

# NCSRA



National Cyber Security Research Agenda

# Preface

The challenges we face in the digital domain are very real. On a daily basis Dutch society is threatened by cyberattacks in varying degrees of severity and from various actors. As societies become ever more digital, managing security risks is now more urgent than ever. To deal with these threats we need state of the art knowledge that will guide us in formulating effective policies. A strong foundation of cybersecurity knowledge and understanding is also vital for the education of our next generation of cybersecurity professionals. This is not, as traditionally seen, exclusively the domain of scholars and universities. In cybersecurity it must be a collaborative endeavour of science, business and government.

This is why I am pleased to see that this National Cyber Security Research Agenda, the third edition (NCSRA III), has been a far-reaching collaborative effort. The Dutch Cybersecurity Platform for Higher Education and Research (dcypher) has brought together a team of main authors/editors from academia and has taken a central role in coordinating the input from additional experts from the public, private and academic domains. The main authors have fully embraced the modern working tools of collaborative editing and have been open to the contributions from various disciplines, for example social science, humanities, computer science and engineering. This agenda has additionally been aligned with the efforts of the Dutch Top Sectors and those of the National Research Agenda (NWA) research routes. Various experts have been interviewed in order to target the particular cybersecurity concerns of the widening Dutch digital landscape. It also included a field consultation where experts were able to speak to the main authors and provide their ideas for the text in near-real-time.

This agenda is a true product of the triple helix approach to research. We hope the contents of this agenda will shape the research future of the field, creating new technologies, solutions, and routines that will make our society safer in the digital domain.

The NCSRA III provides a backbone to fulfil the ambitions of the National Cyber Security Agenda (NCSA). The NCSA includes concrete goals and measures to enhance cybersecurity in the Netherlands. The research pillars of the NCSRA form an excellent guide for researchers and can help them to select cybersecurity research topics. This leads to knowledge development in the field of cybersecurity that contributes to achieving the ambitions of the NCSA and lay the groundwork for a more secure digital domain in the Netherlands.

## **Dick Schoof**

National Coordinator for Counterterrorism and Security,  
co-chair of the Netherlands Cyber Security Council



# Content

Pillars and Research Themes	4
 Design	8
 Defence	12
 Attacks	16
 Governance	22
 Privacy	26
Context & Societal Ambitions	30
Acknowledgements	36
Abbreviations	37
References	38

# Pillars and Research Themes

## About this Agenda

For the 2018 edition of the Dutch National Cyber Security Research Agenda (NCSRA) we decided to use a different approach compared to the earlier two versions. The NCSRA III is no longer framed as a list of concrete research themes. Such lists tend to reinforce disciplinary boundaries, are often a bit haphazard, and more importantly, they describe a topic area rather than a research direction. In this edition, we describe five pillars with a relatively high level of abstraction. These pillars are the capabilities and requirements we need for cybersecurity and therefore span the full spectrum of cybersecurity research. Each pillar requires contributions from computer science, engineering, social science and the humanities. In other words, each pillar represents the overall objective that should be achieved through the specific research projects within that topic.

Field consultations were part of the process composing this agenda. They started off at the dcypher Symposium 2017 and were followed by interviews with representatives of economic top sectors and research routes of the

Dutch National Research Agenda (NWA). A questionnaire was designed as guidance for the interview process. Questions promoted contributors to share how cybersecurity may positively impact a (top) sector, research route and/or societal challenge. In addition to the one-on-one consultations, a larger and more inclusive consultation meeting was held with representatives from industry and government. These broad consultations contribute to dcypher's belief that one single national cyber security research agenda is sufficient within the Netherlands, and should transcend the top sectors and NWA research routes, and should align with the societal challenges of a secure digital society.

Predominantly, the NCSRA III provides a roadmap for technical solutions to address technological challenges that cause social impact. Though the agenda promotes further research into societal solutions, the authors recognize that there is some emphasis on technology. As the field of research addressing social challenges within cybersecurity is growing, we envision that the next reiteration of the NCSRA will address the humanist and behavioural side of cybersecurity to an even larger degree.

## Introduction

We are rapidly evolving into a digital society. This creates huge opportunities for advancements, but also makes us more dependent on technologies. This dependence makes us vulnerable. Attacks come from a variety of sources, ranging from young kids, via organized crime to state actors. All aspects of our daily lives, from pacemakers to power plants, and from DigiD and social media to IoT, depend on the trustworthiness of our ICT infrastructure. The cybersecurity risks to our critical infrastructures are only growing as they become ‘smarter’, with for instance smart grids to cope with the energy transition or intelligent transport systems to cope with higher densities of traffic.

In early 2018, the whole connected world was talking about two new vulnerabilities, Meltdown and Spectre, which both affected almost all computer systems worldwide. Rather than software issues, these were *hardware* vulnerabilities, making them more difficult to fix. Meltdown and Spectre are just two of a wave of new hardware vulnerabilities that have appeared in recent years. While until recently we would have dismissed attacks using such vulnerabilities as science-fiction, we now know they are a truly realistic threat.

Around the same time, several Dutch banks were victims of a series of DDoS attacks, which continued for multiple days and were more extensive and advanced than previous attacks. It was later discovered that these attacks required little technical skill and were launched by an 18-year young man, using a “DDoS as a Service” website, of which hundreds can be found online and in the dark web.

Hardware vulnerabilities and DDoS attacks are just some of the many security issues that we witness today. In 2017 the NotPetya ransomware attack hit, amongst others, APM Terminals in the port of Rotterdam. The damage caused by this attack in Rotterdam alone reached as high as hundreds of millions of Euros. Earlier in the same year the Wannacry ransomware attack even put the lives of patients in UK hospitals in danger.

Apart from cyber criminals, state actors are also increasingly launching cyber-attacks. For example, in 2018 the German ministry of foreign affairs was hacked by groups with alleged links to the Russian government. The leaks of the Democratic National Committee in the US in 2016 demonstrated that attackers have the motivation to interfere with elections and that the dependence on ICT makes the most advanced nations more vulnerable to such attacks. The list of high-profile attacks goes on and on: The German parliament was hacked, allegedly by the Russians, Belgacom was hacked, allegedly by the British, Iranian nuclear facilities were hacked, allegedly by the US and Israel, and Ukrainian power plants were compromised by, allegedly, Russia. The attacks mentioned above were fundamentally different from previous attacks we have seen. These attacks mark a shift in motive, signalling a change from disruption for economic profit to disruption to influence societal values and fundamental rights.

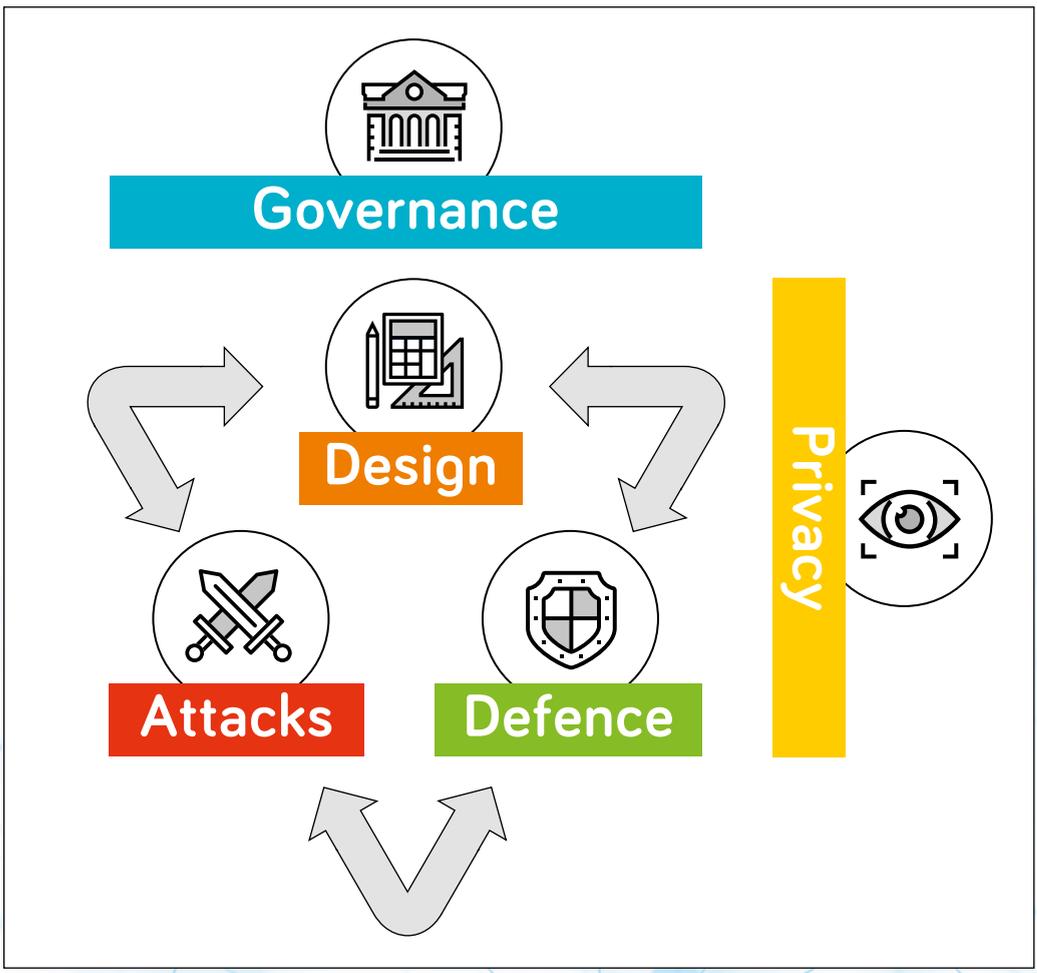
The Netherlands has the ambition and ability to keep its digital society safe and secure. Our cybersecurity should depend as little as possible on foreign countries and organizations. Digital sovereignty should be high on the agenda of Dutch politicians, agencies and companies. A crucial requirement for digital sovereignty is a strong and independent cybersecurity knowledge infrastructure. Executing this agenda is prerequisite for keeping our knowledge infrastructure strong!

