National Cyber Security Centre
*Ministry of Justice and Security*

# NCSC-NL Research Agenda 2023 – 2026

*Doing Cybersecurity Research Together!*

# Foreword

## Dear reader,

In today's society, a solid knowledge position is essential. This is why the exchange and development of knowledge is one of the pillars of the work of NCSC-NL and why we provide our partners in the field and our own organisation with the most recent insights based on applied and academic research. This way, we enable them to contribute to the creation of an increasingly digitally secure society in the most effective way possible. While knowledge of today's world is of great importance, insight into the challenges of the near and distant future arguably is of greater importance in order to prepare for things to come, as well as giving us insight into chances that lie ahead with regards to shaping our shared future. This is no simple task – few topics evolve as quickly as cybersecurity does.

The evolution of the NCSC-NL Research agenda also reflects these developments within the field, as this new Research Agenda builds on a theoretical framework that combines various themes from several disciplines, while the previous agenda focused on a number of individual themes. NCSC-NL promotes and focusses on the amplification of the collaboration between several disciplines by investigating developments and incidents from multiple perspectives. This does mean that cybersecurity research can be quite the task, but that this will ultimately lead to people and resources being put to use in the best possible way, as in the currently tight labour market, we cannot afford to be careless with these scarce resources.

The NCSC-NL Research Agenda 2023 – 2026 is essential in the continuation of NCSC-NL as an authoritative knowledge and expertise centre in the cybersecurity field in the Netherlands. I highly recommend reading this new agenda and invite you to look for opportunities to cooperate with our researchers, as (partly because of the aforementioned multidisciplinarity) the mutual exchange of different research disciplines is of great importance.

This Research Agenda is a preview of what our researchers will be working on for the coming years. The agenda itself will be officially presented at the ONE Conference on October 18 and 19 2022: the perfect opportunity to meet our researchers and discuss future possibilities with them. It is by joining forces that we will be able to combine the power of our research resources and come to meaningful results. Ultimately, this will allow us to contribute to a more secure digital society. I hope you enjoy reading this Research Agenda and look forward to a fruitful collaboration.

Kind regards,

**Birgit Dewez**
Head a.i. Knowledge Exchange
National Cyber Security Centre

# Introduction

## Introduction NCSC-NL and Research Team

The National Cyber Security Centre (NCSC-NL) focusses on **understanding** vulnerabilities and threats in the digital domain, **connecting** parties, knowledge, and information, **preventing** societal damage and mitigating threats. We work together with several partners to achieve these goals. The NCSC-NL research team contributes to this by identifying scientific innovations in these areas and by defining and carrying out relevant research. You can find our team's contact details at the back cover of this Research Agenda.

## Review Research Agenda 2019 – 2022

In 2019, NCSC-NL released its first Research Agenda that guided our work for the last couple of years. Within the themes of crisis management, risk management, technology, and strategic and social aspects of cybersecurity, we have conducted, supervised and supported research with funding and expertise. Some of the research results can be found on our website. The Research Agenda has enabled us to build up and exchange cybersecurity knowledge in many areas and with our partners.

Some of the best results have been input for further research, organisational changes, and public attention at conferences, and in scientific and professional magazines, such as IB-Magazine in the Netherlands. For example, we contributed to the increased attention for SBOM, and mandated a study into the impact of the new EU NIS2 Directive on NCSC-NL, and interesting results have emerged from our shared research program with TNO. These and more studies will also be featured on the program of the ONE Conference 2022 on October 18 and 19 in The Hague.

On several of our research projects, we have worked with various partners and we asked some of them to reflect on past, current and future research projects; their responses have been included throughout this Research Agenda.

## Goal NCSC-NL Research Agenda 2023 – 2026

The NCSC-NL Research Agenda 2023 – 2026 is a product of our research ambitions. In this Research Agenda, we give an outline of our vision and activities for the coming years based on the Dutch Cybersecurity Strategy (published in October 2022), our statutory tasks in the Wbni, and NCSC-NL's mission. We use the Research Agenda to formulate research questions, to decide on project participation, and to initiate and carry out our own research. Our team seeks a balance between fundamental, applied, and other research that contributes to our mission. For each subject and research project, we determine who will be carrying out the research and how that will be done. Here NCSC-NL can act as originator, coordinator, researcher and distributor of research and knowledge. If you wish to explore the possibilities of collaboration, please find our contact details in the colophon at the back.

