defence Programme (ACD).

The Active Defence Programme

Part of the Centre's work includes the progression and implementation of security measures to render digital infrastructures firmer in face of threats. The UK NCSC's ACD programme seeks to 'protect the majority of people in the UK from the majority of the harm caused by the majority of the cyberattacks the majority of the time'.[416] The programme consists of a set of seven tools and services provided free of charge to UK central government and some public sector organisations:

1. **Protective Domain Name System** (PDNS) – A secure DNS service for the public sector.
2. **Web Check** – A service that helps organisations proactively identify and fix common web vulnerabilities.
3. **Mail Check** – A platform for assessing email security compliance that collects, processes and analyses DMARC reports from across the public sector.
4. **Host Based Capability (HBC)** – A software agent to detect malicious activity on UK government endpoints.
5. **Logging Made Easy (LME)** – A service to help organisations set up basic logging capability to enable routine end-to-end monitoring of their Windows-based IT systems.
6. **Exercise in a Box (EiaB)** – A framework for running cybersecurity exercises for the government.

[414] NCSC-UK (n.d.c).
[415] Hannigan (2019).
[416] See NCSC-UK (n.d.d).

7. **Vulnerability Disclosure** – The provision of vulnerability reporting and vulnerability disclosure services.[417]

C.4.3. Evaluation and performance

House of Commons Committee of Public Accounts Review on UK Cybersecurity

In 2019, the House of Commons Committee of Public Accounts conducted a review of cybersecurity in the UK, which included an evaluation of the National Cyber Security Strategy 2016–2021, and recommendations for the future. The main findings and recommendations of the report were that:

- **The UK remains vulnerable to cyberattacks** – The government should ensure that a long-term coordinated approach to cybersecurity will be in place before the current National Cyber Security Strategy runs out in 2021.
- **The current approach to cybersecurity does not demonstrate value for money** – The National Cyber Security Strategy and the National Cyber Security Programme did not include a business case. Instead, each of the 12 programme objectives included individual business cases. This causes difficulties in measuring overall VFM, so the future strategy should include an overall business case.
- **The current approach to cybersecurity is not based on a robust evidence base** – The Cabinet office reported to have 'high confidence' in its evidence base to measure progress of one strategic outcome (incident management), but 'low confidence' in its evidence base to measure progress of the remaining 11 strategic outcomes. In implementing the National Cyber Security Strategy and the Programme, there was a lack of an appropriate and robust 'lessons learnt' exercise based on the previous National Cybersecurity Strategy (2011–2016). Any future approach to cybersecurity should be based on such a 'lessons learnt' exercise of the present strategy.
- **The National Cyber Security Strategy 2016–2021 did not clearly state what it aimed to deliver** – The Cabinet Office claimed it did not intend to deliver all 12 strategic outcomes by the end of 2021, while performance indicators suggest only three of the 12 objectives are currently being achieved. No progress updates have been published despite the Cabinet Office committing to annual reports in the strategy. Clarifications around what the strategy should be expected to deliver by 2021, complete with risk assessments showing why some objectives might not be met, should be made.
- **The current approach to cybersecurity has been insufficient in enhancing the security of the digital economy and protecting consumers –** Although some progress has been made in this area, it remains difficult for consumers to know whether their Internet-enabled devices and online-stored data are safe; more transparency vis-à-vis the consumer is needed, which will

[417] NCSC-UK (n.d.d).

enhance individual cyber resilience. The government should continue to focus on developing basic cybersecurity guidelines and should collaborate with large organisations to implement basic cybersecurity down the supply chain.[418]

To conclude, the lack of an overall business case for the National Cyber Security Strategy and Programme, along with the weak evidence base on which they were constructed, means the evaluation was unable to comprehensively assess its performance, determine appropriate VFM, or predict whether all relevant objectives would be met by 2021. An improved performance measurement process was recommended, along with continued and improved efforts to ensure the security of the digital economy and adequately protect customers.[419]

National Audit Office (NAO) Progress Report

In 2019, the NAO produced a progress report on the National Cyber Security Programme, with the goal of determining whether the Cabinet Office had been effectively coordinating the programme and whether the Programme is contributing to the National Cyber Security Strategy's overarching strategic objectives.[420] In evaluating the Programme, the NAO identified several of the same problems also mentioned by the House of Commons Committee of Public Accounts Review on UK cybersecurity, presented in the section above. More specifically, the NAO progress report noted:

