



# Cybersecurity

## A State-of-the-art Review

Executive summary

Erik Silfversten, Erik Frinking, Nathan Ryan, Marina Favaro

© 2019 Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC),  
Ministerie van Justitie en Veiligheid. Auteursrechten voorbehouden.



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).

WODC publications do not represent the opinions of the Minister of Justice and Security.

All WODC reports can be downloaded free of charge at [www.wodc.nl](http://www.wodc.nl)

# Preface

---

The NCTV (*Nationaal Coördinator Terrorismebestrijding en Veiligheid* – ‘National Coordinator for Security and Counterterrorism’) partners with government, science and business in order to both protect the Netherlands against threats that can disrupt society, and ensure that Dutch vital infrastructure is – and remains – safe. This document presents the executive summary of a RAND Europe study commissioned by the WODC (*Wetenschappelijk Onderzoek- en Documentatiecentrum* – ‘Research and Documentation Centre’), on behalf of the NCTV. The study examines 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 document and its accompanying report cover the methods and analysis undertaken to assess the state-of-the-art in the field of cybersecurity, and provides research questions for the NCTV to consider in the preparatory work for the research agenda. 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, UK, 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

---

## Background and context

Digital transformation has reshaped our world and will continue to disrupt the status quo. While technology is a key driver for realising societal and economic benefits, it also brings about new security challenges. The government of the Netherlands, Dutch businesses, civil society and individuals currently face a range of prominent, emerging and resurgent cybersecurity risks and threats. As concluded in the Cyber Security Assessment Netherlands (CSAN) from the *Nationaal Coördinator Terrorismebestrijding en Veiligheid* (NCTV) the country's digital resilience continues to lag behind the growing cyber threat.

The mission of the NCTV is to protect the Netherlands against threats that can disrupt society, and to ensure that Dutch vital infrastructure is – and remains – safe. To fulfil its mission, the NCTV is preparing a broad research agenda in order 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 work comprises three 'state-of-the-art' studies in the fields of counterterrorism, crisis management and cybersecurity.

## Objectives of the study

On behalf of the NCTV, the *Wetenschappelijk Onderzoek- en Documentatiecentrum* (WODC) commissioned RAND Europe to examine the current state-of-the-art in cybersecurity. In this context, state-of-the-art refers to a snapshot overview of prominent risks, threats or policy issues in the field of cybersecurity, as well as issue areas that are perceived to be overlooked by the NCTV or the scientific community.

The cybersecurity state-of-the-art review is divided into two phases:

- 1) **Phase 1** aims to perform an initial scan of the cybersecurity field in order to highlight prominent or underexposed issues that are perceived to warrant further attention from the NCTV;
- 2) **Phase 2** aims to investigate the research questions identified in Phase 1, and will be carried out through a separate study.

**The study only covers Phase 1 of this process.** The overarching aim of this study is therefore to explore which current cybersecurity topics are relevant to be explored further through additional research in Phase 2. This core objective of Phase 1 was further supported by three sets of questions, as shown in Table 0.4

**Table 0.4 Overview of Phase 1 questions**

<b>Q1. About current and emerging cybersecurity topics</b>	<b>Q2. About the NCTV domain</b>	<b>Q3. About the approach to be taken in Phase 2</b>
Q1.1 What are the most prominent current and emerging cybersecurity topics that are being investigated?	Q2.1 Which of these prominent cybersecurity topics fall within the NCTV's domain?	Q3.1 How can the cybersecurity topics examined above be formulated into future research activity, which may include the development of research questions and the identification of appropriate methodologies?
Q1.2 How thoroughly have these topics been investigated?	Q2.2 Which cybersecurity topics are included and excluded from the NCTV's domain, and why?	Q3.2 Is a systematic review of the literature review a suitable method? If so, which kind of systematic review is most appropriate for the research questions identified?
Q1.3 Have the topics been investigated using high-quality data and appropriate methodologies?		Q3.3 How could the scope of a literature review potentially be defined (e.g. by publication period, groups by which the greatest threat emanate from etc.)?

