National Cybersecurity Research Agenda IV

Science for a resilient digital ecosystem

July 2025

The cover image of this Research Strategy was created by Artificial Intelligence. It took many prompts to generate a representative image of a community of scientists as these exist in universities and universities of applied science today. Unfortunately, with each refinement of the prompt, the system introduced body parts that appear to float in space without a body attached or, vice versa, that were attached to bodies that already had plenty of hands or feet. We decided to leave it as it was, to express our inclusive perspective on science and to reflect the strengths and weaknesses of current-day AI technologies.

Contents

Preface

Cybersecurity is of crucial importance for our highly digitized society. Keeping digital networks and systems secure and protecting our data is a multi-faceted, complex challenge, especially since technological advancements are fast and threats, risks and dangers evolve at a rapid pace. Science is essential for innovation in cybersecurity. It forms the foundation for solid solutions now and in the future. We need research findings from a wide variety of different disciplines, including but not limited to computer science and engineering, law and governance, political science and public administration, psychology and behavioural science, organisational and management science, and even history and philosophy. Ideally, these disciplines bring their knowledge and research to bear in multidisciplinary consortia that tackle the many thorny challenges we face to keep cyberspace secure.

The fourth National Cybersecurity Research Agenda presents the multidisciplinary vision of Dutch scientists working in the field of cybersecurity for the years to come. It describes the themes that researchers in the Netherlands excel at in this field as well as the topics they believe require urgent study in the near future. The creation of this Research Agenda was a collaboration between researchers from academia, united in ACCSS, the ACademic Cybersecurity Society, and researchers from universities of applied science, united under the umbrella of PRIO, Platform Praktijkgericht ICT-Onderzoek. This collaboration, resulting in the joint product before you, is a first. It embodies the scientists' recognition of the fact that innovation for cybersecurity requires research on different levels, on an innovation ladder that ranges from fundamental academic studies to applied research at universities of applied science. The innovation ladder then proceeds into a translation towards real-world products and services. While the latter fall outside the scope of the current Research Agenda, the document aims to help shape the ecosystem for future products and services for cybersecurity in the Netherlands by providing innovative insights and ideas, thus aligning, among other things, with the Action Agenda Cybersecurity, the Netherlands Cybersecurity Strategy (NLCS) and the Dutch Digitalisation Strategy.

During the composition of this fourth National Cybersecurity Research Agenda, the authors of this preface acted as liaisons to ensure connections with society, with businesses, with government, and with our national funding organisation NWO. For the researchers who participated in creating this document, it was crucial that the Agenda should be composed in collaboration with the 'Umwelt' of

academia and universities of applied science, so that it aligns with, for instance, government policy on cybersecurity in the Netherlands broadly, and with government policy on cybersecurity innovation more specifically. It also sought to align with upcoming government funding funnels and schemes and incorporate viewpoints and challenges put forth by the cybersecurity sector in the Netherlands as well as by large corporations in the country. Multiple consultation rounds, meetings and conversations have led to the end product before you today.

As liaisons from government, private organisations and the Dutch Research Council, we oversaw the process, and we identify with the end product. We are the key stakeholders of this Agenda, and we will take it upon ourselves to carry it forth into our respective domains and help materialize the ambitions laid down in it from our respective roles.

Eddy Boot
Director of dcypher
Chair of the steering committee for the NCSRA-IV

Christiane Klöditz
Head of Mathematics and Computer Science
at the Dutch Research Council (NWO)

Martijn Neef
Coordinator Knowledge & Innovation
Cybersecurity at the Ministry of Economic Affairs

Liesbeth Holterman
Director of Cyberveilig Nederland

Frits Grotenhuis
Director of Topsector ICT

The fourth National Cybersecurity Research Agenda: NCSRA-IV

Digital networked technologies are the backbone of our economy and our society. Without them most of our communications, our data and information sharing, and many of the services we rely on daily would no longer be available. At the same time, they are also the enabler for the realisation of the society we aspire to live in tomorrow. Because of this cybersecurity is essential, today and in the future.

Digital networked technologies are evolving rapidly, and with new developments new threats and vulnerabilities emerge. These can be exploited by malicious actors or lead to unintentional outages and accidents. The societal and economic costs of both can be high: due to our widespread reliance on digital technologies, the resilience of our economies and societies is at stake when these technologies fail. This is why it is crucial that we invest in a solid understanding of how to make and maintain digital networked technologies optimally resilient, and that we seek to resolve vulnerabilities and risks as best we can. We must do so through technical interventions, through organisational and behaviour change, and through policies and regulations that help increase security in and of cyberspace. Moreover, it is important that we think about tomorrow and prepare for future risks and vulnerabilities, so that we can make cyberspace more fundamentally and sustainably resilient and secure. Scientific research plays an important role in tackling both current cybersecurity challenges and in improving resilience in the future. This Research Agenda describes the vision of Dutch cybersecurity researchers on accomplishing both, and presents a set of themes for research that contribute to realising them.

The purpose of the National Cybersecurity Research Agenda

The National Cybersecurity Research Agenda IV (NCSRA-IV) serves three main purposes. First, it informs and ties in with other existing and upcoming national strategies and agendas that drive cybersecurity research and innovation in the Netherlands while setting goals for funding and thematic profiling. It shows the thematic strengths of Dutch cybersecurity research and answers the question: what do we excel at in the

Netherlands in terms of research? It also provides a vision of the themes that Dutch cybersecurity researchers deem important for the (near) future.

The Research Agenda forms an important link in the ecosystem of strategies and agendas that inform public policy and public spending on this vital societal and economic challenge. By clarifying the contribution of fundamental and applied science to tackling this challenge, the Netherlands can make coherent investments in designated key areas for cybersecurity, thus strengthening innovation where strengths already exist and focusing on novel areas of importance for the protection and resilience of the Netherlands. This benefits Dutch society and the Dutch economy. It also provides direction for the topics and innovations that the Netherlands may choose to export to other countries.

Second, the Research Agenda unites the cybersecurity research field in the Netherlands and provides a banner for the scientific community to follow. The agenda provides internal direction in the sense that it clarifies what Dutch scientists see as the core themes they will jointly take up in years to come. This agenda was written as a communal effort, bringing together scientists to discuss the question: what are the main challenges that Dutch cybersecurity research focuses on and how do we maximise the societal and economic benefit of our research?

Finally, by uniting the field and clarifying the directions of research on cybersecurity in the Netherlands the National Cybersecurity Research Agenda IV provides unified, multidisciplinary input, and acts as a source of inspiration for other scientific fields in which grand economic and societal challenges are tackled, such as the energy transition, climate change or migration. The Research Agenda shows how a collective narrative may contribute to more coherence in innovation addressing such challenges, whereby the entire chain of levels of innovation, ranging from fundamental science to ready-to-market solutions, provides its best contribution. This agenda harmonizes the lower half of the innovation stack.

Prof.dr. Bibi van den Berg
(Universiteit Leiden, ACCSS)
Dr. Ben Kokkeler (Avans Hogeschool, PRIO)
Melanie Lemmen (NWO)

The Hague, July 2025

Introduction

In 2024, almost 18 million Dutch citizens had access to the internet, which places the Netherlands at the top of the list in terms of internet use in Europe [1-3]. Digital networked technologies are vital for Dutch society, with 90% of citizens using online banking [4], 85% of the population using social networks such as WhatsApp, Facebook and Instagram [5], and 78% of Dutch citizens engaging in online shopping [6]. The Dutch government uses a variety of (inter)national online platforms to connect with citizens and to provide them with services. In sum, the use of digital networked technologies has become an essential infrastructure for social connection, for information sharing and provision and for a wide variety of day-to-day activities in the Netherlands.

