The Hague Centre for Strategic Studies

NWO FUNDED CYBERSECURITY RESEARCH:

# A BIRD'S EYE VIEW OF THE CURRENT RESEARCH PORTFOLIO

*The Hague* Centre for Strategic Studies

SECURITY


NWO FUNDED CYBERSECURITY RESEARCH: A BIRD'S EYE VIEW OF THE CURRENT RESEARCH PORTFOLIO

*The Hague* Centre for Strategic Studies (HCSS)

ISBN/EAN: 978-94-92102-29-4

**Authors:** Erik Frinking, Maarten Gehem, Nicolas Castellon.

**Special thanks to:** Jan Piet Barthel (NWO) en Paul Sinning (HCSS) for providing us with project data and numerous (text) suggestions.



*The Hague* Centre for Strategic Studies

Lange Voorhout 16
2514 EE The Hague
The Netherlands

info@hcss.nl
HCSS.NL

The Hague Centre for Strategic Studies

HCSS helps governments, non-governmental organizations and the private sector to understand the fast-changing environment and seeks to anticipate the challenges of the future with practical policy solutions and advice.

This report is part of the HCSS theme SECURITY. Our other themes are RESOURCES and GLOBAL TRENDS.

SECURITY

HCSS identifies and analyzes the developments that shape our security environment. We show the intricate and dynamic relations between political, military, economic, social, environmental, and technological drivers that shape policy space. Our strengths are a unique methodological base, deep domain knowledge and an extensive international network of partners.

HCSS assists in formulating and evaluating policy options on the basis of an integrated approach to security challenges and security solutions.

# *NWO funded Cybersecurity Research:*

## *A bird's eye view of the current research portfolio*

***The Hague*** **Centre for Strategic Studies (HCSS)**

## Table of Contents

# 1 Introduction

Cyberspace is an increasingly broadening concept that has been defined in numerous ways by multiple scholars. It is a unique combination of physical (e.g., infrastructure) and virtual (e.g., information) properties.[1] One of its main elements is the Internet, a global interconnected network of networks, which has dramatically altered since its establishment as a research network more than forty years ago.[2] Changes have been apparent in the technology on which it is build, the type of activities it is supporting, and the type of actors that are making use of it.

There is considerable insecurity in cyberspace because of the low barriers to entry and the fact that offense is cheaper than defense. The recently concluded Global Conference on Cyberspace (GCCS) 2015 dealt with issues ranging from economic growth and social development, and Internet governance to cybersecurity, cybercrime, international peace and security, and freedom and privacy.[3] The prominence of this high-level conference, held in The Hague, also demonstrates the increasing attention that is paid to cyberspace and cybersecurity. The increased dependency on ICT in society increases the potential impact of vulnerabilities in ICT. In particular, the term cybersecurity has emerged in recent years, and security issues and incidents have increased significantly.[4]

Yet, cyberspace is a relatively new domain. Due to some of its characteristics (e.g., its permission-free environment that allows people and devices to join it without prior screening) the infrastructure, its services and the behavior induced by it are extremely complex to understand. Thus, the need for research in this domain to improve the understanding of technical, social, economic, and political issues remains clear.

This paper provides an overview and analysis of 23 research projects funded by the Netherlands Organisation for Scientific Research (NWO) over the past two years in its cybersecurity research program, guided by two editions of the Dutch National Cybersecurity Research Agenda (NCSRA I and NCSRA II). NWO's cybersecurity research program aims to strengthen the (scientific) cybersecurity knowledge base in the Netherlands. The importance of this research field is increasing and requires the continuous and intensifying generation of cybersecurity knowledge and the delivery of sufficient cybersecurity experts on a scientific level to the Dutch society. A multidisciplinary approach is important as cybersecurity threats often have multi-dimensional characteristics.

The analysis is intended to support NWO's assessment of its current cybersecurity research project portfolio, to assist in identifying whether gaps or mismatches exist in the portfolio, and to define ways to address these potential gaps in the articulation of possible follow-up calls for proposals. *The Hague* Centre for Strategic Studies (HCSS) conducted this analysis, requested by the NWO division of Physical Sciences and the division of Social Sciences. To put the analysis of these projects into context, we first examined some emerging trends in cybersecurity as well as described Dutch strategic cybersecurity priorities.

# 2 Trends and Developments in Cyberspace

The cyberspace domain is a rapidly changing environment. Expectations of developments beyond a time horizon of 5 years are hard to give as technological developments keep moving forward at a fast pace in a world that itself is showing rapid changes in political and economic interests.

There are various ways in which subdomains of cyberspace can be distinguished, with one of which considering cybersecurity next to cyber economy, human rights, and technology. However, these domains are constantly converging and diverging, which makes it difficult to assess cybersecurity without consideration of the other domains.

The following section 2.1 clearly demonstrates the relevance of cybersecurity research in many disciplines, other that computer science, i.e. shows the broad spectrum of challenges related to the maintenance of a high cybersecurity level.