- **The Programme did not include an overall business case**, resulting in difficulties in assessing whether funding was appropriate, and whether the Programme produced VFM.
- **The Programme might not deliver all 12 strategic objectives on time**, with only three (those related to 'incident management', 'active cyber defence' and the 'international' approach) currently progressing as required. Eight of the remaining objectives are expected to be achieved in proportion of 80 per cent, while the ninth, which is related to 'national critical infrastructure', is expected to be achieved in proportion of less than 80 per cent. Furthermore, the report noted that funding for the remainder of the programme lies below the recommended level, which might further impact the delivery of objectives by the end of 2021.
- **The Programme does not have a robust evidence base**, which does not allow the Cabinet Office to prioritise the objectives and activities that deliver the biggest impact, address the greatest needs and demonstrate the best value for money. This is because the Cabinet Office only introduced a robust performance framework to measure the Programme and the Strategy's performances in 2018, while also demanding that lead departments spend more time and resources on measuring progress at the individual project level.[421]

At the same time, the NAO report noted that one of the prominent successes of the Programme has been the establishment of the UK NCSC in 2016. The UK NCSC has played the main role in the Programme's ability to reduce the UK's vulnerability in cyberspace. For example, by developing tools to

[418] House of Commons Committee of Public Accounts (2019).
[419] House of Commons Committee of Public Accounts (2019).
[420] NAO (2019).
[421] NAO (2019).

counter phishing, the UK NCSC reportedly contributed to the reduction of the UK's global phishing attacks from 5.3 per cent to 2.2 per cent in two years.[422]

Regarding the UK's National Cyber Security Strategy, the NAO report noted that it is unclear whether the Strategy will achieve its strategic outcomes on time. The Cabinet Office remains in charge of coordinating the delivery of the Strategy, but the overall outcomes depend on the delivery of the Programme's objectives and related projects by the lead departments, on the contributions and cooperation of organisations and individuals outside government, and on other government expenditure. As a result, due to this diffusion of responsibility, along with the complex and constantly evolving nature of cyberspace and the fact that the question of whether the funding was adequate cannot be established, the Cabinet Office cannot carry out an accurate risk assessment to determine whether the outcomes will be achieved on time.[423]

To conclude, despite improvements and achievements, both the Programme and the Strategy were set up without an appropriate evidence base to serve decision making on resource allocation and to measure progress. As a result, neither can demonstrate VFM, and both risk failing to deliver all objectives and outcomes in time.[424] As a result, the NAO review offered several recommendations to help the Cabinet Office build on this experience and guide a smooth transition from the end of the Programme and Strategy in 2021 to future activities:

- **The Cabinet Office needs to establish which areas of the Programme address the most significant threats and/or vulnerabilities or have the greatest impact**. This assessment should then be used in the adequate (re)allocation of resources within the current Programme, as well as contribute to a business case for a future Programme.
- **The Cabinet Office should continue to communicate and cooperate with government departments and public sector bodies to understand cybersecurity vulnerabilities and priorities across the board**. This will ensure an adequate understanding of the cybersecurity landscape, as well as contribute to a business case for a future Programme.
- **The new Strategy should cement the central role of the government, as well as set out clear divisions of responsibility** in collaborating with both the public and the private sectors.
- **The Cabinet Office should consider a more flexible approach to cybersecurity**. A combination of shorter programmes that are more responsive to changing vulnerabilities and threats, and longer term investment in areas such as skills development, could be the best approach.[425]

NCSC Evaluation of the Active Cyber Defence Programme

The UK NCSC has published annual reviews of the ACD Programme, which aims to raise the cost of commodity cyberattacks against the UK. The reviews are part of a process of ensuring that the services provided through the ACD Programme are evidence based. Transparency regarding the level of

[422] NAO (2019).
[423] NAO (2019).
[424] NAO (2019).
[425] NAO (2019).

effectiveness of its various work strands is further aimed at building an evidence base that can be used by multiple organisations to increase the speed and efficiency with which they adopt cybersecurity measures to target any relevant vulnerabilities.[426]

Among several services provided, the evaluation reported on progress on the aforementioned areas:

- **Protective Domain Name System (PDNS)** – The PDNS service proved to provide a protective effect at the scale needed by the customer. New features due to be introduced in 2019 were expected to improve the service by enabling it to provide customers with enhanced actionable intelligence and, as a result, an increased cybersecurity benefit.
- **Web Check** – The number of unique URLs more than tripled from 2017 to 2018, suggesting an increase in users of the Web Check database. The checks introduced in 2017 continued to produce advice requiring action, while the new checks introduced in 2018 provided new insights for users.
- **Mail Check** – The number of public sector domains using DMARC increased from 412 at the end of 2017 to 1,369 at the end of 2018. Furthermore, the number of domains with a DMARC policy that actively prevents suspicious emails from being delivered to recipients' inboxes increased from 192 to 572 in the same time period. This suggests a significant increase in the adoption of email security protocols. However, the evaluation underlines that more actions need to be implemented to further increase adoption of stronger DMARC policies, across both the public and private sectors.
- **Host Based Capability (HBC)** – As part of the ACD Programme pilot, this service was deployed to 26,000 government devices across five departments. As a result, seven incidents were identified and 15 'Threat Surface Reports' submitted to network owners. In 2019, this service was due to further expand in the public sector.
- **Logging Made Easy (LME)** – This was due to be launched in 2019.
- **Exercise in a Box (EiaB)** – The first cybersecurity exercises were primarily designed to help small- and medium-sized enterprises and local government agencies to research incident management plans. They were due to be launched in 2019.
- **Vulnerability Disclosure** – The service began in November 2018 and resulted in 11 submissions in November (of which ten were resolved) and 27 submissions in December (of which 19 were resolved).[427]

To conclude, the evaluation determined that the ACD programme had brought demonstrable and sustainable benefits, proving the value of the UK government undertaking a more active role in cybersecurity.[428]

[426] NCSC-UK (2019).
[427] NCSC-UK (2019).
[428] NCSC-UK (2019).

C.5. The United States

C.5.1. Background

Over a period of decades, the United States of America (US) has developed and implemented a range of major cybersecurity regulations and strategies in order to ensure national cybersecurity. Cybersecurity is also a recognised priority in the US's approach to national security. The 2017 National Security Strategy acknowledges that the ascension of technologies in modern society increases vulnerabilities to cyberattacks.[429] The document flags the protection of cyberspace as a major priority and underlines the necessity to better defend critical infrastructures. Reflecting on the growing threats from state and non-state actors, the 2018 National Defense Strategy similarly presents cyberspace as a warfighting domain and demands investment in cyber defence, resilience, and the continued integration of cyber capabilities into the full spectrum of military operations.[430]

Specific to cybersecurity, the White House issued the National Cyber Strategy in 2018, which presents four strategic priority areas: [431]

1. Protecting the American people, homeland, and way of life by safeguarding networks systems, functions and data;
2. Promoting prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation;
3. Preserving peace and security by strengthening the ability of the US, its partners and allies to deter and punish those who use cyber maliciously; and,
4. Advancing influence to extend the key tenets of an open, interoperable, reliable and secure Internet.[432]

Echoing the 2018 National Cyber Security Strategy pillars, the US Department of Defense (DOD) issued its own cyber strategy in the same year, structured around five lines of effort:

1. Building a more lethal force;
2. Competing and deterring in cyberspace;
3. Strengthening alliances and attracting new partnerships;
4. Reforming the department; and
5. Cultivating talent.

The 2018 DOD Cyber Strategy underlines the conduct of cyberspace operations 'to collect intelligence and prepare military cyber capabilities to be used in the event of crisis or conflict'.[433] This concept of 'defending forward' introduces the possibility for DOD to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict.[434]

[429] The White House (2017).
[430] US Department of Defense (2018a).
[431] The White House (2018).
[432] The White House (2018).
[433] US Department of Defense (2018b).
[434] US Department of Defense (2018b).

From a domestic security perspective, the 2018 DHS Cybersecurity Strategy guides the DHS to execute its cybersecurity responsibilities.[435] The strategy sets an array of goals based on the five pillars, with a great emphasis on: better understanding the US's risk posture at the strategic level in order to optimise resources and efforts toward threats and vulnerabilities; reduction and mitigation of vulnerabilities and threats, and the potential consequences from cybersecurity incidents; and assisting efforts to strengthen the security and reliability of the overall cyber ecosystem to make cyberspace more defensible.