Cyberspace is also vital for the Dutch economy. The digital infrastructure in the Netherlands forms the backbone for almost all economic activities in the country. The Netherlands has an extensive digital infrastructure, consisting of a vibrant cloud industry, several large telecommunications and internet service providers and a significant number of data centres [3]. It is the fastest growing sector of the Dutch economy, with a revenue of €24.3B per year – the digital infrastructure has a bigger impact on the Dutch economy than Schiphol Airport or the Port of Rotterdam [7-8]. Moreover, with internet traffic increasing by 22% annually through AMS-IX [9], one of the largest internet hubs in the world, this sector is expected to remain one of the growth engines of the Dutch economy. Because of the solid digital infrastructure in the Netherlands, new developments in cloud computing, Artificial Intelligence (AI), the Internet of Things (IoT), industrial or operational technology (OT), and quantum computing all offer opportunities for the Dutch economy.

Since digital networks and digital networked technologies are so important for Dutch society and the Dutch economy, the topic of cybersecurity has gained a prominent place on the agenda for public and private organisations and for the Dutch government. One of the key ambitions of the Dutch Digitalisation Strategy (2021) is to ensure that trust in digital products and services is warranted, and that digital networked technologies can be used in a safe and secure way, with respect for fundamental rights and freedoms [10]. The Netherlands Cybersecurity Strategy 2022–2028 (NLCS) states that security is indispensable if we want to make

use of the full potential of cyberspace in the years to come [11].

Cybersecurity is a *sine qua non* as well as a critical enabler for a country with such a high dependency on digital network technologies. It should not be considered as a cost, but rather as an investment in the future of our economy and our society. It is indivisible from other security interests, such as physical and economic security, territorial and environmental security, and social and (geo)political stability [11]. Ultimately, cybersecurity is about the protection of the public values that we hold dear in the Netherlands and in Europe. Its objective is to ensure that individuals, groups and collectives can fully and freely participate and thrive in the digital ecosystem. It is also about warranting that cyberspace is an open and free space on the one hand, and an ecosystem in which values and laws are upheld on the other.

Current gaps

In today's reality, also in the Netherlands, the safe use of digital networked technologies is an individual responsibility for both citizens and consumers and for public and private organisations. Governments aim to provide direction towards a more secure cyberspace through legislation, regulation and policies, but ultimately the responsibility for making digital networked technologies more resilient is scattered across many different parties – who oftentimes lack the connections, means and skills to protect themselves well. With the ever-increasing density and complexity of digital networked technologies, placing the responsibility for the secure use of the digital ecosystem in the hands of individual citizens and organisations is no longer tenable. What is required, as a dot on the horizon, is a fundamental change to ensure that digital networked technologies become what we call '**straightforwardly secure**' (or 'vanzelfsprekend veilig' in Dutch): the security of systems, networks and data ought to be facilitated 'behind the screens' for end users, who can use cyberspace without concerns for their security in the same way as they can use safe drinking water from the tap or access a safe airplane to fly to another location.

Security by design & by default

Generating a world in which digital network technologies are straightforwardly secure is no easy feat. Visions such as **security by design** or **security by default** can help us move in that direction [12-13]. Security by design envisions that digital networked technologies will be made secure during the design and development phase and will remain so

throughout their deployment, i.e. throughout their entire lifecycle. Security by default stipulates that secure settings ought to be the standard mode for the use of digital networked technologies and that the responsibility for making this a reality lies with tech companies, vendors and suppliers.

Moving towards security by design and security by default entails several fundamental system changes: it requires different approaches to the design, development and deployment of technologies by manufacturers and distributors, and it demands political and economic choices by governments and companies which drive digital innovation in the direction of inherently secure products and services. It also requires the right incentives to be in place to drive the right outcomes. This will at least in part need to be achieved by developing and maintaining effective legal and normative standards for secure technologies, accompanied by effective enforcement mechanisms. Moreover, it calls for standardisation and harmonisation of security requirements to ensure compliance. Finally, it calls for scientific contributions, both fundamental and applied, on the technical, legal, organisational, behavioural and public policy challenges that need to be addressed to accomplish a straightforwardly secure digital ecosystem. In sum, generating truly secure-by-design digital networked technologies can only be accomplished through fundamental changes in the ecosystem as a whole. This will take time and the involvement of many different stakeholders – the scientific community being one of them.

Strategic autonomy & digital sovereignty

A second challenge for cybersecurity in today's reality is the fact that many parts of our digital ecosystem are in the hands of private parties, including parties with significant market power that are often located in China and the US. The private nature of the digital ecosystem has profound implications for the realisation of the security of data, networks and systems in the Netherlands, due to differences in legislation and limitations in our control over them. A major complication is that cybersecurity is subject to geopolitical dynamics. Concerns on the power of big tech broadly have been growing in recent years, as has an awareness of the geopolitical power of China with respect to the digital ecosystem. This year, the political course taken in the US led to the realization that alliances that were stable for many decades can suddenly be less so. This has added urgency to debates on our international dependency on non-Dutch and non-EU technology companies. In combination with an unstable geopolitical climate this may lead to significant risks for citizens and consumers, for public and for private organisations, and for governments in the EU.

Since upholding and protecting our public norms and values is essential for the Netherlands, **strategic autonomy** and **digital sovereignty** are crucial themes for the upcoming years [14-15]. Both can take many different forms, ranging from developing an independent European tech sector to focusing on increasing control over non-EU-based technologies through regulatory and governance interventions, with many shades in between. Science has a key role to play in feeding policy and politics with realistic ambitions for strategic autonomy in the Netherlands and the EU, and with input on the legal and economic requirements for its accomplishment. Moreover, it can provide technical, organisational and behavioural solutions towards EU-based innovations for secure technologies that respect fundamental European values.

The role of science

Science thus has a crucial role to play in both challenges: in the development of a straightforwardly secure cyberspace, and in finding ways to increase the Netherlands' and Europe's capabilities to protect and promote core public values in and via cyberspace. Collectively, these two contributions will be key drivers in the Netherlands' aim to increase societal and economic resilience.

Dutch universities and universities of applied science are home to a variety of research groups, whose research can boost innovations to tackle the challenges that citizens and consumers, public and private organisations, and the government face with respect to securing cyberspace. They play an important role in the Dutch innovation ecosystem, which runs from fundamental scientific research to the creation of practical products and services.

This Research Agenda is a strategic document that shows the full breadth of scientific contributions Dutch researchers are currently making to raise the security of cyberspace, and which themes they aim to work on in the upcoming years to take steps in the direction of a straightforwardly secure cyberspace. As the discussion above reveals, challenges for the security of cyberspace are inherently multi-disciplinary: they embody a mixture of technical, legal, ethical, behavioural, and organisational puzzles that are most effectively addressed through contributions from a variety of different academic disciplines, including but not limited to computer science, engineering, mathematics,

organisational and management science, behavioural science and psychology, sociology, law and criminology, philosophy, and governance and public administration. As this Research Agenda shows, cybersecurity challenges are studied from all these angles in the Netherlands, and the research community collaborates in a multidisciplinary fashion.