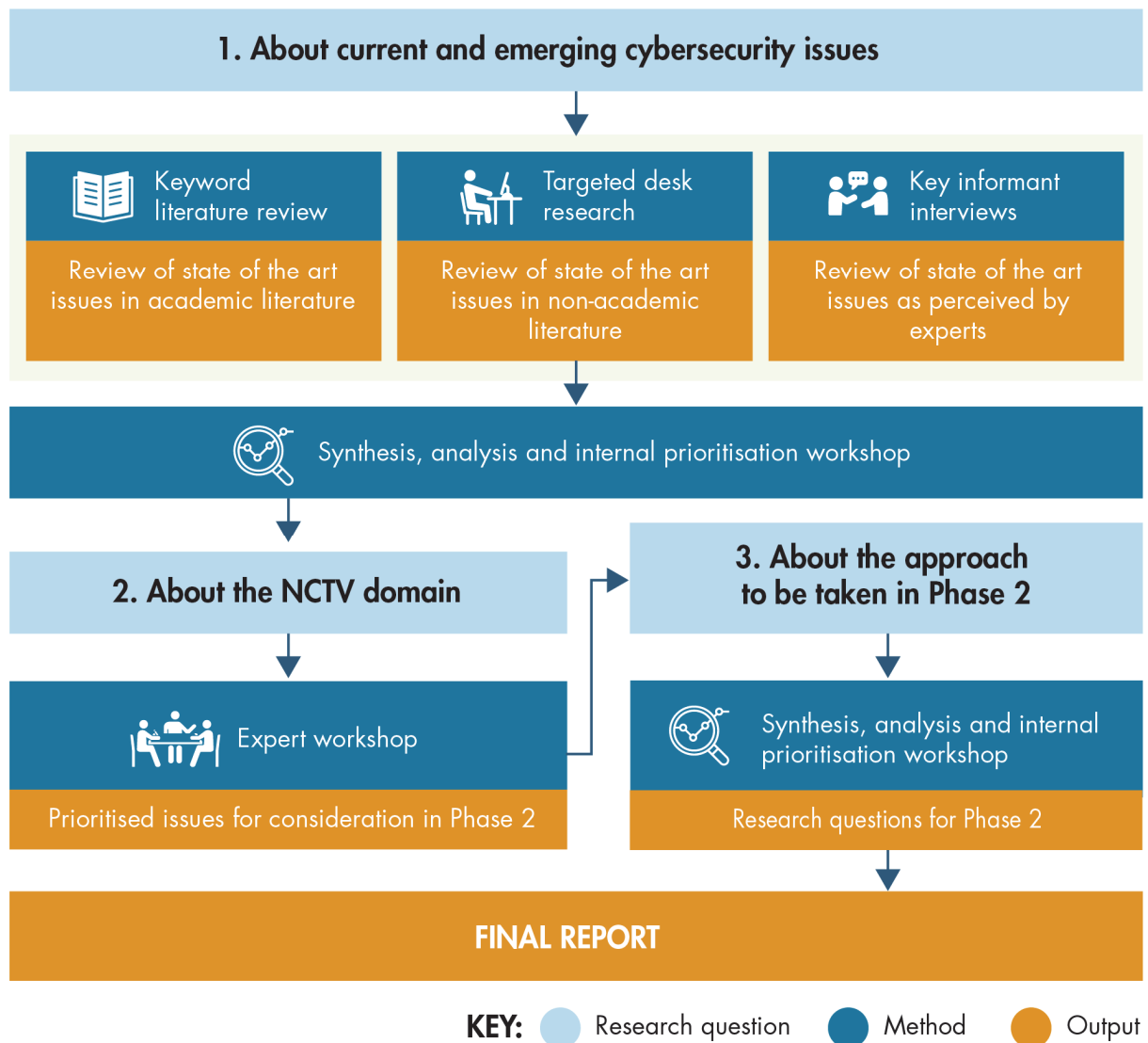
The NCTV currently uses a conceptual ‘triangle model’ of interests, threats and resilience to guide its work. In order to assist with the development of the future research agenda, the NCTV has developed an alternative framework that takes a predominantly actor-centric approach to cybersecurity issues. As part of the broader work around the state-of-the-art studies, the NCTV is seeking to bridge the two conceptual frameworks to incorporate the NCTV’s emerging focus on actor behaviour. These conceptual frameworks were not part of the study’s research questions, and are therefore discussed separately to the main report. As such, Appendix 1 of this report comprises a more detailed explanation of the conceptual frameworks, and a discussion of their strengths and weaknesses in light of the study findings.

## Methodology

We used a structured mixed-methods research approach, as illustrated in Figure 0.3. A full overview of the methodology used in delivering this study can be found in Annex A. This approach was adopted in order to allow for the development of a ‘snapshot’ overview of the state-of-the-art in cybersecurity that clearly illustrates the current and emerging prominent issues and perceived knowledge gaps.

To ensure that the state-of-the-art review was as comprehensive as possible, a mixed-methods approach was adopted, in which a variety of sources were consulted and a range of expert and stakeholder views captured. Lastly, the expert engagement process during the prioritisation of cybersecurity topics for the NCTV helped to ensure relevant study outputs.