### Five cybersecurity research pillars in perspective

The NCSRA III describes the research challenges in cybersecurity and privacy around five pillars.

These five pillars are:

- 1. Design
- 2. Defence
- 3. Attacks
- 4. Governance
- 5. Privacy



Our assumption is that all cybersecurity and privacy research fits under this set of five pillars. When concerning cybersecurity, we want and expect the *best possible design, defence, governance, and privacy*. We also need a better understanding of *attacks*. We need such knowledge to understand what we are up against and what our weaknesses are, to test designs and defensive measures, and to disrupt and take down malicious infrastructures.

In the following sections each pillar is described using the following template:

- Summary
- Discussion of links & overlaps with the other four pillars
- Motivation
- Research challenges associated with this pillar
- A small sample of possible topics

As each list of example topics is inevitably going to be limited, we include them mainly for illustrative purposes. Each pillar contains many more topics. It should be noted that actual research questions are going to be more specific than these topics. The ambition of the NCSRA III is for projects to combine approaches associated with hitherto different topics, disciplines and expertises. Overall, the agenda supports an interdisciplinary approach, including reflections on the societal and normative values at stake. As a society, we need novel and boundary-crossing proposals that innovate beyond the state of the art and increase our capability in each of the areas of these pillars. To illustrate this, we include five examples of the kind of innovative research questions we hope each pillar will solicit. An additional example touches two pillars.

### Design:

“What are the most effective methods to deploy in the development process in order to achieve systems that are secure by design?”

### Defence:

“How can we build and embed fully-supervisable systems and software in our defensive capabilities?”

### Attacks:

“How can we better understand the attack surface of increasingly complex ecosystems that involve hardware, software, and people?”

### Governance:

“Which national and international regulatory frameworks for intermediate liability of network operators cause more resilient networks and lower incident rates?”

### Privacy:

“How to protect people in a world obsessed with their data?”

### Cross-pillar question (Attack & Defence):

“How can we create a self-healing system that can automatically detect vulnerabilities, and automatically generate and apply patches for these vulnerabilities?”



# Summary

Many security problems can be prevented by designing systems and services to be more secure before they are deployed in a live environment in the real world. Designs should ideally take security into account right from the start, in what is known as Security-by-Design. For the purposes of this research agenda, we take a very broad view of what constitutes “design”, including all the activities in the software and hardware development life cycle prior to the system being deployed, from the initial requirement engineering phase to the actual implementation and final testing\*. The precise border between development and deployment may be difficult to draw, as, for example, trends in software development such as Agile, DevOps and continuous delivery are blurring the distinction.

\* One could argue that this pillar should be called Design & Build, but we opted for the more concise term Design instead.

## Links with other pillars

Design is closely linked with

- **Privacy:** Design is linked with Privacy, as Security-by-Design and Privacy-by-Design should be part of one and the same process.
- **Governance:** Design is linked with Governance as studies into the incentives for adoption of new secure technologies and designs methodologies are crucial for ensuring deployment.
- **Attacks:** Understanding attacks and attackers are important pre-requisites to designing secure systems. In fact, the very definition of what it means for a system to be secure requires a clear understanding of the attacks it has to withstand. There is even a partial overlap between Design and Attacks as test techniques for security are effectively also attack techniques.
- **Defence:** Design and Defence can – or may have to – complement each other. For instance, there may be a choice between *preventing* a certain security problem or *detecting* it – assuming one can *recover* from the problem. When designing a system, we need to understand the possibilities for defending it, in order to make wise choices about design trade-offs in prevention vs detection. A good design will have to provide features to facilitate good defence, such as secure logging and management controls.

In the end, Design, Defence, and Attacks all co-evolve, with better practices in design and defence trying to keep up with improved attacks, and new attacks evolving to circumvent advances in design and defence.

## Motivation

Despite the great advances that have been made in building more, and ever more powerful systems in the past decades, we are still not capable of building 100 percent *secure* ICT systems. A lot of fundamental work is needed to develop more secure designs. This spans innovations to make hardware more attack resistant; innovations in tool chains to better support

secure design and development, such as new compiler techniques or testing methods; innovations in organizational practices to come to a secure software development; innovations in improving usability to steer users into secure behaviour; and secure designs tailored to specific environments, such as for low-powered devices in the Internet of Things.

## Research Challenges

Carrying out *secure system design* and *secure software engineering* are still major research challenges, for all the phases in the development life-cycle: from requirements analysis, architectural principles, to tools and techniques for security analysis. The over-arching question is how to perform *security assessments* to provide mission assurance about the security of products, services and processes.

Striking the right *balance between usability and security* is a recurring and crucial challenge in design. The systems we build are socio-technical systems, that consists of more than just ICT: they involve users, administrators, developers and maintainers. Secure solutions that are too cumbersome to use will fail to be adopted, and complex solutions that are tricky to implement, configure, or maintain will not be secure in the long run.

## Smart industry security

A key consideration is that the security of singular component systems does not guarantee the security of overall combined cyber-physical systems that are the result of 'plug and play', servitization / customization, custom product configurations and automatically reconfigured supply chains.

### Smart Industry Roadmap



Apart from methodology to build more secure systems, we also need secure building blocks and technologies as components. These components include authentication mechanisms such as *biometrics*, the platforms provided by hardware, programming languages, APIs, operating systems, cloud solutions and other online platforms that play a vital role in modern ICT ecosystem, and attestation mechanisms to attest to the security of these platforms. Building more secure systems requires better usage of these technologies, but also improvements of these technologies. Cryptology is an important technology that will be used in new innovative ways, but also comes under threat from advances in computing technology, in particular quantum computing.

### Example Topics

- Usable security and user-centric design, also taking the user's (mobile) devices into account
- Shaping secure end user behaviour through design
- Understanding and countering (dis)incentives for good security practices, for users and for developers alike
- Security solutions for device management for industrial and consumer products, including IoT devices, spanning the entire lifecycle
- Coping with legacy systems and design for upgradeability
- Resilient design for security in insecure environments
- Security assurance in agile, DevOps, and continuous delivery paradigms
- Methodologies for security assessment and certification, for concrete products and services, and for higher level specifications and designs (e.g. by logical analysis, analogous to provable security in cryptology)
- Safer programming languages, APIs, and platforms. Safer compilers for unsafe languages, with associated secure coding guidelines and best practices
- Compartmentalisation solutions for hardware, software, and networks
- Post-quantum crypto, and associated migration paths
- Side-channel resistant design of hardware and software

### Experienced security, privacy and trust

Maximum technological security and privacy guarantees are not always in line with the trust users of digital systems experience. Affective trust is as important as cognitive trust for secure digital environments. Research may support the creative industry optimizing trust of users in the digital domain, through design, interaction design and communication design.