In the past years, in response to the societal, economic, and scientific challenges in the field of cybersecurity, the research community on this topic in the Netherlands has formed close ties through the creation of two academic societies, through joint research and education projects, and through a variety of meetings. The creation of this Research Agenda has further strengthened these ties and united the researchers in their ambitions and vision. The Agenda itself is also envisioned to act as a catalyst for coherence and collaboration in the field in years to come. Through increased collaboration, new research and innovative ideas are generated for cybersecurity, which in turn also affect work in other, related domains. A scientific unified stance for cybersecurity thus benefits society and the economy, but also science itself: it may act as fertile ground and take an exemplary role for other grand societal challenges and for other multidisciplinary research fields.

The setup

This Research Agenda was created through a collective effort of the cybersecurity researchers working at Dutch universities and Dutch universities of applied science in consultation with external stakeholders, such as cybersecurity companies and a variety of government representatives. ACCSS, the ACademic Society for Cybersecurity and PRIO, the society for ICT research in the universities of applied science, drove the composition of this agenda. Its creation started with a broad survey inventorying cybersecurity research themes in the fall of 2024. Almost 80 participants responded to this survey by submitting key themes for (future) research in cybersecurity for the Netherlands. Based on this survey, a first mapping was made providing a broad overview of the Dutch research landscape.

In the spring and early summer of 2025 multiple consultations were held with scientists and stakeholders from government and industry. In these sessions over a hundred people provided their input on both the research themes that scientists in the Netherlands currently work on and should work on in the future, and on the overarching

shared vision that scientists and external stakeholders share on the role of scientific research in cybersecurity for the Netherlands. The latter is embodied in this introduction.

Finally, a number of scientists provided input on the writing of this document in several rounds of edits, complemented with feedback from stakeholders from public and private organisations. The end result provides an overview of the key themes that, according to scientists in the Netherlands working in the field of cybersecurity, require research to increase the economic and societal resilience for the Netherlands. They express a vision of straightforward security for digital networked technologies that respects the core public values that we hold dear in the Netherlands.

Five pillars of research

Building on the outcomes of the survey and the consultation rounds, the key research themes for cybersecurity in the Netherlands have been clustered into five pillars in this Research Agenda:

- Design
- Defend
- Attack
- Use
- Recover

Design refers to security challenges that are discovered and security solutions that are generated in the process of designing and developing novel or improved digital technologies, or in creating novel or improved processes, policies, laws and regulations. Note that the term 'design' is used in alignment with the vision of security by design, which entails that security is not just built into technologies, systems, processes and structures from the start, but remains a core value in development and deployment until the end of the lifecycle thereof.

Defend and **Attack** are two closely related pillars, that focus on the discovery of vulnerabilities and threats, and on the potential acts and actors that may abuse these vulnerabilities. For a solid understanding of the ways in which we can increase resilience and cybersecurity through defensive technical, behavioural, organisational, and legal means we also need to understand the ways in which vulnerabilities may be exploited through attacks, including having an understanding of the motives, techniques, drivers and actions of attackers.

Use refers to the challenges that may arise when digital networked technologies are used in practice for instance in organisations, between organisations in chains of suppliers, or by citizens and consumers. It focuses, for instance, on the role of security cultures in organisations, on the origins of cyber accidents, on non-use or delayed adoption of new standards, and on measuring the effectiveness of cybersecurity interventions, ranging from cybersecurity trainings to applying new management and governance practices.

Finally, **Recover** refers to those situations in which cyber attacks or accidents lead to incidents or crises despite all the preventative and preparatory measures taken to avoid their occurrence. Unfortunately, due to the complexity and interconnectedness of digital networked technologies such incidents are no

longer a matter of *if* but *when*. The evolving strategies of international criminal actor networks and new forms of hybrid warfare initiated by state actors only exacerbate this challenge. As a consequence, individuals, organisations and governments need to invest in technical, organisational and legal mechanisms to respond to incidents and crises, to help mitigate them, and to learn from them.

There are clear connections and overlaps between the five pillars, which reveal the need for joint research. Some would argue, for instance, that research in Defend and Attack are two sides of the same coin, or that there is a close connection between the research in Design and in Use of digital networked technologies. The pillars are intended to structure the research landscape and do not express a compartmentalised view on academic research. Separating themes into distinct pillars has the advantage that it may put the spotlight on those places where the pillars do not overlap. Where overlaps and interconnections do exist, these will be addressed in the descriptions of each pillar below through links in the text.

Each of the five pillars embodies research questions, challenges and goals from computer science and engineering, from management and organisation sciences, from behavioural science and psychology, and from law and public administration. They are all thoroughly multidisciplinary — as they should be if science is to contribute to these challenges in a comprehensive and meaningful way. The **matrix** on the next page combines the five pillars with these different scientific lenses and displays the variety of research themes that Dutch researchers in universities and universities of applied science see as the **main contributors to strong economic and societal resilience in the upcoming years, with a special focus on straightforward security and the protection of Dutch public values.**

In the next sections of this Research Agenda each pillar will be discussed in more detail. A similar structure will be followed in each description: the pillar will be introduced in a short overview that captures its focus area and lists some of the fundamental themes this pillar seeks to address. This is followed by an overview of some of the research challenges that are studied in relation to these questions. Each section ends with a description of some of the example topics that are studied under this pillar.

The five pillars at a glance: the matrix

	DESIGN	DEFEND	ATTACK	USE	RECOVER
	[create, develop, implement]	*[prevent, protect]*	*[abuse, sabotage, steal, harm]*	*[apply, understand]*	*[respond to incidents, investigate incidents, improve, learn]*
computer science	artificial intelligence cloud computing privacy-enhancing technologies secure hard- and software smart technologies, infrastructures & environments (quantum-safe) cryptanalysis	artificial intelligence attribution intel & threat modeling monitoring & detection patching (automated) vulnerability research (quantum-safe) cryptanalysis	artificial intelligence cyber attacks on hard & software intel & threat modeling attacker behavior malware analysis side-channel analysis	smart technologies, infrastructures & environments social media	forensics incident response threat intel
behavioural science, management & organization science	behavior change risk management user centric (security) design	behavior change cybercrime resilience risk management	behavior change cybercrime	cyber accidents usable security cybersecurity training measuring security (technologies) security culture social media	foresight preparedness & resilience learning from incidents
law, governance & regulation	ethics & values in design new & upcoming legislation standardization & harmonization	cyber warfare & state sponsored attacks cybersecurity governance international law	cybercrime cyber warfare & state sponsored attacks	certification enforcement & compliance dual use privacy & data protection	preparedness & resilience crisis management incident management

Figure 1: An overview of key themes for the Research Agenda in the upcoming years per pillar and cluster of scientific disciplines.

Design

It all starts with design & development

1 Security by design and security by default are two of the guiding principles that cybersecurity researchers in the Netherlands follow. By making products and services secure from the start, security incidents may be prevented. Similarly, by setting products and services to secure defaults, security risks may be reduced greatly for the vast majority of end users. In recent years, a body of academic research has emerged, both in the Netherlands and abroad, to explicate what security by design and security by default consist of in a constantly evolving world of technological development.