The strategy further describes the DHS's guiding principles to achieve its cybersecurity missions:

- Risk-prioritisation with a focus on systemic risks and greatest threats and vulnerabilities;
- Cost-effectiveness through permanent evaluation of the DHS's efforts;
- Ensuring the DHS is on top in researching, developing, adapting and employing cutting-edge cybersecurity capabilities, as well as remaining agile in its efforts to keep up with evolving threats and technologies;
- Greater collaborative work within the DHS along with other federal and non-federal partners; and
- Maintaining a global approach, balanced equities and national values.

To enable the implementation of the numerous cybersecurity strategies, the US has also established a set of noteworthy regulations on cybersecurity. Some of these are the 1986 Computer, Fraud and Abuse Act,[436] the 1999 Financial Services Modernization Act,[437] the 2002 Federal Information, Security Management Act,[438] and the 2015 Cybersecurity Information Sharing Act.[439]

Key regulations and policies for cybersecurity

Various federal legislation and policies require federal agencies to protect their networks and cyber infrastructure, as seen in the table below.

[435] US DHS (2018).
[436] US Congress (1986).
[437] US Congress (1999).
[438] US Congress (2002).
[439] US Congress (2015).

Table C.5.1 Key US federal regulations and policies for cybersecurity

Date	Legislation or policy	Description
2013	Presidential Policy Directive – Critical Infrastructure Security and Resilience (PPD-21)[440]	Established to strengthen and maintain a secure, functioning and resilient critical infrastructure. The directive establishes sector-specific agencies (SSAs) as the federal entities responsible for providing institutional knowledge and specialised expertise for securing critical infrastructure.
2014	Federal Information Security Modernization Act of 2014[441]	Enacted in order to require federal agencies in the executive branch to develop, document and implement an information security programme for their information systems and evaluate it for effectiveness.
2016	Presidential Policy Directive 41[442]	Governs the federal government's response to cyber incidents involving government or private sector entities.
2015	Cybersecurity Information Sharing Act[443]	Sets a platform for information-sharing between the private sector and federal government entities, allowing for diverse entities including non-federal government, to monitor information systems and conduct defensive measures.
2017	President issued Executive Order 13800	Clarifies that the President will hold agency heads accountable for managing cybersecurity risk to their enterprises.
2018	Cybersecurity and Infrastructure Security Agency Act of 2018	Primary regulation of CISA outlining its responsibilities and activities.
2018	White House National Cyber Strategy[444]	The National Cyber Strategy details the executive branch's approach to managing the nation's cybersecurity. It is also the guiding document for the 2019 National Security Council Implementation Plan.
2019	National Security Council Implementation Plan[445]	The implementation plan for the 2018 National Cyber Strategy. It consists of a total of 191 activities that federal agencies are to undertake to execute the priority actions of the National Cyber Strategy.

Source: RAND Europe analysis.

C.5.2. Overview of governance approach

The following sections outline the various government departments involved in US federal cybersecurity, their roles and responsibilities.

[440] The White House (2013).
[441] CISA (2014).
[442] The White House (2016).
[443] US Congress (2015).
[444] The White House (2018).
[445] GAO (2020).

Roles and responsibilities

There are numerous agencies and departments involved in US federal governance of cybersecurity. From a national security perspective, both the DHS and DOD safeguard US national interests from cyberattacks of considerable effect. However, the DHS is the main US agency responsible for safeguarding civilian national cybersecurity. The DHS acts along the spectrum of anticipation, protection, mitigation, response and recovery in order to evaluate cyber risks and encourage security and resilience of ICT systems.[446] The DHS also holds responsibility for the protection of critical infrastructures and civilian federal cybersecurity. On the other hand, the DOD assists the DHS's coordination of efforts to protect the Defence Industrial Base (DIB) and the DOD Information Network (DODIN). The main responsibilities of the DHS include:

- Monitoring federal network security and further acting against threats directed towards federal agencies;
- Protecting critical infrastructure through risk mitigation, risk assessments of entities and technical assistance;
- Law enforcement responsibilities and the investigation of cybercrimes;
- Enhancing the overall level of cybersecurity in the US by information-sharing with federal and non-federal authorities, including the private sector; and,
- Research and development funding of technologies fostering cybersecurity.