### Secure behaviour

Human behaviour is the greatest risk for cybersecurity: ignorance, laziness or naivety of implementers and users make systems just as unsafe as technical imperfections. The creative industry and its tradition of “design for behavioural change” can answer the question of how to encourage sensible choices and secure behaviour.



**Top sector Creative Industry can offer added value to cybersecurity research by a user centric approach**

# Defence



# Summary

Regardless of how good we are at designing and building secure ICT solutions, we cannot – and should not – expect that all security problems can be prevented. Systems, both newly developed and legacy, and organizations need to be defended. In this section, ‘defence’ means the set of tools and processes that need to be put in place after a system is deployed, to *discover and identify* assets to be defended, *prevent* and *detect* attacks and security problems, to respond to incidents, mitigate the impact of attacks, and to recover from them. This covers a broad range of techniques, both at technical and organisational levels, ranging from intrusion detection to internal processes for security, from patching to human aspects such as behavioural influencing, training and awareness of users and system administrators.

## Links with other pillars

Defence is closely linked with

- **Design:** Lessons learned in defending systems should ultimately feed back into better design. Conversely, systems can be designed with defensibility in mind. An example of this is by providing good possibilities for logging and monitoring and responding to attacks.
- **Attacks:** Understanding attacks is crucial to prevent and proactively detect attacks and effectively respond and recover. Capturing and automated sharing of this understanding in Cyber Threat Information sharing can be of great value for Defence. Testing defences by simulating attacks is another link to this pillar.
- **Governance:** Empirical data gathered by defences is valuable information to improve governance.
- **Privacy:** Achieving privacy protection starts from solid defence foundations, such as in how we detect leaks, tentative attacks, and contain them.

## Motivation

Defence is an area of security where there is a clear need for disruptive innovations. In the battle between cyber-attackers and cyber-defenders, the cyber-defenders seem to be losing terrain. This is true both from the quantitative and the qualitative viewpoints. From the qualitative point of view, recent attack campaigns show that it is dismayingly easy for attackers to inflict serious damage, as seen by the cases of Black Energy Industroyer, WannaCry, NotPetya. It was also shown that even the most well-kept forts were vulnerable to being penetrated, as the attack on the Italian based company, HackingTeam demonstrated. Attackers have an easier task than defenders, mainly due to the fact that the attack surface is constantly expanding. Recent IoT-based attacks have demonstrated that even seemingly uninteresting devices such as video recorders, CCTV camera's and 'smart' fish tanks can be leveraged by criminals to carry out large DDoS attacks and to penetrate inside the logical perimeter of targeted

corporations. The threat landscape is evolving continuously, the level of automation, and the speed of cyber-attacks is increasing while Incident Response is still a predominantly human-based process. Similarly, human aspects such as social engineering, phishing, and insider threats remain a challenge that must be addressed to secure our systems and processes.

## Research Challenges

The primary general need for this pillar is to dramatically increase the efficiency and the effectiveness of defensive measures, which is to be understood as the speed at which attacks are detected, understood and responded to. A recurring challenge in monitoring is obtaining useful information from huge amounts of log data. There is a need for effective defences at many levels. At the high level for corporations effective defences are needed, where events are aggregated and analysed in SOCs, then down to the network level, the host level, and device level. At the device level, research on host-based protection such as control flow integrity is needed to counter new forms of attacks focusing on the lower parts of the software stack. An example of this can be seen in firmware, like in the HatMan malware affecting specific PLCs.

New solutions to authentication, and internal processes for security at the organization level must be developed. Better defence requires better risk management under uncertainty, with new techniques for asset management

## Reliable transition management

By switching to non-fossil fuels, electricity will fulfil a much larger share of our energy needs. Digitization of the power supply requires research into (new) vulnerabilities in equipment, networks and processes, connected worldwide via the Internet, which may impact their accessibility. A challenge of a public-private nature is reliable transition management of the electricity supply.

**Raad voor de leefomgeving en infrastructuur (Rli)**



## Development of security methods to cover threats for connected automated driving

Already today, cybersecurity and vehicle safety are strongly linked due to continuously increasing connectivity. Higher levels of vehicle automation even increase the need for secure electronics architectures significantly. On one hand, vehicle control will be automated: the human driver will not be enabled to intervene immediately in case of a cyber-attack. On the other hand, in many automation use cases, off-board data will be used for immediate driving decisions. The used data channels are potential entrance gates for attacks. The challenge is to protect the electronics architecture from remote attacks in general and in particular for automation. To ensure accessibility and integrity of automated driving related data, these have to be constantly and reliably accessible and its integrity must be guaranteed.

### Top sector HTSM - Automotive



and attack surface evaluation. We must develop techniques to identify which controls are most effective, how to account for often-overlooked productivity effects of security policies, and to develop new technologies to contain the effects of the suffered impact, such as by deceiving the attacker on the successfulness of their attack.

At the same time, there is a call to develop new enabling technologies for information and intelligence sharing, as well as new forensic and attack

reaction techniques. The effect of attacks on society and the behavioural aspects attached to it, such as how people will react, also call for a better understanding of the implications of threat materialization.

Advances are also needed in empirical 'field' studies, for example to understand how attackers operate, as well as new training approaches. As social engineering and phishing attacks will probably remain a central attack vector for decades to come, specific multidisciplinary research in this area is required to counter their effects.

Finally, the physical aspects of cybersecurity are of central importance, as the boundaries between the security and safety domains are becoming more and more blurry. Maintaining the security of hardware deployed in hostile environments, as well as designing and monitoring secure spaces are central, yet widely unexplored, areas of research.

### Example Topics

- Automated defence (e.g. automating software-defined networking and attack reaction)
- Intrusion detection and prevention, anomaly detection, threat intelligence in defence, and indicators of compromise
- Technologies for attack containment and deception (e.g. to thwart attacks)
- Hardware defences, and safe and secure deployment of physical devices
- Enabling technologies for information sharing and joint threat evaluation
- Asset management and supply chain security (e.g. software libraries)
- Cost and benefit analysis of defensive technologies and processes
- Monitoring and improving situational awareness and context-aware event correlation (e.g. using AI, machine learning or visualization)
- Human aspects of threat generation and risk, including awareness and training
- Security controls (e.g. access control and patch management)
- (Dynamic) Risk management
- Security operations and incident response (organization and processes)

# Attacks



# Summary

For effective security, the offensive side is as important as the defensive one, for two reasons. On the one hand, we cannot defend ourselves unless we understand what we are up against and what our weaknesses are. This includes awareness of designs, protocols, systems, crypto solutions, and existing defences. Similarly, we need attacks to test designs and defensive measures, such as in the case of penetration testing. On the other hand, we also need offensive techniques to disrupt criminal activities and take down malicious infrastructures.

## Links with other pillars

Attacks is closely linked with

- **Design:** With a growing understanding of attack techniques and attackers' modus operandi, we also increase our knowledge of the true nature of the systems themselves. This allows us to develop better systems that do not exhibit the same weaknesses.
- **Defence:** As we learn more about the attacks, we increase our ability to develop defence mechanisms to detect and response to such attacks. Research in automated vulnerability discovery and exploitation on the attack side should be closely linked to research in automated patch generation on the defence side. These research topics are strongly related.
- **Governance and Privacy:** The ability of agencies to employ offensive measures is subject to legal and ethical boundaries, while disclosure of vulnerabilities and exploits, or a lack thereof, drives both legitimate and underground markets. Likewise, novel attacks on privacy measures impact the confidentiality of information.

## Motivation

Where classical texts on security position security at the intersection of confidentiality, integrity, and availability, which are all positive properties, experience has shown that deep knowledge of attack techniques is essential to guarantee any of them. Phrased differently, if we do not know the enemy's potential weapons, strategies or motivation, we cannot defend ourselves against them.

Research is needed on vulnerabilities, new attack vectors, modus operandi, and automated vulnerability discovery and exploitation. Similarly, we need active probing of designs and cryptographic systems – asking ourselves if they are as secure as we think or want them to be. Importantly, this would allow us to stay 'a step ahead' of the cyber attacker by playing an active role in their same game, as opposed to 'running after' (often too late) whatever

the attacker has decided to do. While some of the attack techniques are technical, others involve a mixture of technology and criminal human activity, such as social engineering. At the same time, a deeper understanding of the attack selection, production, delivery process, and effect would allow us to make realistic forecasts of the materialization of an attack. This is not possible without more research on the offensive aspects of security both from a technical and a social sciences perspective. For instance, on the technical side one of the large research topics in advanced countries such as the US is the development of fully automated exploitation technology. From a strategic point of view, the Netherlands cannot afford to not develop knowledge about such technology. As an example of equally relevant research on the human side, consider studies of the development of advanced digital attack capabilities among extremists, terrorists and state actors.