Figure 0.3 Overview of state-of-the-art development



## Key findings of the state-of-the-art review

### Q1: About current and emerging cybersecurity topics

The state-of-the-art review has three overall findings:

1. **One of the overarching challenges in the field of cybersecurity is its complexity and poor definition.** In most other fields, the research community explores the boundaries of the research field while building on a core body of knowledge assembled over time. In contrast, the boundaries of the field of cybersecurity are constantly and rapidly evolving and it can be challenging to identify which areas have been researched and which ones remain overlooked or poorly understood.
2. **Knowledge or research gaps are frequent and often persistent.** The field has a number of research gaps, which are often not answered by Dutch studies. For instance, there is a lack of research into national security issues, governance, ethics and legal concerns. There is a persistent

unknown risk posed by dependencies of foreign technology or supply chains outside the Netherlands, which experts and available literature was unable to answer. Emerging topics are often under-researched (e.g. Internet of Things (IoT), AI, cryptocurrencies, the dark web, quantum-related technologies) and their impact on Dutch national security remains unknown.

- a. **Research in the field of cybersecurity often suffers from inadequate or missing data and methods – both in the technical and the policy domains.** The field seems to suffer from a scarcity of reliable, verifiable data, and particularly large scale, longitudinal datasets, across many of the clusters. 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.

The state-of-the-art review identified a wide range of cybersecurity topics that were presented as prominent issues or as significant research gaps in the literature or brought up by experts. In order to consolidate the findings, the study team clustered key themes and prominent issues, and identified research gaps or blind spots from each group of evidence (e.g. the different sets of literature and interviews). Ultimately, 60 prominent cybersecurity issues or perceived research gaps were identified.

We then grouped similar topics together using a structured and iterative approach in order to reduce the number of overall topics, with the ultimate aim to produce a shortlist of topics for the expert workshop. Following from the synthesis and consolidation activities, we produced a shortlist of 11 topics, which formed the basis for the expert workshop. An overview of how the long-list of 60 topics was used to develop the 11 topics is provided in Figure 0.4.

Figure 0.4 Long-list funnel to short-listed topics



The study team produced a shortlist of issues to score and discuss in an expert workshop. The aim of the workshop was to identify the most pertinent issues for the NCTV and analyse which topics should be included in a future research agenda. Ultimately, 11 broad cybersecurity topic areas were identified, as described in Table 0.5 below.

**Table 0.5 Shortlisted prominent cybersecurity topics identified in the state-of-the-art review**

<b>Topic</b>	<b>Title</b>	<b>Description</b>
1	Understanding cybersecurity from a national security perspective	In relation to national security, the field of cybersecurity is broad, and contemporary conceptualisations lean towards a ‘whole-of-society’ manifestation of the field. Among experts in the field, there are low levels of understanding of how different aspects of cybersecurity manifest themselves in a national-security perspective, and how different nation states approach and operate within the cyber domain.
2	National cybersecurity governance	The increased dependency on ICTs across society poses a challenge for governments in terms of how to best organise the governance of cybersecurity at a national level. It is increasingly important that countries anticipate, detect, mitigate and prevent a wide range of cybersecurity incidents and attacks, as well as coordinate these efforts between the public and private sector, both domestically and across international borders.
3	Cybersecurity education and skills	Cybersecurity cannot be achieved without having access to appropriate levels of suitably qualified and experienced cybersecurity professionals. Due to the perceived shortage of cyber professionals and the highly competitive cybersecurity labour market, organisations are increasingly engaging in dedicated efforts to recruit and retain skilled professionals. Public sector organisations tend to face considerable competition from the private sector in a competitive labour market.
4	Challenges associated with implementing basic cybersecurity arrangements	Organisations continue to struggle when implementing basic and effective cybersecurity controls to defend themselves from incidents and attacks. In both the public and private sectors, large-scale cyber incidents continue to occur due to failures in the implementation of appropriate cybersecurity arrangements in areas such as governance (i.e. roles and responsibilities within the organisation), risk management procedures and technical controls.
5	Supply chain security concerns	Supply chain security issues are relevant to all technology-enabled organisations and sectors. In a world of increasingly connected and interdependent supply chains, there is a need to understand what technology is used, where it comes from, how it operates and how it can be tested, verified and assured to work as expected and in a secure manner.
6	Human aspects of cybersecurity	There is a range of human behaviours in cyberspace that compromise systems and render security protocols ineffective. Humans are continually a source of weakness for secure information systems, given that individual behaviours can lead to insecure activities (e.g. password re-use) and are vulnerable to social engineering attacks (e.g. phishing, impersonation, shoulder-surfing, etc.). Individual behaviour may also jeopardise other security interventions.
7	Understanding cybercrime adversaries and victims	Combatting cybercrime has been a priority for the Dutch authorities for some time. However, the field of cybercrime is evolving continuously and the commodification of cybercrime tools, new technologies and increased avenues for exploitation (e.g. increased number of Internet-connected devices) pose current and emerging challenges.