As such, the DHS works closely with other federal agencies and private sector companies. In relation to federal agencies, the DHS has created forums, coordination mechanisms and agreements to enhance inter-agency cooperation towards national cybersecurity, for example in the framework of its mission to enhance the security of technology deployments on agency networks.[447] With the private sector, the DHS collaborates to develop and implement improved cybersecurity tactics that could be deployed at the national scale. The 2016 Presidential Policy Directive 41 (PPD-41) places the DHS as the authority responsible for asset response and assistance to victims of cyberattacks.[448] The DHS is therefore the lead agency to interact with the private sector on cybersecurity. The cybersecurity responsibilities of the DHS are primarily regulated by the 2014 National Cybersecurity Protection Act, which gives the DHS the power to oblige federal agencies to act on cybersecurity advice. In contrast, the DHS cannot oblige private sector companies, but instead works in a collaborative and advisory role.[449]

Towards the achievement of its cybersecurity missions, the DHS mobilises several entities. The main DHS department for cybersecurity is the Cybersecurity and Infrastructure Security Agency (CISA), which was established by the Cybersecurity and Infrastructure Security Agency Act of 2018.[450] The CISA builds national capability to protect the US against cyberattacks. The CISA works to this end with federal government to provide digital tools, incident-response services and evaluation capacity to protect the

[446] CRS (2018).
[447] CRS (2018).
[448] The White House (2016).
[449] US Congress (2014a).
[450] CISA (2020a); US Congress (2018).

government domain 1.gov' and networks that contribute to critical operations of partner departments and agencies. For cybersecurity, the CISA's principal priority areas entail:

- Cyber incident response;
- Combatting cybercrime;
- Securing federal networks, protecting critical infrastructure, and providing cybersecurity governance; and
- Promoting information-sharing, training and exercises.[451]

The CISA's duties are executed through a variety of centres and initiatives, including the National Cybersecurity and Communications Integration Center (NCCIC)[452], the National Risk Management Center (NRMC)[453] and the National Cybersecurity Protection System (NCPS).[454]

Since 2009, the NCCIC has served as an interface of exchange between the federal government and non-federal entities for cybersecurity, communication and technical expertise and, as such, helps the DHS to coordinate civilian cybersecurity activities.[455] The NCCIC is composed of four branches:

1. **NCCIC Operations and Integration** plans, coordinates and integrates capabilities to synchronize analysis, information-sharing and incident management.
2. **US-CERT** builds digital expertise on malicious activity targeting US networks. It further shares information to federal departments and agencies, state and local governments and private sector and international partners. US-CERT operates NCPS, which provides intrusion detection and prevention capabilities to covered federal departments and agencies.
3. **Industrial Control Systems CERT (ICS-CERT)** reduces risk for critical infrastructure by strengthening control systems' security via public-private partnerships.
4. **The National Coordinating Center for Communications (NCC)** monitors and coordinates the initiation and restoration of National Security or Emergency Preparedness telecommunications services or facilities. NCC leverages partnerships with government, industry and international partners to obtain situational awareness and determine priorities for protection and response.

Within the CISA, the NRMC plans, elaborates analysis to determine and tackle significant risks for critical infrastructure. Towards its aims, the NRMC engages with the private sector and other major stakeholders of the critical infrastructure field.[456] From an operational perspective, the NCPS provides integrated capabilities against cyberattacks, thus supporting the DHS mission of federal network defence. The NCPS spectrum of actions includes intrusion detection and prevention, and information-sharing to protect the civilian federal government's IT infrastructure.[457]

[451] US Department of Homeland Security (2020).
[452] National Cybersecurity and Communications Integration Center (2020).
[453] CISA (2020b).
[454] CISA (2020c).
[455] CRS (2018).
[456] CISA (2020a).
[457] CISA (2020c).

Governance and management of significant cyber incidents

Should significant cyber incidents occur, the National Cyber Incident Response Plan (NCIRP) sets the national approach to address adversarial events.[458] The NCIRP describes the role of the private sector, state and local governments, and multiple federal agencies in reacting to incidents. In this perspective, the NCIRP recognises four lines of efforts:

1. Threat response;
2. Asset response;
3. Intelligence support; and
4. Affected entity response.

The Department of Justice (DOJ) is the lead agency for threat response, acting through the Federal Bureau of Investigations (FBI) and National Cyber Investigative Joint Task Force. The entailed activities cover law enforcement, investigation, evidence and intelligence gathering, providing attribution, carrying out action to mitigate threats, facilitating information-sharing and operational coordination with asset response. The DHS is the lead agency for asset response, acting through the NCCIC. Its missions include providing assets protection to affected entities, mitigating vulnerabilities, identifying other entities at risk in the sector or region – including cascading effects – facilitating information-sharing and operational coordination with threat response.