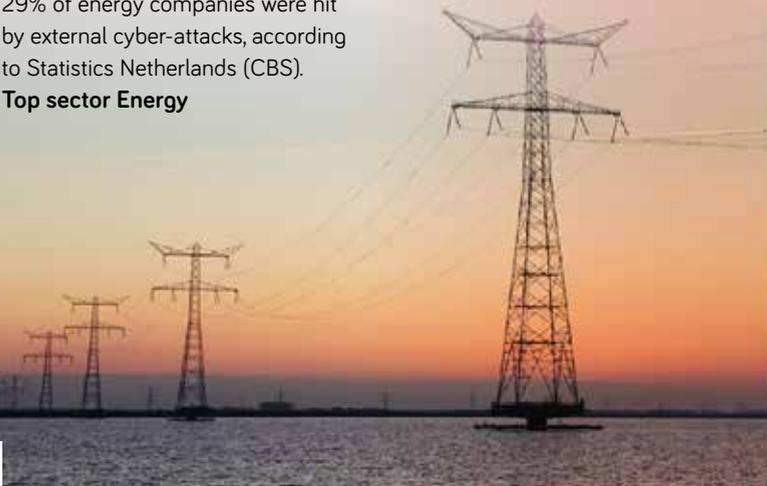
In addition, this pillar covers technical and non-technical attacks on malicious activities and infrastructures such as botnets and online crime markets. Non-technical aspects comprise all manner of disruption, by law enforcement authorities or by parties in the private sector, such as financial service providers or platform owners such as Microsoft, Apple, and Google. Interesting non-technical questions arise with respect to the roles of such parties. What role do 'super controllers' like Google, and Facebook have in the fight against cybercrime? Does the current legal framework for ISPs provide sufficient safeguards for super controllers and is there enough space for cooperation with law enforcement agencies in the fight against cybercrime? Clearly, public-private partnerships can be effective, but may also raise questions. Private parties proactively sharing large data sets with law enforcement agencies to detect cybercrime obviously raises questions about privacy. A clear and effective legal framework is important.

Most subfields of criminology, victimization studies, and aggressor studies that relate to ICT security also fall under this theme. Additional areas in the technical/ICT domain include post exploitation such as lateral movement

## Favorite target for hackers

The Dutch energy industry is the favorite target for hackers. In 2016, 29% of energy companies were hit by external cyber-attacks, according to Statistics Netherlands (CBS).

### Top sector Energy



and exfiltration, malware production, analysis and reverse engineering, as well as methodologies to take down botnets and other malicious infrastructures.

In addition, we envision that much of the research under this pillar will be neither exclusively technical, nor exclusively non-technical, but multi-disciplinary and/or inter-disciplinary in nature. For example, attack attribution or law enforcement operations against cyber criminals involve multiple disciplines.

## Research Challenges

A fundamental problem in security may be that we do not understand our hardware-software-people systems well enough. We do not know what vulnerabilities may arise and could be exploited by attackers. Attack techniques considered unrealistic or even science fiction only a few years ago, and thus ignored, are now practical attack vectors. Good examples of attacks rapidly evolving from sci-fi to real life can be found on the growing list of attacks on hardware. These can be seen from hardware glitches such as 'Rowhammer' to side channels such as the Meltdown and Spectre vulnerabilities that caused much commotion in early 2018. There is no doubt that more such vulnerabilities will surface in the next few years. Trends such as smart *everything* and the IoT will bring new exploitation opportunities of which we have never even heard.

But even in less sci-fi areas, we need a deeper understanding of the systems that involve hardware, software, and people in complicated eco systems with intractable interdependencies. Today, it is increasingly hard to understand where the weaknesses are, or, once found, what the consequences of a vulnerability may be. We need research to help us understand these eco systems.

Another major challenge is change. From a high-level perspective, the objectives of criminals do not really change. Using weaknesses in computer systems or humans, they want to steal money or information, manipulate people, and compromise systems. Even so, changes present problems. Every change in the modus operandi of criminal activities presents new challenges. Whenever criminals develop new means to make money from criminal activities, by mining cryptocurrency for instance, by organizing themselves, or by selecting new classes of victims, the security community must adapt. Whenever policies change with respect to vulnerability disclosure, or the herding of exploits, perhaps by law enforcement or intelligence agencies, the security community must adapt. We need to

become better in automatically finding new types of attacks or forecasting the attackers' next move.

One of the most pressing issues in research into the human factor in cybercrime and cybersecurity is the lack of longitudinal studies. The majority of studies that have been executed are based on cross-sectional data, meaning comparisons are done at a single point in time. Longitudinal studies make comparisons over time and provide insight into cause-and-effect relationships. Additional research challenges on human factors, like offenders, victims and tackling cybercrime, can be found in the research agenda: The Human Factor in Cybercrime and Cybersecurity.

Another open research question is how to counter-attack criminal infrastructures, or the desirability of doing so. Botnets have evolved at a rapid pace and are now so sophisticated that we may lack the technical means to take them down within the boundaries of the law. Similarly, the effectiveness of takedown actions on underground markets and organizations is limited by the resilience and fluidity of the cybercriminal community as a whole. We need research to study incentives and effectiveness of measures. The analysis of malicious software is extremely challenging, considering that the number of malware samples keeps growing. Reverse engineering in itself is extremely tedious, let alone attributing malicious code to developers, determining the lineage of malicious code, or classifying such programs according to the risk they pose.

### Example Topics

- Extending the attack surface and finding new attack vectors, e.g.:
  - Side channels, hardware attacks, software attacks, social engineering, cryptanalysis, etc.
  - Attacks on new ICT (e.g. AI and machine learning, big data, SDN/NFV)
  - Challenging common assumptions
- Human factors related to cyber-attacks (e.g. attacker studies, social engineering, profiling, and victimization)
- Automated vulnerability detection and exploit generation
- Trends in modus operandi of attackers
- Predictive analysis to identify malicious activity trends and attackers' next steps
- Attacks on and security evaluation of cryptographic systems
- Reverse engineering and malware analysis
- Techniques, tactics, procedures and conditions for offensive cyber operations, including disruption of malicious activities or infrastructures

## Increased political and economic espionage

In 2017 more and more countries used digital means to carry out political espionage in attempts to uncover or covertly influence Dutch decision-making. Cyberattacks are accessible, cheap and difficult to trace to the actual perpetrator, and their impact can be quite extensive. With regard to economic espionage, the AIVD notes an increase in the number of attacks on companies and organizations in Europe. In addition to targeted attacks, states have also engaged in untargeted attacks to hit and damage as many organizations as possible.

**Annual Report AIVD: 'Classic' threats become increasingly digital**





# Governance



# Summary

At its very core, cybersecurity is determined by the decisions of those who guard the systems and services on which we depend. If they do not adopt the available security solutions, then nothing changes. In other words, security depends on the incentives of companies, citizens and governments. These actors might or might not adopt more secure designs or stronger defence measures, they might choose to mitigate attacks or ignore them, or they might enhance privacy or undermine it. Such decisions are made in the context of different socio-economic, legal and normative environments. Governance is about assigning responsibility to the agents who are in the best position to act and shaping the objectives and means for these agents to act. Many of these environments are markets, as nearly all systems and services are in private hands. These markets suffer from a variety of failures that cause them to underinvest in security and externalize the damage of incidents to third parties and society as a whole. This brings into focus the repertoire of institutional solutions to combat market failures, including but not limited to regulation, self-regulation, information sharing, property rights, transparency, liability, and social norms. Beyond correcting market failure, governance is shaped by wider political value systems and the institutional structures. In the area of international relations, formation of formal and informal norms and rules across different cultures provide emerging forms of governance.

## Links with other pillars

Governance is closely linked with

- **Design:** There is a strong link with Design, as many existing more secure designs for hardware, software, internet architecture, and protocols are not adopted because of misaligned incentives. Design without better governance is dead in the water and vice versa. Better design can realize values and outcomes sought by governance.
- **Defence:** Along similar lines, governance is linked to Defence. As security always comes at a cost, it is rational for actors to tolerate some level of security failure. That being said, when those who guard systems and services do not suffer the consequences of such failures, they tend to underinvest in better defence.
- **Attacks:** There are several links with Attacks, most notably the governance of crime prevention and mitigation, but also the governance mechanisms that govern the development and use of offensive technologies (e.g. the Wassenaar Arrangement).
- **Privacy:** Many of the Privacy threats are less about technology and more about the economic incentives and business models around personal data. This is a key link to governance, though the governance of privacy might be incorporated within that pillar for the sake of clarity.

