Cybersecurity

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

Summary

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).

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.