New technological trends urge us to rethink this question each time. For instance, the spread of cloud computing requires us to rethink security requirements for cloud architectures and for the safe storage and distribution of data. Advances in networking of industrial control systems and other operational technologies require work on secure hard- and software. Infrastructures such as the energy grid or water management and environments such as cities and homes increasingly 'turn smart', which means that privacy- and security-preserving techniques are vital to protect the data, networks and systems connected in and via them.

2 A topic that is highly relevant to secure design and development is artificial intelligence. AI can be used to enhance the security of systems and networks, to strengthen defences, increase the likelihood of detecting anomalies and automate steps to mitigate vulnerabilities or attacks. At the same time, it is essential that new AI tools and services themselves are designed responsibly and ethically with security by design and security by default principles in mind.

3 Moreover, for the secure exchange of data and information, cutting-edge cryptography remains essential. Quantum computing is often seen as one of the grand challenges for cryptanalysis in the near future. New quantum tools and techniques need to be developed, and these techniques are then applied to both soft- and hardware.

4 To address the cybersecurity challenges of today and tomorrow it is also essential to come up with insights on effective interventions for behaviour change. In the design process of new digital services and

products, the behaviours, thoughts and desires of end users ought to be taken into consideration, thus enhancing user-centric design. The latter is closely related to value-sensitive and to participatory design, which ensure that products and services not only align with industry-wide (EU) standards, but also with public values expressed and propagated by European or Dutch regulations and societal norms.

5 There are pressing challenges for organisations as well. While risk management is the main focus for many organisations today in addressing cybersecurity risk, it requires continuous updating and innovation to meet new threats and increasing interdependencies, most notably supply chain risk and a lack of digital autonomy. Moreover, in a world with increasing uncertainties new frameworks and toolkits need to be developed to help organisations secure their assets.

Finally, in the past decade a significant body of 6 new laws and regulations has come into effect to steer and influence a wide variety of cybersecurity-related themes, such as the protection of critical infrastructures (NIS2), consumer protection (CRA), privacy and data protection (GDPR) and IT and cybersecurity regulation in the financial sector (DORA). New laws, for instance with respect to AI, are in the pipeline. Increasingly, this legislation pushes towards secure-by-design and secure-by-default products, services and solutions. There is also an increasing emphasis on standardisation and harmonisation in order to increase security and improve oversight.

Research challenges

1 The fact that digital networked technologies develop rapidly and dynamically within a geopolitical and economic ecosystem that is in constant flux entails that the fundamentals and practices of security by design and security by default need to be updated continuously. What secure design is, therefore, remains elusive up to a point, and is always part of research on the design of new technologies, but also of new behavioural, organisations or regulatory interventions.

The rapid rise and spread of various forms of 2 AI brings forth a host of research challenges, not only as a topic of investigation, but also with respect to doing the research itself. Ethical and legal questions, for instance in relation to autonomy, privacy and data protection, and intellectual property, in relation to the implementation of new regulations and the adoption of norms must be addressed in fundamental and applied research in years to come.

3

With the increasingly urgent call for strategic autonomy with respect to digital networked technologies in Europe and the Netherlands, there is pressure on technology developers and companies but also researchers to generate innovations to strengthen the European tech sector and/or increase more control over infrastructures, networks and data in the EU and the Netherlands. Dutch R&D activities must move to the forefront in (co-)defining industry standards for, for instance, 6G or quantum computing, and meet the challenge on delivering new technologies with the highest security standards.

4

The networked character of both critical infrastructures and the digital ecosystem itself entails that there are interdependencies and supply chain challenges in technical, economical, organisational, practical and legal sense of the term. This means that it is impossible for the Netherlands (or Europe) to design and develop new cybersecurity solutions in isolation. Investing in international collaborations and fostering sustainable relationships with trustworthy partners is a key cornerstone of research in all pillars of the NCSRA, but especially in relation to design.

Example topics

- Developing secure-by-design and secure-by default cloud, energy grid and water management solutions.
- Designing AI solutions for cyber defence.
- Developing future-proof crypto solutions for hard- and software.
- Designing behaviour change programs with measurable effects.
- Developing participatory design models for the creation of user-friendly products and services.
- Designing measurable, effective methods for dealing with organisational cybersecurity risk.
- Developing policy and regulatory requirements for the realisation of a straightforwardly secure cyberspace that respects and promotes EU and Dutch core values.
- Developing secure-by-design and secure-by default cloud architectures, and/or secure-by-design and secure-by-default architectures for specific sectors, such as energy, water management or transport.

Defend

Robust defences increase resilience

1 For improved resilience we must increase the security of systems, networks and data, and hence it is vital that we develop and improve defensive mechanisms to keep up with the ever-changing threat landscape of cyberspace. In its 2024 annual report, published in the spring of 2025, the Dutch Military Intelligence and Security Service MIVD warned that the Netherlands (and Europe) is now in a 'grey zone' between war and peace, with continuous attacks happening both in the physical world and in the digital world []. Until now, the attacks remain below the threshold of acts of war. However, the increase of state-actor or state-sponsored attacks is noteworthy and worrisome, since these attacks are more complex and more difficult to defend against.

Much of our (critical) infrastructure has been designed and built with a peace-time perspective. The emphasis has been on functionality and on the benefits of connectivity. However, the current geopolitical situation forces us to rethink and redesign the existing ecosystem in the Netherlands and in Europe. Significant investments need to be made to systematically invest in European (open source) office and productivity software alternatives such as Nextcloud and Openoffice. This shift may also offer an opportunity to integrate (usable) security deeper into the ICT-infrastructure than in the earlier designs. Research is needed to aid in securing EU-based alternatives for office and productivity software.

2 Meanwhile, we need a keen awareness of new and evolving vulnerabilities in the data, systems and networks we use. Due to the complexity of current-day technologies and the density of networks, vulnerability research must increasingly be automated. The same goes for patching detected vulnerabilities. Self-healing software is an example in case. Moreover, because the threat landscape constantly evolves, efforts must be made to improve our intelligence gathering and our capabilities to model those threats. Improved monitoring and detection mechanisms and capabilities are core as well. The technical attribution of cyber attacks also remains a challenge that deserves attention.

3 Just like in design, the role of AI for research on defence cannot be understated. Artificial Intelligence can play a crucial role in increasing

our ability to discover vulnerabilities and facilitate automated responses.

4 To improve the defences of public and private organisations and to increase protections for citizens and consumers it is crucial that we develop a good understanding of developments in cybercrime and the profiles of cybercriminals. This entails understanding what drives these criminals, how they collaborate, how they commit crimes in a dynamically changing environment, and how economic or other incentives can be used to curb their behaviours. Moreover, it is vital that we understand the constantly changing economics of crime, for instance with respect to cybercrime as a service. All these themes may also support law enforcement in its attempts to combat cybercrime.

5 A related theme is the role of offensive cyber operations by state actors. With changes in the geopolitical landscape there are increasing threats from state (sponsored) actors. The nature of these threats changes rapidly and involves an understanding of state posturing in international relation, norms for state behaviour in cyberspace, and a keen technical understanding of the (im)possibilities of using offensive digital capabilities. Gaining insight into the drives and activities of states in relation to cyberspace may lead to developments in international law in the middle long term.

6 Understanding state actor and cybercriminal threats may also help us increase our defences both in terms of national security, for instance through improved cybersecurity governance, and in terms of the cybersecurity of organisations, for example through better risk management. Increasing the level of resilience of systems, data, networks, people and organisations is one of the key areas of focus for both the state and for individual organisations. Furthermore, if we have a better understanding of the ways in which both individuals and organisations may fall victim to attacks by different types of actors, we may also improve our ability to raise defensive mechanisms against such attacks. There are close ties with the work done on the use of cyberspace around this theme.