## Motivation

In past decades, many technical advances in secure design and better defence have been developed and ignored. We tend to devote a lot of attention to the most advanced attacks. They are clever and often lead to countermeasures that are very difficult to implement. The spectacular new attacks might distort our view of security. In reality, the overwhelming majority of attacks are not new. We have the technology to prevent them or defend against them. Think of phishing attacks, which are hardly new and used by all attackers, from 419 scammers to nation states.

So why are these types of attacks still happening? Because they are successful. That changes the question to: why are straightforward phishing attacks still so devastatingly effective? In answering this question, we often end up blaming the user. It is often heard that “they clicked on the wrong link”. Though users are trained to be less susceptible to these tactics, we tend to ignore that for this end-user failure to be so consequential, many other actors have already failed to adopt sufficient secure designs or defensive measures. These failures include the mail server operators that have not adopted sender authentication so mail domains can be easily spoofed, the hosting operators that did not detect or takedown the phishing sites on their network, the software vendors that allowed vulnerabilities in their products that the phishing payload could exploit, the ICT administrator of the user that did not apply the security patch to the user machine, and several others.

Cybersecurity is highly interdependent. All these actors make their own security decisions, based on their own incentives, but these decisions affect others in the network as well. When the owner or guardian of the system or service that is being abused, does not bear the full cost of security failure, they tend to underinvest in security. This means the damage of incidents is externalized to other actors. In other words, information asymmetry, externalities, monopolies and other issues lead to misaligned incentives which, in turn,

## Medical instrumentation and information security/privacy

Healthcare institutions have large numbers and diverse sets of medical equipment, with more and more connections to internal and external networks and databases, in which confidential and safety-critical information is processed. The lifetime of this medical equipment is relatively long, which carries the risk of outdated software and technology.

**LUMC and HMC**



cause market failures. Research is needed to develop better governance mechanisms to combat market failures. Beyond markets, innovations are needed in international institutions for governance. Examples of this include possible treaties on the proliferation and use of offensive capabilities and mechanisms for robust and independent attribution of attacks.

## Research Challenges

Governance, market failures and decision-making have been studied widely in many areas of society, but we do not know how these lessons translate to cybersecurity. Furthermore, novel technologies also offer new mechanisms to improve governance by combining technical advances in measurement ('big data') with law and economics.

One core area of innovation is around transparency. Many security-related data can be collected cheaply and at scale. Think of large-scale measurement techniques to detect vulnerabilities and security failures across markets. This can be leveraged to develop security metrics and benchmarks. By greater transparency around the security performance of market players, we can reduce information asymmetry and strengthen their security incentives. Such metrics also lay a basis for other forms of governance, such as self-regulation, insurance markets and public oversight. At a higher level, we need better statistics on different types of cybercrime, incidents, and victimization. More reliable quantification is a condition for effective policies and governance.

A second area where innovation is needed is that we currently know little about the effectiveness of security measures. Governance needs to be based on an understanding of which controls (at the level of users, firms, sectors) actually help to increase security or the perception of security. How do human factors shape security outcomes and how can they be improved? This requires research into the causal link between security measures on the one hand and vulnerability and incident rates across firms and

sectors on the other. Understanding this requires research into human and organizational behaviour around security.

A third area would be to study the design and empirical effects of known governance mechanisms in the new environment of cybersecurity. This could be seen in thinking of how to translate underlying normative values into regulatory frameworks for firms and platforms, the effects of mandatory standards, private law mechanisms, certification, responsible disclosure and vulnerability notification mechanisms, information sharing arrangements among private and public actors, multi-actor coordinated incident response, ethical hacking exercises, international institutions and norm formation, liability assignment, and insurance. International and cross-sectoral comparisons seem especially suited for this purpose. Specific sectors will have different needs in terms of the mechanisms that need to be in place. Critical infrastructures and health, for example, would probably need more binding norms, integrated with the safety regulation that is already well established in these sectors. Other sectors could operate more via self-regulation and liability. The government itself also faces specific challenges in ensuring secure practices across different agencies and levels, such as the local, regional, national, and international.

## Example Topics

- Legal mechanisms and normative frameworks
- Standards and certification
- Security metrics and benchmarks
- Intermediary Liability
- Insurance
- Effective information sharing
- Measuring economic impact
- Securing SMEs
- Empirical drivers of weak / strong security in the wild
- Regulating offensive technologies



# Privacy

# Summary

Privacy is a fundamental right in the European Union. Proper understanding of the risks to privacy, its conceptualization, and the necessary design of privacy protection is essential to protect privacy related interests of individuals. This includes the more normative and ethical aspects, and also includes the related area of identity. In particular data protection aims at preventing and mitigating risks that arise from authorised and unauthorised access to data, where accessing, processing, storing, and disseminating data may lead to harm, discrimination, exploitation, manipulation or erosion of self-determination of human beings. As businesses and governments exceedingly use personal data for their day to day operations, it is crucial to respect privacy in a broad sense and protect individuals from possible misuses and abuses of personal data.

## Links with other pillars

Privacy is closely linked with

- **Design:** as the whole concept of privacy-by-design closely resembles security-by-design, albeit with a broader scope and using the risks of the user, known as the data subject, instead of the risk to the organization, known as the data controller, as point of departure.
- **Governance:** as the economic aspects and market failures studied within that pillar may help to understand the economic, regulatory, political and normative aspects of proper privacy protection, and vice versa. The same goes for the study of regulatory approaches to address possible market failures.
- **Attacks and Defence:** There are also links with the Attacks and Defence pillars, because threats to privacy, and their mitigation, may inform the research studied within those pillars, and the other way around.

## Motivation

The EU's General Data Protection Regulation (GDPR), which came into force in May 2018, mandates a number of principles, such as data minimisation, data protection by design and by default, the right to access, the right to erasure, and the right to object automated decisions. Implementing these obligations is a serious challenge. Addressing these issues to protect privacy in the age of 'surveillance capitalism' requires multidisciplinary research combining the technical, social, ethical, legal, and policy perspectives. Privacy is of crucial importance in democratic societies, yet it is often neglected. This is because, in addition to the technical and incentive challenges regarding security in general, there is a hard trade-off at play. Collecting large troves of data has economic value and improves the functionality of many Internet services and national security policies, while privacy risks and damages are uncertain and distant. However, mega-breaches, voter manipulation, commercial exploitation on the basis of consumer profiles, changing power relationships show that the damages are very real. Governments increasingly rely on the collection of large data sets

about their citizens in order to increase efficiency, combat fraud or improve homeland security. The resulting surveillance infrastructure is easily abused for nefarious purposes. Privacy is fundamental to build trust in the digital economy and digital society at large and although data protection is often seen as an impediment to innovation, it can also lead to responsible digital innovations and new economic opportunities.

Technological developments like the Internet of Things (IoT), edge / fog computing, peer-to-peer approaches, as well as a fast-moving ICT infrastructure create both opportunities for and threats against our privacy.

## Research Challenges

Privacy is a multidisciplinary research field that requires combining technical sciences, such as computer science and data science, as well as social sciences and humanities, such as communications, economics, ethics, and law. Privacy is influenced by theories on identity construction and technological methods for identity management, that should similarly be studied from this multidisciplinary perspective.

At a fundamental technological level, there is a need to further develop privacy enhancing technologies (PET), and to study the application of new cryptographic primitives, such as Multi-party Computation, Fully/Somewhat/Additive Homomorphic Schemes for this purpose. This also includes privacy friendly methods for identity management. Many privacy enhancing technologies rely on certain properties regarding the

## Balance between information freedom and privacy

Can we find a balance between information freedom and privacy with big data challenges like the encryption of data and the anonymization and sharing of user data? Likewise the GDPR is perceived a security issue.

**NWA route: Value creation through responsible access to and use of big data**



## Safe and secure data sharing

How can I share my data with someone else, in such a way that my data is only used for specific purposes? How can you do that along supply-chains or along series of institutions (like various departments in hospitals or across hospitals)?