## Theoretical foundation and themes

The upcoming chapters outlines the theoretical foundation of this Research Agenda and its three main themes. With these three themes, we approach cybersecurity research from three levels: macro, meso, and micro. This allows us to research cybersecurity on a strategic, tactical and operational level. Furthermore, this enables NCSC-NL to enhance the digital security of countries, organisations, individuals, and everything in between with the insights from scientific and applied research.

The three themes are divided into various subthemes with corresponding possible research questions, which indicate the

scope of each. Continuing from this, we carry out the research ourselves, outsource the research or take it on with our partners.

### The three main themes of the NCSC-NL Research Agenda 2023 – 2026 are:

- Cybersecurity ecosystem
- Socio-technical cybersecurity: people, processes, and technology
- Technology in cybersecurity

More information on the theoretical foundation of this Research Agenda can be found in the next chapter.

## Next steps

We prioritise which main and subthemes will be developed into research proposals every year. We do this based on previous (research) results and on current developments in cybersecurity, such as those set out in the Cyber Security Assessment Netherlands. After selection of a subtheme, we will use the research questions mentioned in the chapters below as a source of inspiration. In consultation with colleagues, partners, and our constituency, we develope these into research proposals. After careful consideration, we will either carry out the research ourselves or contract it out to one of our partners. The Research Agenda will be evaluated annually to determine sustainability of prioritization, themes and subthemes. This will then lead to continuation, termination or expansion of the specific themes. Research results are shared with our constituency via email and our website, in (scientific) publications such as journals, and during conferences.

# Theoretical Foundation

## Cybersecurity is an integral part of national security.

The Dutch government offers security in many forms to enable the proper functioning of society. Due to the ever increasing digitalisation of daily life, digital security, and thus cybersecurity, has become an essential part of daily lives. This requires a proactive attitude from the Dutch government by ensuring a society in which the government itself, companies, and citizens can move and exists freely in both the physical and the digital domain. On the one hand, this means there needs to be a basic level of cyber resilience, and on the other, that government, companies, and citizens need to be able to respond promptly and adequately to existing and future threats. Because digitalisation and cybersecurity are now interwoven in all layers of our society, it is necessary that we conduct research from multiple perspectives and angles.

## The starting point of this Research Agenda is that cybersecurity is to be researched from several different disciplines.

This means there is value and worth in researching and studying events, incidents, digital phenomena, and digital technologies from multiple perspectives. The NCSC-NL Research Agenda 2023 – 2026 is therefore based on a three-tier model, consisting of the macro, meso, and micro level, with which we conduct social, behavioural, and technologically oriented research, meaning that a particular research or theme does not have to be confined to one level, as it is research that uses multiple theories and makes use of different specialisations that prove to have a lot of added value for us. The NCSC-NL research team is ideally suited for this, mainly due to the diverse backgrounds and research interests of its members.

Cybersecurity is a rapidly developing field, and this makes it a popular research topic. The NCSC-NL Research Agenda sets out which themes and topics the team will focus on in the upcoming years. Furthermore, the broad scope and the use of the three-tier model gives us sufficient scope to take part in interesting collaborations with external partners.

*"Innovations in cybersecurity are of vital importance to being resilient now and remaining resilient in the future. Therefore, it is of great importance that the Netherlands has a strong international position regarding knowledge and innovation. In this regard, the knowledge development by NCSC-NL is of great value because of their unique position straddling the day-to-day practice of cybersecurity and the research community. dcypher stimulates knowledge development through collaboration between the corporate sector, government authorities, and knowledge institutions. To be successful, we all need to know what the other is working on and is working towards. From this point of view, this Research Agenda is of great value to the cybersecurity innovation chain."*