8	Trust in information and data	Society simultaneously produces and consumes increasing volumes of data. As society increasingly relies on data and progressively autonomous analysis or decision-making aids – through technologies such as machine learning and artificial intelligence – it will become increasingly crucial to verify and assure data and emerging decision-making techniques to ensure that they are accurate and without bias and prejudice.
9	Trust in computing	Technological developments have fundamentally changed the ways in which society functions. With technology becoming more ubiquitous, being used in every sector, and replacing all kinds of manual tasks, we are becoming more dependent on computer-related hardware and software than ever before. There is therefore a significant need to ensure that there are appropriate mechanisms to test, certify, verify and assure that systems used across all aspects of society are secure and perform as expected – and continue to do so throughout their lifecycle.
10	Critical infrastructure security	Critical infrastructure (CI) encompasses the physical assets (facilities, sites, hardware, etc.) that are indispensable for the seamless functioning of the economy and society (e.g. energy power plants, dams, government data servers, etc.) and is typically perceived as one of the pillars of national cybersecurity. Recent trends to Internet-enable certain parts of critical infrastructure and the adoption of new or emerging technologies or solutions (e.g. automation, virtualisation, cloud services, AI, etc.) are presenting new and significant security challenges.
11	The economics of cybersecurity and their impact	Cybersecurity failures can be caused by bad design, failure to implement appropriate cybersecurity arrangements, and human error. However, in many situations the underlying causes for security failure are actually bad incentives. There are several underlying factors that contribute to the persistent nature of vulnerabilities in hardware, software and services. The market economics of cybersecurity suffers from a range of negative economic factors (e.g. tragedy of the commons, network effects, externalities, asymmetric information and adverse selection, liability dumping, moral hazard etc.).

## Q2 About the NCTV domain

The 11 topic areas were assessed, discussed and prioritised through an expert workshop attended by Dutch cybersecurity experts in order to identify the most prominent issues where the NCTV should take further action. The workshop highlighted blind spots in each topic, as well as the way that cybersecurity is currently conducted and practised in organisations across the Netherlands, from universities to businesses and government. The 11 topic areas were assessed on the following criteria:

- **Their prominence** in the field (i.e. if a topic is perceived by experts to be a minor, emerging, or significant issue, risk or threat).
- **The perceived level of understanding** of the topic from the perspective of experts and practitioners (i.e. low, emerging or established understanding).
- **Their relevance to the NCTV** (low/medium/high).
- **The urgency for action** (low/medium/high).

Four topics emerged as the most prominent, most urgent and most relevant questions for the NCTV to consider exploring further in Phase 2 of the state-of-the-art project. The study team notes there is a reportedly low understanding of these topics, despite their prominence and the previous work that has been conducted in these areas.

1. **Cybersecurity governance from a national security perspective** is concerned with the rising use, adoption and disruption caused by ICTs, which has led governments to question how best to govern cybersecurity issues that relate to national security. In the Dutch context, a prominent view suggested by workshop participants was that a different governance structure might make the Netherlands more resilient to cybersecurity concerns. They reported that challenges of unclear roles and responsibilities, inconsistencies in language, ineffective organisational structures, and insufficient legal mandates have the potential to jeopardise national security.
2. **Trust in information and data** is focused on the increasingly large volume of data that businesses, government, society and individuals are producing and consuming. Trust in information and data has been eroded by the increasing societal reliance on digitised information and news sources. To cope with the huge volumes of data generated by online activity, public and private organisations are using novel approaches to analyse big datasets, including progressively autonomous analysis or decision-making aids from technologies such as machine learning and artificial intelligence. It is becoming increasingly important to verify and assure data and emerging decision-making techniques to ensure that they are accurate and without bias and prejudice.
3. **Critical infrastructure security** encompasses those services deemed necessary for the well-functioning of society (e.g. power plants, water supply systems, transport infrastructure, etc.). Among Western nations, this is typically perceived as one of the pillars of national cybersecurity. Recent trends to Internet-enable certain components of critical infrastructure and adopt new or emerging technologies or solutions (e.g. automation, virtualisation, cloud services, AI, etc.) are presenting new and significant security challenges. While these are new trends, there are also persistent gaps in the sector's ability to address legacy issues, defend against known vulnerabilities and modernise cyber-physical systems.
4. **Supply chain security** is a concern to the public and private sectors, which are equally exposed to risks in their supply chains, given their increasing connections and interdependencies. The ubiquitous use of ICTs means that organisations should identify the security risk posed by third-parties and establish security controls (e.g. user management, read/write permissions and data-sharing agreements) to mitigate against possible security breaches or cyber incidents. Increasing complexity (e.g. more embedded systems/CPU's) and emerging technologies (e.g. use of third-party algorithms) make it difficult to assess, verify and assure the security of all components and systems used throughout the supply chain.