7 Finally, identity and access management (IAM) are vital for defence. In the next few years Europe will introduce digital identity wallets (EUIDs), inspired by the academic research efforts in the Netherlands (resulting in the Yivi app). This is a clear showcase of the huge effect that security and privacy research can have. These wallets will offer many new possibilities for securing online transactions, including digital signing and possibilities for authenticity guarantees. This is crucial in a

world plagued by mis- and dis-information, often artificially generated. At the same time these new identity wallets form obvious points of attack. They need to be defended, via a combination of rigorous security analysis and new (cryptographic) protection mechanisms. Indeed, these wallets need to be 'cryptographically agile', allowing updates of their crypto infrastructure, for instance for a future shift to postquantum.

Research challenges

1 Improving defence entails making steps towards strategic autonomy and digital sovereignty, which, in a densely global interconnected ecosystem requires bold choices, significant investments, a careful rethink of designs and implementations, and time. One of the challenges of the next years is how to balance proper, robust combinations of local control in the EU and the Netherlands with controlled, monitored connectivity in our ICT infrastructures. Research into the institutional design of governance structures combined with technical advances in a digital ecosystem that respects and promotes core EU and Dutch values contributes to accomplishing this.

2 Automation is key to increasing our abilities to detect and address vulnerabilities in existing soft- and hardware. AI will play an increasingly important role in facilitating this in the next years. Harnessing the possibilities of AI to do so is challenging, especially when attackers also strive to use AI to increase their power.

3 Cybercriminal networks and their ways of working evolve rapidly, and research is needed into improved defences for novel modus operandi and novel attack surfaces. This is especially important when criminal networks fuse with, or work with support of state actors, and thus develop more sophisticated attack patterns and approaches.

4 State actor cyber threats are high on the agenda. The lack of internationally binding standards surrounding cyber warfare is problematic. Research has revealed that different state actors have different motives to engage in attacks on other states, with some aiming to destabilise existing power blocks to change the power balance and others focusing mostly on economic gain. So far, our defensive measures and responses have not diversified sufficiently to align with these findings. Research can improve the development of different strategies for the various types of state actor threats.

5 One area for improved defences is increasing monitoring capacities within organisations but also for national defence. A key challenge is to find the right balance between privacy protection and detailed monitoring for defensive security purposes only.

Example topics

- Designing AI solutions for cyber defence.
- Developing governance and regulatory proposals for international standard setting and improved strategic responses to organised crime and state actor attacks.
- Providing insights into the economic, technical, governance and legal requirements for a (more) digitally autonomous European Union.
- Developing privacy-preserving monitoring techniques.

Attack

Increasing security by understanding attacks and attackers

1

To improve our defences, it is essential that we understand the state-of-the art in terms of attacks as well. We cannot increase resilience and security without knowing how attackers find and abuse vulnerabilities, both in hardware and in software. We also need to have advanced knowledge of attacks to be able to test new designs or improve the defences of existing designs. Moreover, we may sometimes wish to use offensive mechanisms to stop state or criminal actors. The work in this pillar, therefore, is related to work done in the Design pillar and even more closely related to that in the Defend pillar. Improving threat modelling, increasing our intelligence position and learning about attacker behaviour are important for defence as well as for attacks. There are some differences, too. One key area of attack-oriented research is malware analysis: gaining a deep understanding of the ways in which code is (ab)used by attackers to accomplish certain goals, such as sabotaging a system, exfiltrating data, or disrupting a network. Side-channel analysis is another topic of focus: through this type of analysis the implementation of a system may be mapped, thus bringing to light weaknesses that can be exploited even when cryptographic mechanisms are in place. Moreover, research is needed to discover new vulnerabilities and chart the ways in which these might be exploited and to explore the potential of automated vulnerability discovery.

2

Today's understanding of offensive techniques is not sufficient for a world where the number of devices is measured in tens of billions and where software is everywhere, often tightly integrated with hardware. Today's methodology of ad hoc probing of the security of a handful devices is thus no longer an option. As of yet, however, we cannot assess the security and find dangerous weaknesses automatically at scale, covering a vast multitude of (systems of) devices with a wide variety of design processes and defences.

3

Major effort must be put into the development of automated techniques to detect vulnerabilities in complex constellations of digital systems, as well as to guide patching, and to guide these efforts by prioritizing the most dangerous weaknesses. Related to this is a need for attack prediction models, based on empirical evidence which may help security analysts focus on the most important systems and attack vectors, for instance because they

are widely used among attackers, on the rise, or relevant for specific sectors such as energy or finance. In addition to vulnerability analysis, evidence-driven prioritization of what are important attack vectors and modus operandi will provide input and directions to the Design, and Defend pillars.

4 Artificial Intelligence may help us better understand the security and vulnerability of (collections of) modern systems. For instance, AI-based analysis may help developers understand and improve the security posture of systems that have become too complex for humans to fully grasp, and to find patterns that lead to vulnerabilities too subtle for humans to detect. Conversely, attackers may harness the power of AI to create better attacks and to create them faster. 'AI for cyber attacks' is an umbrella term comprising an arsenal that benefits both benevolent and malicious actors. Despite its strategic importance, this area is relatively unexposed in analysis, policy and regulations. Several large countries are making significant resources available for the development of offensive capabilities using AI. It is to be expected that the same applies to criminal organisations. Sovereignty in the digital world mandates the pursuit of deep understanding of these developments which can only be obtained through research.

5 Understanding attacks also entails understanding attackers: gaining a better understanding of developments in new modus operandi, of the changing dynamics of criminal networks, of the maturation and professionalisation of these networks. Research has revealed a double trend in the past years. On the one hand criminal networks increasingly join forces with offline criminal networks, thus merging traditional and digital crime. This leads to novel challenges for law enforcement and prosecution, which need to be studied in more detail. On the other hand, criminal networks increasingly engage in collaborations with, or gain support from, state actors, thus blurring the lines between crime and acts of state aggression. This raises legal, ethical and political questions that require research.

6 Social engineering remains a topic that is high on the agenda, both in terms of understanding the psychological mechanisms (ab)used and the responses this may call forth in victims, and in terms of victimisation: what is the psychological or emotional impact of cyber-attacks on victims and can we detect predictors in terms of behaviour or socioeconomic status for an increased risk of victimisation? The latter is essential is we want to make headway in improving resilience in end users through effective interventions geared towards behaviour change.

Research challenges

1 While important steps have been made in automated vulnerability detection, doing so at scale – across many different systems and devices – remains elusive. Moreover, finding vulnerabilities is one thing, but remedying them in an automated way is the next big challenge. Developments in automated patching and self-healing software are vital in the upcoming years, especially once AI gets into the mix, both as an enabler and as a means for attackers to generate new forms of abuse.

2 Cybercriminal networks are evolving and this requires constant study in different directions: new modus operandi need to be investigated to discover trends and facilitate better defences, the economic and other drivers of cybercriminals need to be investigated, and it is vital that we understand the blurring lines between offline and online crime, as well as between crime and state actor activities.