**Eddy Boot**
Director of dcypher

# 1. Cybersecurity ecosystem

**With this first main theme, we study cybersecurity as an ecosystem and the cybersecurity ecosystem itself from the macro level. From this perspective, we take a broad look at the cybersecurity ecosystem. Theories from the social and behavioural sciences are particularly relevant to this theme. This gives us insight into the field of influence in which NCSC-NL and the Dutch government in particular have to operate. This theme is split up into the subthemes of geopolitical influences, risks to the ecosystem, and collaboration in various forms and at various levels.**

## 1.1 Cybersecurity in an era of great power competition

The past two decades have seen a (cautious) return to a world of competition between superpowers in the international political system. The end of the Cold War meant the beginning of a period of US hegemony. This time seems to be coming to an end now that China and Russia are clearly claiming their place in international politics. This has major effects on international security, and thus also on cybersecurity. Recent changes in the focus of Western countries show that the protection of their own territory and the protection of their own norms and values in their own countries have become more prominent. The results of this return to a "great power competition" are clearly visible in the cybersecurity domain. This has direct consequences for the types of cyberattacks that countries and organisations face. For international organisations, this means that China and Russia are challenging the status quo regarding the organisation of the internet. In addition, digital sovereignty and strategic autonomy are subjects that require increased attention on an international level. Research within this theme should give us insight into the influence of geopolitics on the work of NCSC-NL and provide support for what the role of NCSC-NL can be on an international level.

### Possible research questions

- What are the effects of the desire for more digital sovereignty within the EU on the position of the Netherlands, and NCSC-NL in particular, within international bodies such as in IWWN, ICANN, IETF, and FIRST?
- What role could NCSC-NL play in issues surrounding strategic autonomy? How does this role relate to other Dutch organisations in the cybersecurity ecosystem?
- How does the use of key technologies, such as 5G and AI, influence the work of NCSC-NL in international collaborations?
- How can states use any strategic advantages on one or more key technologies to achieve other strategic goals?

## 1.2 Risks to the ecosystem

It is becoming more and more clear that network dependencies between organisations and sectors are crucial for the functioning of various vital processes. Without energy, for example, a lot of things come to a standstill. With the adoption and eventual implementation of the NIS2 Directive, the number of vital sectors and organisations will most likely increase significantly. This makes it even more important to have a clear picture of the interdependence of several vital processes and where any possible risks are located. Research projects will help NCSC-NL with advising its constituency on network dependencies and the risks associated with being part of supply chains and networks.

### Possible research questions

- Supply chain risk management: cross-reference between perspectives of TNO and existing methods and best practices, and creating an overview of different methodologies. This allows for better selection of a method that fits the organisational needs and context.
- What impact does the convergence of IT and OT have on the safety and security of the critical infrastructure in the Netherlands?
- How is the collaboration between chain partners organised outside of formal initiatives? (E.g.: in non-critical processes.) What does the collaboration between large corporations and non-vital SME businesses that are suppliers of critical processes look like?
- How can cybersecurity risks surrounding the dependencies of service providers be made transparent?
- How are risks in one sector related to other risks in other sectors and how to model this?

- What is the risk perception of consumers of essential services and how does it differ from the risk assessment of the suppliers of these services? What do consumers or buyers need to make cybersecurity aspects an important part of their purchasing decision? Which actionable (behaviour-influencing) information do they need?
- What are the lessons learned (for both supervisor and supervised) from the current NIS1 Directive and what can newly designated critical organisations learn from this?
  - What is the influence of legislation and regulations on the effective collaboration between supervisory bodies, CSIRTs, ISACs, and other stakeholders in the Netherlands?
  - Which frameworks, processes, and tools should be developed for the central collection of mandatory and voluntary incident reports and root cause analyses?
- **Organisational**
  - What is the influence of an organisation's governance on its level of cybersecurity?

## 1.3 Collaboration

Within this theme, we look at the influence of legislation and regulations, organisational governance, and partnerships on the level of cybersecurity at international, national, and organisational level. The aim of such research is to look at which partnerships are future-proof looking at the probable increase in vital sector organisations. Furthermore, we aim to enhance scientific knowledge about successful collaborations on international, national, and organisational level.