The Office of the Director of National Intelligence is the lead coordinator for intelligence support during a significant cyber incident, acting through the Cyber Threat Intelligence Integration Center. Its responsibilities include supporting federal asset and threats agencies, facilitating the building of situational threat awareness and sharing of related intelligence; the integrated analysis of threat trends and events; the identification of knowledge gaps; and the ability to degrade or mitigate adversary threat capabilities. If a private entity is affected by cyber incidents, the federal government is not involved to a major extent but will remain aware of the affected entity's response activities and in coordination with the affected entity. The relevant agency coordinates the federal government's efforts to understand the potential business or operational impact of a cyber incident on private-sector critical infrastructure.

Through the role division it describes, the NCIRP aims to issue guidance to enable a coordinated whole-of-nation approach to response activities and coordination with stakeholders during a significant cyber incident impacting critical infrastructure.[459]

Other federal agencies with cybersecurity responsibilities

Beyond the main cybersecurity organisations (i.e. the DHS, DOD and the DOJ), there are numerous federal agencies that have a variety of roles and responsibilities in supporting efforts to national cybersecurity. Table C.5.2 provides a summary of US federal organisations with cybersecurity responsibilities and their relevant departments and functions.[460]

[458] US Department of Homeland Security (2016).
[459] US Department of Homeland Security (2016).
[460] For a full description of all federal agencies and their cybersecurity responsibilities, see US GAO (2020).

Table C.5.2 Overview of US federal organisations with cybersecurity responsibilities

Organisation	Relevant departments and functions
White House: Executive Offices of the President	National Security Council, Office of Management and Budget: Office of the Federal Chief Information Officer, Office of Science and Technology Policy
White House: Presidential Advisory Committees	National Science and Technology Council, President's Council of Advisors on Science and Technology, President's National Security Telecommunications Advisory Committee
Central Intelligence Agency Cybersecurity	Central Intelligence Agency
Department of Commerce Cybersecurity	National Institute of Standards and Technology, National Telecommunications and Information Administration
Department of Defense	Chairman of the Joint Chiefs of Staff, Defense Information Systems Agency, DOD Chief Information Officer, DOD Cyber Crime Center, Geographic Combatant Commands, National Guard Bureau, National Security Agency, Office of the Under Secretary of Defense for Acquisition and Sustainment, Office of the Under Secretary of Defense for Policy, Principal Cyber Advisor, US Cyber Command
Department of Energy	National Laboratories, Office of Cybersecurity, Energy Security and Emergency Response
Department of Health and Human Services	Office of the Assistant Secretary for Preparedness and Response, Food and Drug Administration, Office of the Chief Information Officer, Office for Civil Rights
Department of Homeland Security	Federal Emergency Management Agency, Transportation Security Administration, US Coast Guard, US Immigration and Customs Enforcement, US Secret Service
Department of Justice	Criminal Division, Drug Enforcement Agency, Federal Bureau of Investigation, INTERPOL Washington, National Security Division
Department of State	Bureau of Counterterrorism, Bureau of Democracy, Human Rights, and Labor, Bureau of Economic and Business Affairs, Bureau of Intelligence and Research, Bureau of International Narcotics and Law Enforcement Affairs, Bureau of International Organization Affairs, Office of the Coordinator for Cyber Issues, Office of the Legal Advisor, Regional Bureaus
Department of Transportation	Federal Aviation Administration, Maritime Administration, National Highway Traffic Safety Administration, Office of the Assistant Secretary for Research and Technology, Office of Intelligence, Security and Emergency Response
Department of the Treasury	Office of Cybersecurity and Critical Infrastructure Protection, Office of Intelligence and Analysis
Environmental Protection Agency	Office of Homeland Security, Office of Research and Development, Office of Water
Federal Chief Information Officers	Federal Chief Information Officers Council

Federal Communications Commission Cybersecurity	Communications Security, Reliability and Interoperability Council, International Bureau, Public Safety and Homeland Security Bureau, Wireline Competition Bureau, Wireless Telecommunications Bureau
General Services Administration Cybersecurity	Federal Acquisition Service–Office of Information Technology Category, Office of Government-wide Policy, Office of Mission Assurance
National Science Foundation	Computer and Information Science and Engineering, Education and Human Resources, Engineering, Mathematical and Physical Sciences
Office of the Director of National Intelligence	Cyber Threat Intelligence Integration Center, Intelligence Community Chief Information Officer, Intelligence Community—Security Coordination Center, National Aviation Intelligence—Integration Office, National Counterintelligence and Security Center, National Intelligence Manager for Cyber, National Intelligence Manager for Space and Technical Intelligence, National Intelligence Officer for Cyber, National Maritime Intelligence—Integration Office
United States Department of Agriculture	Office of Homeland Security

Source: US GAO (2020).