3

4 When citizens or organisations fall victim to cybercrime, this may have psychological impact on victims. Victim-blaming is sometimes the result, exacerbating the problem. Gaining a better understanding of the psychological impact of cyber incidents on victims may help us change security cultures, develop supportive mechanisms for victims, and raise (organisational and individual) resilience.

Example topics

- Developing (AI) tools for automated vulnerability discovery, with a focus on detection at scale.
- Developing methods and techniques for automated patching and self-healing capabilities for systems.
- Analysing the ethical, regulatory and legal boundaries of AI for cyber attacks.
- Clarifying shifts in modus operandi and the composition of cybercriminal networks and their alliances with state actors.

Use

Understanding the use of technologies in practice

1

By working on security by design and security by default, through high level defences and a good understanding of attacks and attackers many security incidents can be prevented before digital networked technologies enter markets and/or are used in everyday practices by individuals or within organisations. However, in the past decades a large volume of small-scale incidents and a limited number of large-scale crises have taught us that despite our best attempts to prevent attacks and outages, and despite our levels of preparedness, the number and intensity of incidents is increasing. This means that it is essential that we understand why incidents occur in practice in different contexts of use, and in different application domains. Due to the wide variety of use contexts, there is significant room for understanding and addressing cybersecurity challenges in relation to the combinations of technical factors, human behaviour and cultural aspects that define each setting. With the rise of smart environments and smart infrastructures, understanding security challenges in and through the use of systems, networks, and data becomes ever more pressing. Understanding security cultures in organisations may help raise cybersecurity, as does a better grasp of the root causes of cyber accidents — outages and errors that result from non-intentional behaviours or as a result of technical and human accidents.

2

Making steps to improve the user-friendliness of security (related) solutions is also essential, so that end users will be less inclined to make mistakes that endanger their security. One relevant research area in that respect is usable security. Usability aspects have long been ignored in security and privacy research. For instance, while solutions such as PGP solve many email security challenges, for most ordinary users they are far too advanced. Modern message apps often tend to use built-in end-to-end encryption, which is a big improvement from a usability perspective. From a security perspective, there is still room for improvement in these message apps, since authentication is limited and based only on a phone number – which can fail easily (see Signal-gate in the US).

3

For both organisations and end users it would be beneficial to gain more insight into the effectiveness of cybersecurity interventions and protective mechanisms. Currently, organisations train staff to increase their

cybersecurity awareness or change their cybersecurity behaviours, but many training mechanisms have not been proven effective, or have been proven to have no effect. Similarly, when organisations invest in technical cybersecurity controls or roll out new procedures, being able to measure the effectiveness compared to the cost of these interventions is useful, and will promote the wider adoption of these controls, ultimately bringing straightforward security for digital networked technologies closer.

4 Furthermore, to boost resilience, it is also important that sectors and governments gain more insight into what security technologies ought to be prioritized for their ecosystems, by engaging in continuous measurements and assessments of the deployment of security and resilience technologies and best-practices. Such a macro-level 'resilience monitor' is also helpful to increase the Netherlands' preparedness in today's era of geopolitical tensions. A continuous and integrated view on the security and resilience of the digital infrastructure that the Netherlands depends upon does currently not exist.

5 Effective and logical IT (security) architecture decisions at the level of individual organisations may sometimes have a negative impact on the collective level, such as centralization of the digital infrastructure and loss of digital sovereignty. Most Dutch organisations now use office products and cloud services provided by a small group of American big tech companies. At a collective level, this leads to risks and suboptimal resilience. One area of research would be to study which incentives could be used to motivate organisations to consider the systemic impact of their IT architecture decisions.

6 A sixth area of research revolves around laws, regulations and standardization. First and foremost, with the advent of new legislations for cybersecurity, such as NIS2 and CRA, it is important to understand compliance in organisations, and to study the effects of these new laws on markets, on vendors and distributors. The increasing demand for certification, for instance in the EU, plays a role in this dynamic as well, as does the development of the institutional landscape involving oversight and enforcement. Research on dual use remains high on the agenda in relation to different use contexts, too: how do we regulate the use of new and existing technologies that may serve both benign and dangerous purposes?

7 Finally, the use of social media keeps growing in terms of volumes and importance, especially for younger segments of the population. To increase the secure use of social media

research is needed on both the technical aspects (architecture, cloud storage, privacy preserving techniques), on human behaviour (information sharing practices, the role of disinformation), and on the legal and governance aspects of social media (the power of big tech, privacy and data protection, European alternatives for cloud and social media platforms).

Research challenges

1

Compared to research on design, defend and attack, studies into aspects of the use of digital networked technologies are a relatively recent new branch on the research tree, with most of the focus going into behavioural, organisational or legal, regulatory and governance studies. Integrating ideas, theories and perspectives from these different strands of social science would be beneficial. For instance, behavioural and psychological studies on individual use practices could be enriched with insights and methods from organisation and inter-organisation network studies, or from Science & Technology Studies (STS). Organisational and management studies, by contrast, could benefit from theories and perspectives at the microlevel such as those brought forth by psychological or criminological methods and theories. Integration or alignment with technical perspectives would further enrich the field.

2

As the description of the seven research areas under this pillar reveals, 'use' can be studied at different levels. First, at the micro-level, which ranges from individual end users to groups of end users, to organisations. Or second, at the macro-level, for instance by focusing on national governments and the governance of the ecosystem or even reaching to the global level. This entails that a much wider variety of studies – and disciplinary lenses -- can be brought to bear under this pillar. Building shared and coherent narratives, theories, methods and vocabulary can be challenging.

Example topics

- Developing better insights into the role of security culture as well as a clearer understanding of the ways in which to strengthen security culture, with a focus on different application domains, such as energy, transport, or finance.

- Developing effective, strong usable security mechanisms for the protection of end users (e.g. relating to crypto or access management).
- Developing measurable, effective security interventions for organisations, including but not limited to cybersecurity trainings.
- Developing resilience monitoring capabilities for sectors and/or the national government.
- Developing economic or organisational incentives so that decision-makers may include parameters such as strategic autonomy and digital sovereignty in their choices for particular IT (security) architectures.
- Analysing mechanisms that may affect compliance with cybersecurity (related) regulations and legislation, and/or the impact of (changes in) their enforcement, and/or changes brought about by the use of certification and standardisation.
- Developing mechanisms for better security, privacy and protection of end users in relation to social media.

Recover

When incidents happen...

1

With the growing complexity and density of digital networked technologies there is an increasing likelihood that incidents will happen from time to time, despite our best efforts to follow security by design and security by default principles, and despite advanced prevention and detection techniques. Until now, the number of large-scale attacks that debilitate entire sectors, nation states or even regions is limited. However, geopolitical instability, ever more advanced international criminal and state-actor activity, and increasing interconnectedness with and dependency on global platforms and systems warrant investments in preparedness for incidents and crises, and a focus on resilience, on the ability to bounce back quickly and efficiently once incidents and crises do occur. Resilience is not just a theme for cybersecurity in the Netherlands but has gained traction more broadly in light of rising geopolitical tensions and a high interdependency of systems, communities and states. In this light, the notion of 'whole of society' preparedness gets growing attention, both in the Netherlands and in the EU. This concept was promoted by the United Nations with respect to the threats of climate change, but has recently also been adopted by NATO to mobilise a broad range of societal resources to enhance socio-technological and economic resilience. Recovery in this perspective is taken to a higher level: it comprises structural adaptations and innovations across a wide range of interdependent systems and sectors, while involving a wide range of different actors. Recovery from incidents and increased resilience require technical knowledge and expertise, for instance with respect to high-level forensics, gathering threat intel and engaging in the technical side of incident response. Similar to the discussion on automated vulnerability discovery and automated patching, here, too, the issue of scale is pressing: being able to do forensics faster, and gathering and sharing threat intel at a larger scale would greatly improve the security of networks and systems.