### Possible research questions

- What role will NCSC-NL play in the Dutch cybersecurity ecosystem going forward and how can we promote collaboration between organisations?
- **Legislation and regulations at national and international level**
  - What are the similarities and differences between various relevant legislation and regulations, and compliance frameworks?
  - What is the position of the NIS2 Directive within a multitude of norms, standards, and compliance frameworks?
  - How do we move from a culture of compliance to more a risk-driven approach? How do supervisory bodies handle this?
- **International**
  - Do other NCSCs work evidence-based? How do they manage and conduct research, and how do they collaborate with academia? Which (international) collaborations are possible?
  - How can international CSIRTs collaborate effectively when vulnerability information needs to be exchanged?
- **National**
  - Which factors contribute to national situation awareness for national cybersecurity risk monitoring and crisis management?

*"At the Radiocommunications Agency Netherlands, we work towards a country that is securely connected; a country that can rely on good telecommunication and IT networks that can be used safely and reliably. We monitor that everyone adheres to the rules, demands, and standards that are in place. The Radiocommunications Agency researches and signals digital resilience and digital security, and puts various developments in this area on the agenda. Sharing and enhancement of knowledge is essential in this. The collaboration between NCSC-NL and us regarding our research is of the utmost importance and something we are happy to continue. In the past, we collaborated on research on the risk of interdependencies amongst digital infrastructure chain system operator suppliers, as well as on research on the abilities of organisations to recover from an IT incident. Lastly, we collaborated on research concerning the relationship between geopolitical events and technological changes in (future) internet infrastructure, with an emphasis on the transport layer."*

**Dr. Jessica de Groot-Overweg**
Researcher and Coordinator research agenda at Radiocommunications Agency Netherlands

# 2. Socio-technical cybersecurity: *people, processes, and technology*

**To really understand how people behave, it is necessary to get an understanding of people and how they interact with technology and data. The sheer amount of different technologies available today, means there are a lot of options and there always seems to be a cheaper, faster or easier way to go about your work or daily life Security is still seen by many as a hindrance that needs to be worked around in order to be fast and agile. By assuming that technology and security should be facilitating, developers, policymakers and executives can proactively design their products and services with the user in mind.**

## 2.1 Security by design

Together with Leiden University, NCSC-NL has conducted research into 'security by behavioural design'. This research focused on how to improve the security of products and services by taking human behaviour into account. The central question here was: how do organisations currently allow for human behaviour when designing and configuring their products and services. NCSC-NL intends to continue this line of research and also to look at how the use of "security by design" can be applied in both systems and processes. By specifically targeting the behavioural component, we can provide better insight into how this component can be used to develop and use safer products and services.

### Possible research questions

- What are organisational and economic incentives for organisations to increase security?
- How can cybersecurity risks be communicated effectively by the systems themselves? How can a user interface design be modelled in such a way that end users choose the most secure option(s)?
- How can we research topics, such as joint situation awareness, AI, human-computer interaction, computer-computer interaction, and humanistic intelligence, and apply them to cybersecurity?
- What would a process or security technology look like if it were redesigned using "design thinking principles"?
- Can cyber-informed engineering help stimulate soft- and hardware developers to develop secure systems?

*"The collaboration with NCSC-NL enables us to work on interesting research projects that have a direct impact on society. The knowledge NCSC-NL has and produces in collaboration with knowledge institutions, in conjunction with their hub and network function, make it possible to move from theoretical scientific knowledge and insights towards recommendations for cybersecurity solutions in the field. Our project on 'security by behavioural design' combines science with real-life situations by developing guidelines and methods based on scientific insights and empirical research with various organisations in the Netherlands."*

**Dr. Tommy van Steen**
Assistant Professor at Leiden University in "Security by behavioural design"

## 2.2 Communication and a data-driven methodology

The concept of communication is based on the effectiveness of knowledge and information exchange, in which the user of the information and their knowledge and skills take a central position. The data-driven methodology has priority at the Department of Justice and Security as well as in the evolution of the cybersecurity profession. It contributes to improved decision-making, information sharing, and risk analysis and it enhances the impact of communications on the urgency of cybersecurity.