### Commit2Data



underlying infrastructure on which they run. This, therefore, warrants the study of privacy friendly infrastructures, like those that provide anonymous communication.

Privacy engineering is an emergent field of research. Designing and implementing privacy friendly systems, based on privacy by design (PbD), deserves further multidisciplinary study. This field should have a stronger focus on usability and should also study the relationship with, and possible alignment with, security by design. Approaches and methodologies that work in practice need to be developed, especially those that can be applied within modern development practices like agile, and that provide guidance for the development of mobile applications that increasingly rely on third party libraries and services. Also the link between organizational practices and privacy should be taken into account. In addition to this, benchmarking methodologies need to be developed to allow organizations to assess their 'privacy maturity'. The engineering toolbox needs to be extended to also cover 'softer' aspects of data protection like transparency, contextual integrity, and how to obtain proper consent.

From a different perspective, the threat to our privacy and measures to detect and quantify abuses and misuses, such as price discrimination, voter manipulation, filter bubbles, racism, and sexism, need to be further investigated. This includes longitudinal user studies into subjects such as user perceptions of privacy, as well as studies into different conceptualizations of privacy in response to technological and societal changes. Similarly, existing mechanisms to govern data protection, for

instance regulation, need to be evaluated and better data governance mechanisms need to be developed. Methods to incentivize privacy and alternative business models that do not rely on exploiting the value of personal data deserve further study.

Finally, pressing questions in data ethics, such as design for accountability, explainability, contestability, transparency, and non-discrimination need to be addressed, especially now that AI and machine learning approaches are becoming mainstream. An ethical comparison of different PbD and PET approaches is desirable.

### Example Topics

- Privacy enhancing technologies
- Privacy by design, privacy design patterns and value sensitive design
- Privacy friendly infrastructures
- Privacy engineering
- Privacy friendly identity management
- Tools and methodologies
- Measuring / quantifying privacy protection
- Data governance and protecting personal data once it is collected
- Algorithmic accountability and transparency
- Privacy economics
- The interplay between legal and technological developments
- Privacy perception of end users

### Data-privacy and data-integrity

Systems must ensure active and passive data-privacy and data-integrity. Architecting for data-privacy and security. This requires novel means to fulfil system operation in distributed configurations with minimal sharing and storing of information.

#### Top sector HTSM - Embedded Systems

# Context & Societal Ambitions



## Introduction

This section explains how the National Cyber Security Research Agenda NCSRA III fits into the Dutch knowledge and innovation policy landscape. It will also be made clear how the NCSRA III contributes to the realization of ambitions formulated in the National Cyber Security Agenda NCSA and is supportive to a variety of top sector roadmaps and related research agendas.

The NCSRA III is an agenda, not a program, and is positioned as a frame of reference for (thematic) cybersecurity R&D programs, such as the SBIR public tenders and the NWO research programs. The NCSRA III specifies the challenges in research and innovation as outlined by the government in the NCSA and the Dutch Digitization Strategy. We intend it to be a forward looking and guiding document. Organizations who fund research may set conditions. New funding program types and mechanisms may follow, like programs based on the NWA, multidisciplinary cross-over initiatives and / or top sector-based programs such as those agreed in Knowledge and Innovation Contracts (KIC's).

*The NCSRA III is an agenda, not a program, and is positioned as a frame of reference for (thematic) cybersecurity R&D programs*

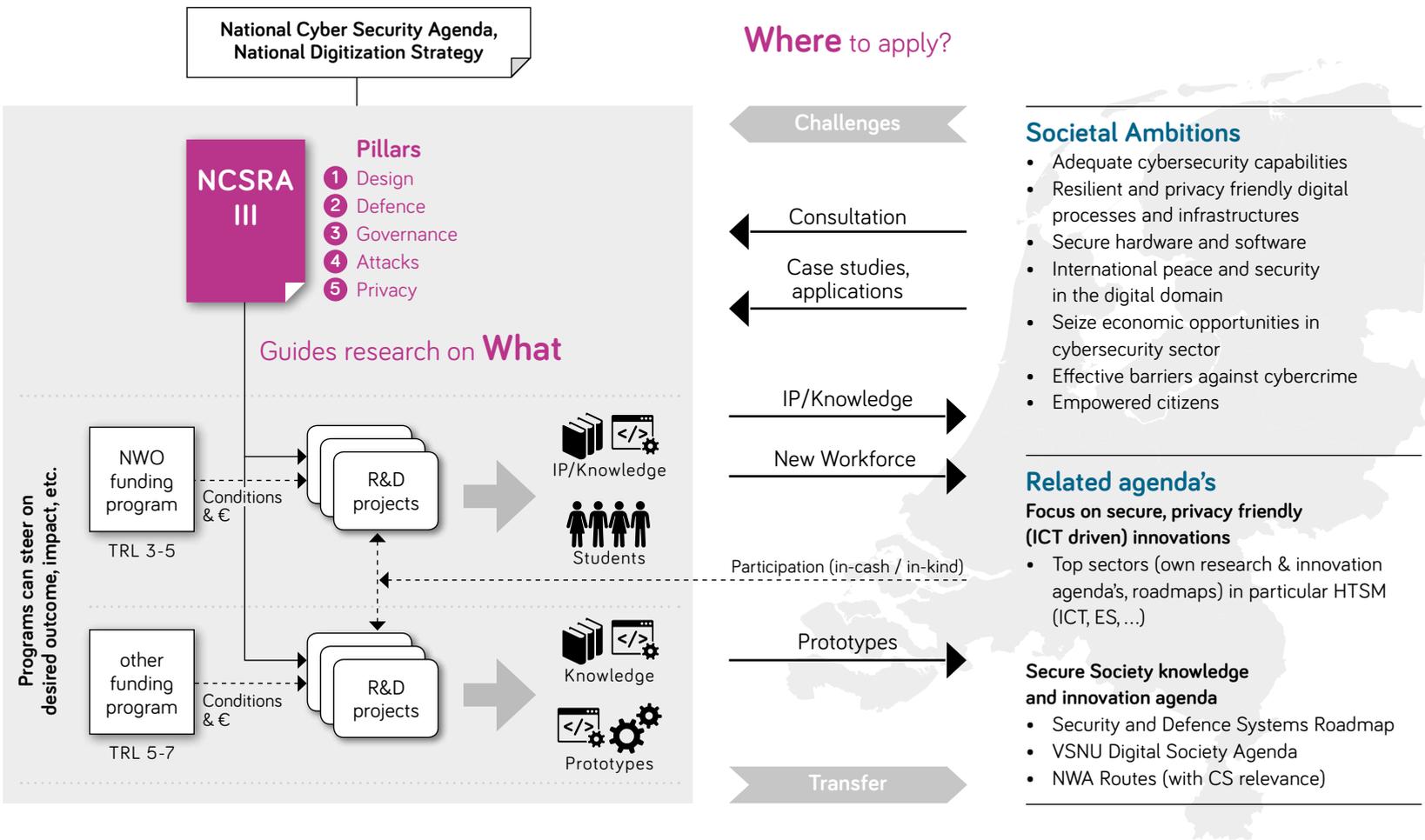
## NCSRA III in context

The NCSRA is a product of bottom-up agenda setting, supported by broad field consultations, and coordinated by dcypher. Users of the agenda are those who coordinate and / or fund R&D in cybersecurity, like NWO, ministries, and knowledge institutes such as universities, TNO, NFI and CWI. Public and private enterprises with R&D departments or participating in publicly funded R&D projects are also considered as users of this document. Research programming, project selection and execution are logical steps following the publication of the NCSRA.

The figure below depicts how the NCSRA III is positioned in the Dutch knowledge and innovation policy landscape. Bi-directional traffic, exchanges, between the left and right side of the picture is / are essential in the public-private collaboration. Transitioning knowledge into practice should not be a 'valley of death'. The cybersecurity research community should feel challenged by ambitions set in broad society, symbolized by the arrow to the left. An important deliverable by the grey box on the left are well educated cybersecurity experts. In addition to this, the Netherlands should benefit from the outcome of research projects itself, symbolized by the arrow to the right.

The cybersecurity community has expressed a growing need for more centralized and active coordination between agenda setting, research programming and distributed higher education, as well as more coordination in the bidirectional traffic between the left and right side of the picture below, preferably by a single entity encompassing the left hand grey box.