2

Increased recovery capabilities and better preparedness also require insights into law and regulation on the one hand, and politics and policies on the other. And for a whole-of-society approach to work effectively, a keen understanding of human behaviour, both on an individual level and in groups, and both during a 'cold phase' and a crisis, is required.

3 Recovery, preparedness and resilience have different aspects, that all require research. Resilience has become a blanket term that is used for any activity ranging from risk management and the prevention of incidents, to increasing the robustness of systems, to the ability to adapt to change, and to the ability to bounce back quickly after an incident has materialised. Conceptual and theoretical clarification and demarcation of these different interpretations may further the field by laying foundations for e.g. frameworks and standards on all elements.

5 A key element of preparedness is scenario planning and conducting crisis exercises. A weakness in this approach to preparedness is that we create scenarios for and practice what we expect, not what may actually happen. Strengthening foresight capabilities is a key area of contribution for science.

4 Recovery, by contrast, involves acting effectively and efficiently after an incident or crisis, by using technical expertise to get systems back online, but also by having effective crisis management structures in place, and by creating a governance landscape with sufficient democratic checks and balances that contains e.g. a clear division of responsibilities between government and private parties for crisis management, crisis response and crisis coordination. Research may contribute to strengthening the Netherlands' recovery capabilities on all these aspects.

6 Moreover, learning from past incidents is crucial. Information exchange within and between organisations is crucial in this respect. Today, there are practical, economic, reputational and legal obstacles that get in the way of structural, large-scale incident information sharing. Research may shed light on the validity and extent of these obstacles, and may contribute to overcoming such hurdles.

Research challenges

1 'Whole of government' and 'whole of society' are often proposed as a key to increasing economic and societal resilience in high tech societies. The idea behind these visions is that complex challenges such as, for instance, ensuring that our society and economy can withstand and absorb shocks because of digital attacks or outages, cannot be a responsibility for a single government entity on its own, or even for a couple of government entities. Instead, it should be a responsibility for the entire government, or even for society

as a whole. Every citizen and every organisation should bring its capacities to bear – proportional to the weight each can carry – to maximise our collective resilience. While this sounds fair, at the same time there is a risk that a notion such as 'whole of society' will be used by parties to shift responsibilities on others, especially on those with less power. While respecting the need for shared responsibilities to accomplish true resilience, then, 'whole of society' should not remain an empty phrase – researchers working on preparedness and recovery might contribute to a critical and foundational assessment of its meaning and value for crisis preparedness and response, and to dialogues on ethics, mutual expectations and trust between civilians and governments.

Cyberspace is a dynamic domain in which both opportunities and threats are in constant flux. Drawing lessons from past incidents and crises with respect to such a dynamic ecosystem requires a fundamental rethink of what it is we want to remember from these events, and how we can make them productive for the future. For learning at a larger scale collecting data in a structured fashion and archiving them is a challenge as well.

Example topics

- Developing improved threat intel and forensics tools and mechanisms, especially at scale.
- Using best practices and lessons learnt from 'whole of government' approaches in other countries to provide input for government policies and laws in the Netherlands.
- Developing conceptual and theoretical clarity on 'resilience' in the context of cybersecurity.
- Improving scenario studies and crisis exercises for digital and hybrid crises.
- Developing integrated recovery methodologies, on the basis of insights from technical, organisational, behavioural and policy-making studies.
- Developing models and mechanisms to understand the current obstacles in learning from past cyber incidents and cyber crises, as well as to (partially) overcome such hurdles.

Science & society

Connecting scientific research with societal challenges

The fact that scientific research has merits for society and for our economy has been proven many times over, not just in vast knowledge accumulation over the centuries, but also through innovations in medicine, energy, industry and production, housing and infrastructure, travel and mobility, and of course in digital technologies. Without scientific research many of the products and services we consider essential today would not have existed. Science helps us understand the world around us better, and to discover innovative ways to make our lives safer, healthier, happier and wealthier. Cybersecurity is one of the grand challenges, or 'wicked problems' [13] of our time. Scientific research generates knowledge and insights that help us understand this challenge and find ways to address it.

The NCSRA-IV clarifies those areas in which cybersecurity research in the Netherlands can make key contributions in the upcoming years. On the one hand it shows which scientific knowledge and expertise is already available in the Netherlands – it provides an overview of the areas we already excel in. On the other hand, the Research Agenda shows which scientific knowledge and expertise we need to develop (further) in the upcoming years in order to address the cybersecurity challenges we face. The National Cybersecurity Research Agenda IV lists the **key topics and themes** that researchers in the Netherlands deem most valuable for the upcoming years, in one of three respects:

1. They may further our **understanding of the societal and economic challenges** we face with respect to cybersecurity, thus providing solid foundations for innovation in the field;
2. They may generate such innovations, i.e. **provide solutions** for real-world societal and economic challenges that are currently visible or on the near horizon;
3. They may generate **fundamental knowledge or insights to advance cybersecurity research in the international arena**, which may (or may not) translate into innovations and solutions for the societal and economic challenges in the longer term.

Explaining the function of the Research Agenda might well be done by comparing it to cooking. The NCSRA-IV provides a menu consisting of multiple dishes in several courses that collectively lead to a wholesome meal, not

a recipe with steps to take for the creation of a single dish. Which of the dishes will be created in each course depends on the choices of researchers themselves, but also on the broader landscape surrounding the universities and universities of applied science in the Netherlands. It relates to the policy directions and legislative/regulatory agenda of the Dutch government, to the funding made available for cybersecurity research in the upcoming years, and to the programmatic choices that guide research and innovation themes, for instance in relation to the energy sector, in developments in OT, or AI. It also connects with market demand and with the role of the government as launching customer for innovative technologies, products or services. Finally, it ties in with scientific and industry-related developments abroad, in the EU and in other parts of the world.

Science is slow, science is fast

One thing to note about the connection between science and society is that they oftentimes move at different paces. Scientific research regularly takes a long horizon, focusing on bigger or more fundamental challenges in the middle long-term. Moreover, scientific findings may take many years, if not decades, to be translated into everyday products or services that directly benefit society. Society, on the other hand, often looks to science to solve the problems of today and tomorrow, with practical outputs that can lead to benefits or gains in the near term. This may lead to a disconnect between expectations from society on the one hand and abilities to show the value of academic research on the other. At the same time, science is also fast compared to society in the sense that, because it focuses on further horizons and is the result of international collaboration, it often sets the agenda for new topics, themes and areas of knowledge development. Research may lead to cutting-edge insights that go against, or are different from, accepted practices, standards or beliefs in society. For scientists it can be frustrating at times to see how slowly society absorbs ideas and innovations that result from scientific progress and how long societies hold on to products, services, and knowledge that have been proven false, ineffective or insufficient in science.