### Possible research questions

- How can communication about cybersecurity risks be adapted to the user's level of knowledge and frame of reference?
- Cognitive dimension of situation awareness: how do you, as an employee, deal with all the information that you receive?
- Which communication strategies can be applied to effectively communicate the urgency of cybersecurity measures to directors and entrepreneurs?
- How can evidence-based decision-making help with more effective decision-making and implementation?
- What is the impact of data visualisation on situation awareness?
- How can (sectoral) incident data be analysed and applied in statistical analyses and predictive algorithms?
- Incident reporting obligation: there are many authorities to report incidents to. The NIS2 Directive requires a single point of contact:
  - What must be reported, and how, when and in what order should this be reported? Is there a best practice or standard for this that we should promote?
  - What is the reporting culture like in these essential services?
  - What technology is used for reporting?
  - How is a report processed and how do the competent authorities work together on these reports?
  - What metrics can be extracted from the reports?
- How can we establish effective communications about the risks of vulnerabilities?

## 2.3 Future Internet

The technical foundation of the Internet have been slowly changed, adjusted and refined over the years. Due to its large-scale use it is now impossible to make any fundamental changes to it. This makes applying new insights in "security by design" on Internet technologies quite difficult, but there are several initiatives right now looking towards developing an alternative "Future Internet".

### Possible research questions

- What are the principles for a more secure Internet? What role does NCSC-NL have in this?
- How are the interests of security and surveillance assessed? And what about other interests?
- Could the further development of any Future Internets lead to a fragmentation of the Internet?
- How can a Future Internet contribute to digital safety in the Netherlands?

# 3. Technology in cybersecurity

**Technology in cybersecurity has a dual role: this is the level at which threats manifest itself, but it is also a tool to achieve security with. This relationship then also interacts with the meso and macro tiers: on the one hand, technology is driven by these levels, and on the other hand, technology feeds those levels to understand the environment.**

## 3.1 Vulnerability information

Dealing with vulnerable software and services will always be the core of cybersecurity. Experience has shown us that it is important to obtain, interpret and exchange information about vulnerabilities as quickly as possible. Some parts of these processes are being automated, while human input remains necessary to interpret and enrich the information and send it to the right organisations. The recipients should then be able to efficiently interpret this information within their own context.

### Possible research questions

- What is the impact of automating information flows with regards to vulnerabilities?
- What opportunities do these automated information flows offer?
- What is the best way to make the different kinds of data on vulnerabilities available as open data?
- CVSS is not a risk-score by its definition. Would it nevertheless be possible to have a risk score run (semi) automatically?
- How can an NCSC-NL vulnerability scoring process be adapted to the broader constituency, each of which has its own context?
- The cybersecurity dictionary has (concise) definitions of terms related to digital risks, but we need a broader explanation and standardisation of this terminology.

*"The growing complexity and impact of cyberattacks requires a solid approach to increase cyber resilience. TNO contributes to this by doing research from a broad perspective, including incorporating technological, organizational, and human factors of cybersecurity, together with organisations such as NCSC-NL. In our research, application and implementation is central: how can research results be used to improve the resiliency of Dutch society against cyberattacks? NCSC-NL plays a vital role here in consolidating demand and supply of knowledge. By programming joint and long-range research, we act on today's and future challenges."*

**Gwen Jansen-Ferdinandus**
Program Manager Joint research program NCSC on behalf of TNO

## 3.2 Impact of encryption

Encryption is a tool for achieving integrity and confidentiality goals. This allows you to protect data and can be used in both a positive and a negative sense. Meaning that it can protect confidential information from prying eyes, but it can also be used to protect (communication with) malware. Within this theme, we examine the practical consequences of the ever-increasing encryption of data. Most network traffic today is shielded one way or another. The continuous development of quantum computer technology makes it necessary to use new forms of encryption, and it is steadily becoming clear what new techniques are currently surfacing.

### Possible research questions

- What is the role of network detection in the future?
- Are there creative solutions so that network detection is still possible?
- What are alternative means to achieve comparable results as network detection has in the past?
- How is the transition towards quantum-secure encryption developing?
- What are the practical implications of post-quantum encryption?
- What new possibilities does post-quantum encryption offer?