# NCSRA III in the Dutch knowledge and innovation policy landscape



## Societal Ambitions

The NCSRA III contributes to the realization of societal cybersecurity ambitions as listed at the right-hand side of the picture. Many of these are inspired by ambitions formulated in the NCSA. For each ambition, a brief explanation follows how execution of the NCSRA III may contribute to its realization.

- **Adequate cybersecurity capabilities**

Nowadays public and private organizations are continuously confronted with all kinds of cyber threats. Moreover, the threat landscape is rapidly changing and attacks are increasingly more advanced and automated. In order to counter these threats, government bodies and organizations need to establish adequate cybersecurity capabilities, such as through SOCs and CSIRTs. There is a clear need for collaboration and sharing of information between government bodies and private organizations, and between organizations, to create a common awareness and readiness to address the cyber threats now and in the future.

As these cyber threats may cause serious problems for the national safety and security, the Dutch security organizations must have the capabilities to fulfil their national security task in the digital and physical domain. Developing and maintaining these cybersecurity capabilities to detect, mitigate and respond decisively to cyber threats requires technological, legal, and societal innovations. Research and developments driven by the NCSRA III should strongly support the establishment and continuous evolution of these cybersecurity capabilities.

- **Resilient and privacy friendly digital processes and infrastructures**

Services are increasingly provided by highly interconnected systems, creating a sort of 'system-of-systems', from a variety of organizations. The interdependency between systems and organizations to provide digital

services has increased drastically, and not without risk. Particularly when considering the chains in critical services. The risk is not only related to continuous and reliable digital processes, but also related to ensuring personal data protection. To ensure that all these risks to our digital processes are correctly managed, all involved organizations have to step up and strengthen the resiliency and personal data protection of the services they provide. This is especially the case for providers of cloud and data communication infrastructures. Government bodies like the Dutch NCSC and the Digital Trust Centre (DTC), play an important role in assisting organisations with the continuous challenge of making the digital processes and infrastructures more resilient.

As new ICT systems and network technologies are continuously being introduced, such as IoT and big data, there is a clear demand for knowledge and expertise resulting from R&D projects. The NCSRA III driven R&D projects should play an essential role in the realisation of this NCSA ambition.

- **Secure hardware and software**

The need for secure hardware and software has become more important as well. This is specifically addressed in the 'Roadmap Veilige Hard- en Software' from the Dutch Ministry of Economic Affairs and Climate Policy. The roadmap contains a set of measures that should lead to significant security improvements of hardware and software. Measures include among other, the best practices, standardization, certification, responsible disclosure and liability aspects for digital security of products. Digital secure products represent a growing export market for the Netherlands. Companies active in this market play an important role in helping the Dutch industry becoming more cyber resilient.

Quality research driven by NCSRA III should support the realization of the ambitions described in this roadmap, and lead to new cybersecurity products and services, thereby supporting existing vendors and service providers in becoming more competitive.

- **International peace and security in the digital domain**

In the Annual Report for 2017 the AIVD writes that traditional threats to national security, such as espionage, covert political influencing, terrorism and sabotage, are moving more and more to the digital realm. In addition, several countries have been actively developing a military offensive cyber capability. Given these developments, it is necessary to develop a capability to respond to cyber threats by state actors in a timely and adequate manner, and have an offensive cyber capability of its own to deter such acts. Furthermore, it is of great importance to promote international law in the digital domain, including protection of human rights and in support of the fight against cybercrime, and to strengthen international cooperation in cyber capacity building.

NCSRA III driven research should contribute to developing capabilities and international law for international peace and security in the digital domain.

- **Seize economic opportunities in cybersecurity sector**

Cybersecurity and privacy protection are by itself also sectors that provide economic and societal opportunities. As there is increasing demand for cybersecurity services and products, opportunities arise for innovative solutions by Dutch companies and start-ups. A strong Dutch cybersecurity sector creates jobs, contributes to the Dutch autonomy, and international position of the Netherlands. A number of Dutch cybersecurity service providers and vendors already acts on an international level. NCSRA III driven research should support these companies to seize these economic opportunities and increasing their international competitiveness. Companies in the cybersecurity sector should grasp the opportunity to work together with knowledge institutions in R&D projects and as such contribute to the execution of the NCSRA III.

- **Effective barriers against cybercrime**

Cybercrime has become a serious problem. In 2017, one out of nine persons in the Netherlands was a victim of cybercrime. In the NCSA the ambition is formulated to create successful barriers against cybercrime. This includes the prevention and combating cybercrime, and limiting the number of victims, perpetration and recidivism rates. Digital investigation and forensics are important capabilities in the fight against cybercrime. These capabilities require continuous development and innovation. Note that also classical crime in which the internet is used, such as selling illegal drugs on the dark web, requires investigation in the digital domain.

The Dutch Computer Crime Act III provides law enforcement authorities with more power to fight cybercrime. This includes the authority to hack computers. In order to apply these new powers, without jeopardising the safety and privacy of citizens, research is needed in many different fields, including technical, legal, and sociological.

Combating cybercrime is a domain in need of continuous innovations and new knowledge. Research driven by the NCSRA III should enable law enforcement agencies and related organizations the establishment of effective barriers against cybercrime.

- **Empowered citizens**

Citizens are more and more confronted with identity theft, ransomware, and breaches of their personal data. It has become clear that citizens need to become more capable in protecting themselves against these cyber threats. Moreover, citizens will be increasingly made aware of their own responsibility and secure behaviour. NCSRA III driven research should contribute to empowering citizens to fend off cybercrime, take control of their personal data, and deal with personal data breaches and other incidents in the digital domain, such as seeking help from the appropriate organizations.

## Related research agenda's

For many top sector related roadmaps, research and innovation agenda's cybersecurity is a condition sine qua non. They constitute another dimension in the research policy landscape. Agenda's and roadmaps consulted during preparation of this agenda are listed as references at the end of this booklet.

### Secure, privacy friendly innovations

All nine top sectors of the Dutch economy have their own research & innovation agendas or roadmaps. Many innovations that are worked on within each of these top sectors depend heavily on the application of, sometimes new, ICT systems. As a consequence, these top sectors are susceptible to cybersecurity challenges such as protection of intellectual property, personal data, and business continuity, and require digital security to fulfil their role as foundation of the Dutch economy. As many innovations in these top sectors are highly dependent on ICT as the key enabling technology, the dependency on ICT and the need for strong cybersecurity will only increase. For that reason, the NCSRA III is closely connected to the ICT Roadmap 2018 - 2021, under the HTSM top sector, in which cybersecurity is mentioned as an essential capacity for businesses,

### Interdisciplinary challenge

One of the biggest challenges is to make the required alpha-gamma-beta connection to research how to improve the (inter)national prosecution and enforcement of cybercrime, gain insight into attack strategies and business models of cyber criminals, and to make end users more resilient to cyber-attacks.

**NWA route "Between conflict and cooperation"**



government agencies and other organizations to thrive. Research and development into new cybersecurity and privacy technology could lead to new business opportunities.

### Secure Society Knowledge and Innovation Agenda

A 'Secure Society' is one of the eight societal challenges as formulated by the Ministry of Economic Affairs and Climate Policy. Knowledge and Innovation agendas were written for each challenge. Digital security is one of the strategic aims of the secure society agenda, next to physical and operational security.

### Digital Society Research Agenda

The Digital Society Research Agenda by VSNU contains a program line closely connected to this agenda: Safety and Security.