What this discrepancy between science and society, operating at different speeds in different respects, reveals, is that research lays the foundation for a ladder with several different rungs that all collectively lead to

innovation. The discrepancy itself cannot be resolved — and is necessary for science and society to play their respective roles. Creating and maintaining a solid innovation ladder with sufficient interconnections is important for Dutch society, however. The Netherlands Cybersecurity Strategy 2022-2028 points out the urgency of improving the connection between cybersecurity research and the market [11]. This Research Agenda contributes to strengthening that connection by providing the bottom rungs of the innovation ladder.

Many strategies and agendas, a single drive

In recent years there is a call for more coherence with respect to cybersecurity in the Netherlands, with respect to policy focus and to channelling budgets as a consequence of that focus. A straightforwardly secure cyberspace with respect for the fundamental values that we hold dear in the EU is the main drive behind this focus — which aligns with the research community's agenda as laid down in this document. Two key policy documents guide the way and form the overarching umbrella:

1. The Netherlands Cybersecurity Strategy 2022-2028 (NLCS) with its vision that cybersecurity ought to be "a given for everyone" [11] and an emphasis on straightforwardly secure architectures, networks, products and services for all citizens; and
2. The Digitalisation Strategy [10], which sets the agenda for the use and development of digital technologies in the Netherlands and emphasizes the importance of technology design that embodies and promotes the fundamental values, freedoms and liberties that Europeans embrace.

Based on the vision laid down in these two strategies the Netherlands has developed a National Technology Strategy (NTS) in 2024 [14], which expresses ten key enabling technologies that the Netherlands will prioritise for the next decade because they contribute to Dutch earning potential or international competitive advantage, play a role in Dutch societal missions or are important for the Dutch autonomy and national security. Cybersecurity is one of the ten key enabling technologies. The text on cybersecurity in the National Technology Strategy mentions 7 ambitions for the years 2025-2035. The Ministry of Economic Affairs is currently working on the so-called Action Agenda Cybersecurity, in which the ambitions of the National Technology Strategy are

translated into a concrete framework to give guidance to and support research and innovation on this topic in the upcoming years.

There are clear connections between the latter document and the National Cybersecurity Research Agenda IV. The Action Agenda Cybersecurity is the programmatic basis upon which research and innovation programs and funding will be made available in the upcoming decade. Vice versa, the Research Agenda aims to feed the content and direction of the Action Agenda Cybersecurity, by making explicit which research themes are important for cybersecurity in the Netherlands in the upcoming decade. Thus a coherent research and innovation landscape may emerge, building up to the solid innovation ladder mentioned above.

Colophon & acknowledgements

The National Cybersecurity Research Agenda IV was written by prof.dr. Bibi van den Berg (Universiteit Leiden, ACCSS), dr. Ben Kokkeler (Avans Hogeschool, PRIO) and Melanie Lemmen (NWO).

A large group of people provided input, helped edit and revise, and contributed to the vision and the research themes in this agenda. A special thanks goes to prof.dr. Cristian Hesselman (Universiteit Twente), prof.dr. Herbert Bos (Vrije Universiteit Amsterdam), prof.dr. Bart Jacobs (Radboud Universiteit Nijmegen), prof.dr. Michel van Eeten (Technische Universiteit Delft), dr. Marten van Dijk (Centrum voor Wiskunde en Informatica), prof.dr. Lokke Moerel (Universiteit van Tilburg), dr. Zeki Erkin (Technische Universiteit Delft), dr. Remco Spithoven (Saxion Hogeschool), dr. Jeroen van der Ham (Universiteit Twente), dr. Martine Groen (Hogeschool Utrecht), dr. Peter Novitzky and dr. Rick van der Kleij (Avans Hogeschool), dr. Erik Schrijvers (NIPV), Joeri Toet (Vrije Universiteit Amsterdam) and Eveline Vreede (Technische Universiteit Delft).

Throughout the process of composing this Research Agenda a steering committee provided supervision over both the process and the content. Many thanks to Eddy Boot (dcypher), Dirk Jan van den Heuvel and Liesbeth Holterman (Cyberveilig Nederland), Christiane Klöditz (NWO), Fadime Keçe and Martijn Neef (Ministerie van Economische Zaken).

ACCSS and PRIO thank dcypher and NWO for co-organising three meetings with scientists and stakeholders from the field, for financial and practical support, and for chairing the board that supervised the creation of this agenda.

References

[1] S. Kemp, '*Digital 2025: The Netherlands*', DataReportal – Global Digital Insights, 25-Feb-2025. Available at https://datareportal.com/reports/digital-2025-netherlands.

[2] European Commission, '*Digital Decade DESI visualisation tool*'. Available at https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts/desi-indicators?period=desi_2024&indicator=desi_iuse&breakdown=ind_total&unit=pc_ind&country=AT,BE,BG,HR,CY,CZ,DK,EE,EU,FI,FR,DE,EL,HU,IE,IT,LV,LT,LU,MT,NL,PL,PT,RO,SK,SI,ES,SE.

[3] International Trade Administration (Trade.gov), '*Netherlands - digital economy*'. Available at: https://www.trade.gov/country-commercial-guides/netherlands-digital-economy.

[4] Statista. '*Online and mobile banking usage in the Netherlands 2020-2023, by age*'. Available at: https://www.statista.com/statistics/575490/share-of-individuals-using-internet-banking-in-netherlands-by-age-group/.

[5] Statista. '*Social media usage in the Netherlands - statistics & facts*'. Available at: https://www.statista.com/topics/5524/social-media-in-the-netherlands/.

[6] Statistics Netherlands (CBS) (2023), '*Nearly 8 in 10 people shop online in 2023*', Centraal Bureau voor de Statistiek. Available at: https://www.cbs.nl/en-gb/news/2023/49/nearly-8-in-10-people-shop-online-in-2023.

[7] R. Harmsen, (2025) '*Economic impact*', Dutch Data Center Association. Available at: https://www.dutchdatacenters.nl/en/data-centers/economic-impact/.

[8] Ecorys (2024) '*Economisch belang van digitale infrastructuur in Nederland*'. Available at: https://www.ecorys.com/nl/case-studies/economic-importance-of-digital-infrastructure-in-the-netherlands/.

[9] Amsterdam Smart City (2016), '*Dutch digital infrastructure: engine of economic growth and prosperity*'. Available: https://amsterdamsmartcity.com/updates/news/dutch-digital-infrastructure-engine-of-economic-g.

[10] Ministry of Economic Affairs and Climate Policy (2021), '*Nederlandse Digitaliseringsstrategie 2021*'. Available at: https://www.rijksoverheid.nl/documenten/kamerstukken/2021/04/26/nederlandse-digitaliseringsstrategie-2021.

[11] Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), '*Nederlandse Cybersecuritystrategie 2022-2028 (NLCS): Ambities en acties voor een digitaal veilige samenleving*', Avaliable at: https://english.nctv.nl/documents/publications/2022/12/06/the-netherlands-cybersecurity-strategy-2022-2028

[12] Militaire Inlichtingen- en Veiligheidsdienst (2025) '*Openbaar Jaarverslag* 2024', Available at: https://open.overheid.nl/documenten/204ba7fc-ee17-4209-b5c7-fdeaa21180ca/file

[13] Rittel, H. W. J. & Webber, M. M.(1973), '*Dilemmas in a general theory of planning*',. Policy Sci. 4, 155–169.

[14] Ministry of Economic Affairs and Climate Policy (2024), '*National Technology Strategy: Building Blocks for Strategic Technology Policy*'. Available at https://www.kia-st.nl/en/kia-key-enabling-technologies/national-technology-strategy-nts