C.5.3. Evaluation and performance

Various parts of US national cybersecurity have been evaluated by various parties, most regularly by the GAO. This case study has examined three recent evaluations of the US national cybersecurity effort:

1. A report on the state of federal cybersecurity by the United States Senate Permanent Subcommittee on Investigations;
2. A US GAO report on leadership in the implementation of the National Cyber Strategy; and
3. The final report of the Cyberspace Solarium Commission (CSC) on the future of US cybersecurity.

United States Senate Permanent Subcommittee on Investigations

The United States Senate Permanent Subcommittee on Investigations (the Subcommittee) reviewed the past ten years of audits for seven federal agencies: the DHS, the State Department, the Department of Housing and Urban Development, the Department of Agriculture, the Department of Health and Human Services, the Department of Education, and the Social Security Administration.[461] While this evaluation did not exclusively focus on the governance of cybersecurity in the US federal system, the evaluation of the cybersecurity performance of federal agencies can be seen as a proxy indicator of how well the system is working.

The Subcommittee's investigations revealed several significant vulnerabilities within the cybersecurity arrangements of the federal agencies, and a historical and current failure to comply with basic cybersecurity standards. These vulnerabilities included:

[461] US Senate (2019).

- **A lack of comprehensive lists of IT assets.** The review identified a persistent failure to maintain an accurate and comprehensive inventory of its IT for five out of the eight agencies.
- **A lack of timely remediation of cyber vulnerabilities**. All eight agencies were found to have failed to mitigate identified vulnerabilities and apply security patches in a timely manner.
- **A failure in ensuring the authority to operate**. Six of the eight agencies were found to have systems without valid authorities, including DHS, which was itself in charge of securing the networks of other federal agencies.
- **An overreliance on legacy systems**. All eight federal agencies were found to rely on legacy systems, including unsupported operating systems such as Windows XP and Windows 2003.
- **A failure in adequately empowering the CISOs.** Recent federal legislation, including the Federal Information Security Management Act (FISMA) and the Federal Information Technology Acquisition Reform Act, have given federal CISOs increased responsibilities, including plenary governance over federal agencies' IT budgets and priorities.[462] However, none of the eight federal agencies were found to have properly addressed the role of CISO as directed by Congress.[463]

Overall, the Subcommittee evaluation concluded that given the sustained vulnerabilities identified, 'the federal government has not fully achieved its legislative mandate under FISMA and is failing to implement basic cybersecurity standards necessary' for national cybersecurity.[464]

United States Government Accountability Office (GAO) Report to Congressional Requesters

The GAO regularly reviews and evaluates various parts of the US national cybersecurity effort and the most recent governance-related evaluation was published in September 2020.[465] This review focused on describing the roles and responsibilities of federal entities tasked with supporting national cybersecurity, and to determine the extent to which the executive branch has developed a national strategy and a plan to manage its implementation. To help answer these questions, the GAO employed a previously developed set of generally desirable characteristics in developing and implementing national strategies and assessed to what degree the 2018 National Cyber Security Strategy and associated implementation plan responded to them. The characteristics that GAO deems necessary for successful national strategies are:

- **Purpose, scope, and methodology** – The reason and process behind the development of the strategy and the decision regarding its scope and coverage.
- **Organisational roles, responsibilities and coordination** – The roles of those implementing and supporting the implementation of the strategy, as well as mechanisms of coordination between these roles.

[462] The Federal Information Technology Acquisition Reform Act was incorporated in the National Defense Authorization Act for Fiscal Year 2015. See US Congress (2014b).
[463] US Senate (2019).
[464] US Senate (2019).
[465] US GAO (2020).