### NWA research routes

NWA research routes with cybersecurity relevance are:

- Value creation through responsible access to and use of big data
- Smart, liveable cities
- Energy transition
- Between conflict and cooperation
- Quantum / Nano-revolution
- Resilient societies

# Acknowledgements

The NCSRA III Board of Editors would like to thank all who contributed to the realization of this research agenda. Contributions were delivered in many ways:

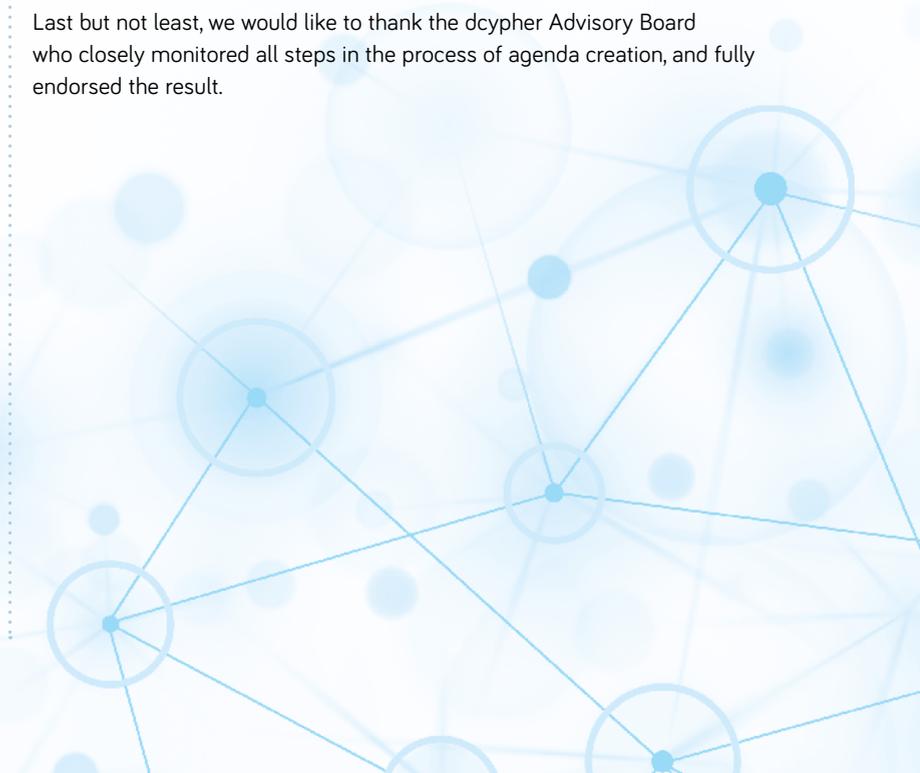
Text contributions and / or extensive comments were delivered by Wolter Pieters (TUD), Hadi Asghari (TUD), Cristiano Giuffrida (VU), André Hoogstrate (Min. of Defence), Luca Allodi (TU/e), Jeroen van den Hoven (TUD), Zeki Erkin (TUD), Rutger Leukveldt (NSCR), Nico van Eijk (UvA), Bibi van den Berg (UL), Aiko Pras (UT) and Joeri de Ruiter (RUN).

The Cybersecurity Special Interest Group (SIG-CS), associated with the ICT research Platform the Netherlands (IPN), reviewed the text, in particular Marc Stevens (CWI), Cees de Laat (UvA) and Veelasha Moonsamy (UU), provided useful comments.

Conversations were held with representatives of many top sectors and NWA Routes about the cybersecurity challenges in their area where cybersecurity research could provide solutions. Conversations with Egbert-Jan Sol (Smart Industry), Jimmy Troost (HTSM - Security), Inald Lagendijk (NWA Route Verantwoorde Waardecreatie met Big Data), Boudewijn Haverkort (Commit2Data), Marleen Stikker (NWA Route Smart Liveable Cities) and John Post (Energy) were very insightful.

Special thanks also for those who attended the field consultation meeting in Utrecht. Inspiring discussions about the different pillars led to many text improvements and helped bridging research and application. Some discussions continued after the consultation meeting demonstrating a strong involvement of a broad community. Thanks to Nicolas Castellon (dcypher) for making a final editorial step to improve text uniformity through copy editing.

Last but not least, we would like to thank the dcypher Advisory Board who closely monitored all steps in the process of agenda creation, and fully endorsed the result.



# Abbreviations

<b>AI</b>	Artificial Intelligence	<b>KIC</b>	Knowledge and Innovation Contract
<b>AIVD</b>	General Intelligence and Security Service of the Netherlands	<b>NCSA</b>	National Cyber Security Agenda
<b>API</b>	Application Programming Interface	<b>NCSC</b>	National Cyber Security Centre
<b>CBS</b>	Statistics Netherlands	<b>NCSRA</b>	National Cyber Security Research Agenda
<b>CCTV</b>	closed-circuit television	<b>NFI</b>	Netherlands Forensic Institute
<b>CPB</b>	Netherlands Bureau for Economic Policy Analysis	<b>NFV</b>	Network Function Virtualization
<b>CSIRT</b>	Computer Security Incident Response Team	<b>NWA</b>	Dutch National Research Agenda
<b>CWI</b>	Dutch national research institute for mathematics and computer science	<b>NWO</b>	The Netherlands Organisation for Scientific Research
<b>DDoS</b>	Distributed Denial-of-Service	<b>PbD</b>	Privacy by Design
<b>DevOp</b>	a clipped compound of “development” and “operations”	<b>PET</b>	Privacy Enhancing Technologies
<b>DTC</b>	Digital Trust Centre	<b>PLC</b>	Programmable Logic Controller
<b>GDPR</b>	General Data Protection Regulation	<b>R&amp;D</b>	Research & Development
<b>HTSM</b>	High Tech Systems & Materials	<b>SBIR</b>	Small Business Innovation Research Instrument
<b>ICT</b>	Information Communication Technology	<b>sci-fi</b>	Science fiction
<b>IoT</b>	Internet of Things	<b>SDN</b>	Software-Defined Networking
<b>IPN</b>	ICT research Platform the Netherlands	<b>SME</b>	Small and medium-sized enterprise
<b>IPR</b>	Intellectual Property Rights	<b>SOC</b>	Security Operations Center
<b>ISP</b>	Internet Service Provider	<b>TNO</b>	Dutch Organisation for Applied Scientific Research
		<b>VSNU</b>	Dutch Association of Universities

# References

- NCSRA II, IIP-VV, 2013
- Societal Challenge #7: The Secure Society, EZK, 2017
- Roadmap Digitaal Veilige Hard- en Software, EZK, April 2018
- Nederlandse Digitaliseringsstrategie/Digitale Agenda, EZK, 2018 (to be published)
- ICT Roadmap (Knowledge & Innovation Agenda ICT 2018 - 2021), 2017
- Roadmap ICT for the top sectors, 2012
- CSBN 2017 (Cyber Security Beeld Nederland), NCSC-J&V
- CSBN 2018 (Cyber Security Beeld Nederland), NCSC-J&V (to be published)
- NCSA: Nederlandse Cyber Security Agenda, Nederland digitaal veilig, NCTV-J&V, april 2018
- Digital Society Research Agenda, VSNU, 2017
- Stroomvoorziening onder digitale spanning, Rli, 2018
- Security and Defence Systems R&D Roadmap, Top sector HTSM, 2018
- Handreiking cybersecurity voor Smart Energy, Top sector Energy, 2017
- Digitalisering in het energielandschap 'Data, the world's most valuable resource', Top sector Energy, 2017
- Smart Industry Roadmap, 2018
- HTSM Roadmap Automotive 2018-2025
- HTSM Roadmap Embedded Systems, 2018
- High Tech to Feed the World 2.0, AgriFood Tech Platform, 2017
- Kennis- en innovatieagenda 2018-2021, Top sector Agri & Food
- LSH-Knowledge and Innovation Agenda 2018-2021
- KIA (Knowledge and Innovation Agenda) Creative Industry, 2018
- Jaarverslag: 'klassieke' dreigingen steeds meer digitaal, AIVD, 2018
- De economische en maatschappelijke noodzaak van meer cybersecurity, Nederland digitaal droge voeten, Herna Verhagen
- What drives Cybercrime? Empirical Evidence from DDoS attacks, CPB Policy Analysis, April 2015
- Onderzoeksagenda voor Blockchain, Dutch Advisory Committee on Blockchain Research, May 2018
- ICT binnen de topsectoren, NWO-bijdrage 2018-2019, topsector ICT
- Naar een veilig verbonden digitale samenleving, CSR, December 2017
- Verantwoorde Waardecreatie met Big Data, VWData Program, 2018
- Leukfeldt, E.R. (ed.) Research Agenda: The Human Factor in Cybercrime and Cybersecurity, 2017

# Colophon

## Board of Editors

prof. dr. ir. Herbert Bos  
 prof. dr. Michel van Eeten  
 prof. dr. Sandro Etalle  
 ir. Frank Fransen  
 dr. Jaap Henk Hoepman  
 dr. ir. Erik Poll  
 drs. Jan Piet Barthel (coordination)

## Production

drs. Juul Brouwers

## Design

Haagsblauw

## Photography

Photo Dick Schoof: Sander Heezen  
 Gettyimages  
 Shutterstock

## Print

Zalsman

## Founders dcypher



Government of the Netherlands

This agenda is the result of a bottom up agenda setting process, organized and made possible by

# dcypher

5 June 2018

The greatest possible care was taken in the composition of this agenda. Acquisition of items from this agenda is permitted provided with full source information.



dcypher