### Q3 About the approach to be taken in Phase 2

Policymakers, researchers and practitioners will all need to adapt to the dynamic cyber ecosystem. The following research questions and suggested avenues for future research will help to develop more effective cybersecurity policy, strategy and interventions.

For each topic area, the study team undertook internal synthesis and consolidation activities to produce a number (i.e. between three and four) of research questions to be considered for Phase 2 of the project, which are shown in Table 0.6 below. The indicative research questions are based on the sum of synthesised evidence gathered throughout the state-of-the-art study. However, they are not the only research questions that could feasibly be pursued within the topic, and it is not an exhaustive list.

**Table 0.6 Overview of prominent cybersecurity topics and research questions**

<b>Topic area</b>	<b>Research questions</b>
1. Cybersecurity governance from a national security perspective	<p>1.1 How is efficiency and effectiveness of national governance systems measured for cybersecurity policymaking?</p> <p>1.2 What capabilities and skills are required across stakeholders and across functions (e.g. intelligence, operations, coordination, command and control, training, etc.) to ensure cybersecurity?</p> <p>1.3 What lessons can be identified through international comparisons of cybersecurity national governance models?</p> <p>1.4 How can the current model of governance and current cybersecurity initiatives (e.g. strategies, research agendas, roadmaps etc.) be aligned and improved?</p>
2. Trust in information and data	<p>2.1 How can emerging decision-making techniques (e.g. algorithms, machine learning and AI applications) be verified and assured to ensure they are accurate and without bias and prejudice?</p> <p>2.2 How can societal trust in information and data be understood and strengthened?</p> <p>2.3 How can trust in information and data be maintained across the information supply chain?</p>
3. Critical infrastructure security	<p>3.1 What is the interplay between legacy technologies and new technologies (e.g. IoT devices and 5G connectivity) that creates more systemic complexities and dynamic threats to CI?</p> <p>3.2 How can current levels of cybersecurity maturity within critical infrastructure sector be measured and understood?</p> <p>3.3 What can be done to improve security of operational technology deployed in critical sectors?</p>
4. Supply chain security; including both technical and information supply chains	<p>4.1 What are the most prominent supply chain issues, risks and challenges in the Netherlands?</p> <p>4.2 What is the scope and nature of current levels of dependencies on foreign supply of ICT in the Netherlands?</p> <p>4.3 How can cyber resilience be built into the supply chain?</p>

The study team listed indicative methods and research approaches for each of the questions. The research questions are time-bound and they might not be applicable in the medium- to long-term (e.g. 24 months and beyond), given the aforementioned dynamic cyber ecosystem. The research question's future applicability is highly contextual to a short-term timeline (e.g. 0–24 months), given that the study has identified predominantly urgent topics.

The findings presented in this report suggest a series of research questions that could be included in a future research agenda for the NCTV, including relevant methods and indicative research approaches. In addition, we offer three reflections for the NCTV:

1. First, the NCTV could consider the inclusion of a ‘bottom-up’ mechanism in the upcoming research agenda. By enabling individuals and organisations to present their research ideas, the NCTV may be able to be more agile in responding to emerging cybersecurity challenges and better equipped to maintain situational awareness of the field.
2. Second, the NCTV should seek to remain agile and willing to take on the responsibility to coordinate government action – even for cybersecurity issues that lack clear ownership, if such issues risk materialising into a national security concern. This is particularly important in relation to topics that may be ignored unless the NCTV takes action.
3. Third, NCTV should also be conscious of cybersecurity issues where additional research may not be the answer. It may be the case that there is an understanding of what needs to be done, but a lack of political will, funding or operational ability to adequately implement these measures. These issues are therefore perhaps better addressed outside a research agenda, but nevertheless warrant the attention of the NCTV.