- **Integration and implementation** – How the strategy interacts and fits with other existing strategies' goals, objectives and activities, and with subordinate levels of government implementation plans.
- **Problem definition and risk assessment** – The problem(s) the strategy is developed to address and a determinant of the level of threat the problem poses to critical assets and operations, from the prism of existing vulnerabilities.
- **Goals, subordinate objectives, activities and performance measures** – The results the strategy is meant to achieve and the determined priorities; the steps needed to achieve the results; expected milestones and performance measures; and a monitoring mechanism.
- **Resources, investments and risk management** – The overall cost of the strategy and an assessment of where resources should be focused on the basis of a risk-reduction versus cost consideration.[466]

The GAO found that the US's National Cyber Strategy and its implementation plan fulfilled three of the six characteristics: the definition of the document's purpose, specification of organisational roles in implementing the strategy and integration with other strategy documents. However, the Strategy and implementation plan were found lacking in relation to their risk assessment, performance measures and resource investment.[467] Specifically, the GAO highlighted:

- **Problem definition and risk assessment** – While the National Cyber Strategy succeeded in highlighting several cybersecurity challenges faced by public and private actors nationwide, as well as naming specific nation-state actors that have previously conducted cyberattacks against US businesses and allies, it ultimately failed to conduct an assessment of these threats and of how they relate to existing vulnerabilities of critical assets and operations. This assessment is essential to making resource-allocation decisions that appropriately minimise risk while maximising returns.
- **Goals, subordinate objectives, activities and performance measures** – The National Cyber Strategy and implementation plan only outlined performance measures for 145 out of 191 activities, and did not establish goals and timelines for 46 out of 191 activities. The strategy also did not provide a formal mechanism to measure progress. The specification of goals and performance measures, and the presence of a progress-measurement mechanism, are all essential parts in ensuring that the involved entities know the goals they need to achieve, and the steps needed to achieve them.
- **Resources, investments and risk management** – The National Cyber Strategy was found to contain no information on the overall cost of implementation, while the implementation plan only outlined the resources needed for 31 out of 191 activities. Both the overall cost of implementation and the identification of required resources for each of the activities are essential

[466] For more details about these characteristics, please see the original GAO publication (GAO, 2004).
[467] US GAO (2020).

to ensure the correct allocation and investment of resources on the basis of risk-reduction versus cost considerations.[468]

In conclusion, the GAO found that the implementation of improvements to the National Security Strategy and the implementation plan are required, to ensure its full effectiveness in providing nationwide cybersecurity. Aside from improvements around risk assessment, goals and performance measures, and resources, investments and risk management, the GAO suggested the additional need for increased clarity and transparency around a well-defined leader, management process and formal monitoring system. This is essential to ensuring oversight over the participating entities and over whether they are executing their duties correctly and on time.[469]

The Cyberspace Solarium Commission

The CSC was created by the 2019 National Defense Authorization Act for Fiscal Year with the aims to 'develop a consensus on a strategic approach to defending the United States in cyberspace against cyberattacks of significant consequences'. The CSC published its final report on 11 March 2020.[470]

In its report, the CSC proposed a new strategic approach to cybersecurity: layered cyber deterrence, which aims at reducing both the probability and the potential impact of cyberattacks of significant consequence. The report outlines three interconnected means of achieving this:

- **Shaping behaviour** – Promoting responsible behaviour in cyberspace by working with allies and partners.
- **Denying benefits** – Increasing national resilience by working with the private sector in securing critical networks.
- **Imposing costs** – Maintaining the capability, capacity and credibility to retaliate in cyberspace.

These means rest on one common foundation, namely the need to reform the organisation of the US government and supporting agencies in matters related to cybersecurity. In particular, the CSC report emphasised the need of the US federal government to increase its capability to organise and conduct concurrent lines of effort to build resilience, respond to threats and maintain deterrence as a collaborative and continuous process. To achieve this, reforms in oversight mechanisms, as well as staff and resources, are needed. The following recommendations emerged as a result:

- **Issue an updated National Cyber Strategy** – To emphasise resilience, public–private cooperation and proactivity in cyberspace.
- **Create House Permanent Select and Senate Select Committees on cybersecurity** – To provide integrated oversight of all cybersecurity efforts across the federal government.

[468] US GAO (2020).
[469] US GAO (2020).
[470] US Cyberspace Solarium Commission (2020).

- **Establish a National Cyber Director** – To act as the President's principal advisor on cybersecurity and to coordinate cybersecurity strategy and policy at the national level, but within the government and with the private sector.
- **Strengthen the Cybersecurity and Infrastructure Security Agency** – To integrate, coordinate and support critical infrastructure cybersecurity efforts within the government and with the private sector.
- **Diversify and strengthen the federal cyberspace workforce** – To develop, recruit and retain cyber talent, and in the process increase the candidate pool for cyber work in the federal government.