## 3.3 The foundation of the Internet

The foundation of the Internet is continuously being improved bit by bit – either to increase resilience or to provide better security. Examples of these developments include additions to DNS and extensions of the BGP standards to improve routing security. At the same time, a lot of measurements are performed surrounding adoption of these standards, developments around these protocols and detection of disruptions.

### Possible research questions

- Are the best practices from the current Internet standards being applied in the Netherlands?
- What kind of threats arise from the current standards of the Internet?
- How can parties be encouraged to improve the foundation of the Internet in a wider sense (open-source community, internet providers, internet exchanges, governments and multilateral organisations)?

# Annexes

## References


1. Council of Europe (CoE), Commonwealth Secretariat (ComSec), the Commonwealth Telecommunications Organisation (CTO), Geneva Centre for Security Sector Governance (DCAF), Deloitte, Forum of Incident Response and Security Teams (FIRST), Global Cyber Security Capacity Centre (GCSCC), Geneva Centre for Security Policy (GCSP), Global Partners Digital (GPD), International Criminal Police Organization (INTERPOL), International Telecommunication Union (ITU), Microsoft, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Potomac Institute for Policy Studies (PIPS), RAND Europe, World Bank, United Nations Institute for Disarmament Research (UNIDIR), United Nations Office of Counter-Terrorism (UNOCT), United Nations University (UNU). (2021). "Guide to Developing a National Cybersecurity Strategy 2nd Edition – Strategic engagement in cybersecurity".
2. Dcypher (2018) "National Cyber Security Research Agenda". Herbert Bos, Michel van Eeten, Sandro Etalle, Frank Fransen, Jaap Henk Hoepman, Erik Poll, Jan Piet Barthel (eds). dcypher.
3. Herve Debar, Fabio Di Franco, Athanasios Vasileios Grammatopoulos, Irene Mantzouranis, Evangelos Markatos (2021) "Cybersecurity Research Directions for the EU's Digital Strategic Autonomy". ENISA.
4. National Coordinator for Security and Counterterrorism (2022), "Cybersecurity Assessment Netherlands 2022".
5. National Coordinator for Security and Counterterrorism, (2022), "Netherlands Cybersecurity Strategy".
6. National Cyber Security Centre Netherlands (2019), "NCSC Research Agenda 2019-2022".
7. National Cyber Security Centre United Kingdom (2021), "NCSC Annual Review".


## Method

### The NCSC-NL Research Agenda 2023 – 2026 was established by following these four steps:

1. **Defining scope and desk research:** The first step was to define the scope of the Research Agenda. Initially, that scope was determined by the NCSC-NL Research Agenda 2019 – 2022, the Cyber Security Assessment Netherlands 2021 and 2022, as well as the legal remit of NCSC-NL. In parallel, desk research was conducted to compare the scope with that of similar agenda's in other EU Member States (UK, DE, DK, BE), the United States, and international organisations (EU, ENISA, NATO, OSCE, Interpol, OECD, UN). The documents used in this desk research can be found under References.
2. **Analysis and development of the initial version:** The results of the desk research have been compared and contrasted with the NCSC-NL's mission. A qualitative analysis looked at similarities and differences in focus areas, objectives and prioritisation. Taking into account the national priorities and focus of NCSC-NL, the scope of the Research Agenda has been determined and the initial version has been written based on the above analysis.
3. **Collecting input from internal and external experts:** Interviews were conducted with internal and external cybersecurity experts in order to triangulate and validate earlier findings within the NCSC-NL network. The interviews contributed to the evaluation of the research themes.
4. **Refining and development of final version:** The final version of the Research Agenda has been written on the basis of all the findings resulting from the desk research and the interviews.

**Publication**
National Cyber
Security Centre (NCSC)
P.O. Box 117, 2501 CC The Hague
Turfmarkt 147, 2511 DP The Hague
+31 (0)70 751 5555

**More information**
www.ncsc.nl
research@ncsc.nl
@ncsc_nl

October 2022