## 2.1 Trends in cybersecurity

This section lists some of the most current and emerging trends in cybersecurity. These trends raise a number of issues that go well beyond the technical characteristics of Information and Communication Technologies (ICT) systems per se.

### *Increasing reliance and risks in all parts of society*

Information and communication technologies are pervasive in many aspects of the economy and society. Their contribution to economic growth and innovation is undeniable.

Thus, the need to safeguard the trust of the citizens and the trustworthiness of systems and to create confidence in further innovation is clear. Governments, companies, and individuals are increasingly using ICT in ever more complex ways, leading to increasing vulnerabilities and problems, increasing dependence on undisturbed performance of ICT systems.[5] This reliance on ICT has also syphoned through in the functioning of our critical infrastructures, such as hospital services, energy provision or water provision services. And because of increased interdependence, failures of ICT systems can lead to massive ripple effects, causing a crisis in one sector to lead to problems in another.[6]

The growing cyber dependence, evident among both public and private actors, is making ICT an ever more attractive target for actors of all types looking to exploit, disturb or destroy competitors and opponents as the potential impact of cyber attacks is becoming greater.

For example, when hackers broke into the Hong Kong stock exchange's website in August 2011, trading of almost 20 percent of all stocks was suspended. More and more, we are dealing with 'hyper-risks', where a small change in one system may have extreme repercussions in another. The impact of these increasing levels of interdependence has created a complex eco-system of responsibilities that involve risks that are often hard to understand.

### *Increasing importance of geopolitics and geo-economics in cyberspace*

Providing security is one of the classic functions of government. As security becomes an increasingly important issue, it could be argued that governments might increase their role in the protection of the Internet so their societies can continue to benefit from it, while at the

same time, they also want to protect their societies from what might come through the Internet.[7]

States have become more directly and actively involved in cyberspace, both as a perpetrator and a target. As a result, geopolitics and cybersecurity have converged in a number of ways.

First, countries increasingly see the importance of cyberspace as a distinctively new domain. Cyber capacity allows governments to project power in a world where direct military strikes are much more costly and dangerous. The usage of unmanned aerial vehicles in interstate conflict is one example, the downing of government services is another (as seemed to be the case in the Estonian and Georgian conflicts).

Second, in the geo-economic spheres, competition between state-sponsored enterprises and multinationals could be influenced. This is when these enterprises receive governmental cyber support, for instance through cyberespionage or intellectual property theft, as cases such as Operation Aurora or Ghostnet were expected to be about. A last example are the fallouts in state-to-state relations with the opening up of classified pieces of information, as the cases of Wiki-leaks and Edward Snowden demonstrate. For each of these, the verification of sources remains a major obstacle in solving potential conflicts as states deny their involvement in activities. Much effort is now being put in reliable confidence-building measures, which aim for more transparency and responsibility of state-led activities.

As a result, from Iran to the Netherlands, governments have started to develop offensive and defensive cyber capabilities. All nations that are developing cyber capabilities indicate to use them for defensive and intelligence purposes, but only a few admit to their offensive ambitions. In one way or another, states are increasingly facing, preparing and mounting cyber-attacks. Some of these attacks resemble acts of war, like the large-scale digital assaults that disabled Estonian computer networks in 2007, or the cyber-attacks on Syrian defense systems before Israeli F16s bombed a Syrian nuclear reactor.[8] In addition, state actors are increasingly using tools widely deployed by cyber criminals or are hiring these groups to achieve their own goals. As the application of these tools merge, the identification of where the threat comes from is even becoming less clear.

Governments, ministries of Defense in particular, have a strong mandate to protect their citizens against such threats and use cyber capabilities in their international security strategies. Interestingly, the corresponding policies and capabilities remain rudimentary at best. Understanding of what cyber weapons and operations are capable of remains limited, as does our understanding on when and how they can and should be used, as part of what strategy, and the conflict dynamics this might spur.

### *Expanding range of threats, in an expanding domain (Internet of Things)*

Rapid technological developments have led to new cyber threats and risks of ICT failure – from script kiddies planting viruses on individual computers and ISIS hacking US twitter accounts, to major economic costs resulting from the disruption of SCADA systems. The potential impact of cyber attacks and disruptions will only increase, due to rapid digitization and difficulty in detecting, lack of investigation and prosecution capacity, permanent gap in rules and regulations. However, the (sometimes latent) theft of intellectual property or credit card fraud through cyberspace remains the biggest threat in the area of cybersecurity. As a

matter of fact, the facilitation of these types of activities as a service is slowly developing into a business model by itself, the so-called Cybercrime-as-a-Service (CaaS).

The number of devices, beyond the traditional computer environment, that are connected to the Internet and exchange information with each other, is rapidly increasing and will easily outnumber the traditionally connected devices. Here, safety and security cultures are sometimes still at a very embryonic stage of development. With a rising number of devices connected to the Internet, new risks are emerging, for example because devices and their software are not maintained by suppliers for extended periods of time.

Also new innovations such as cloud computing, Internet of Things, voice and face recognition, cause new challenges for protocols, standards, codes, and the management of identifiers, such as names, numbers and sensors. For instance, it is increasingly argued that the TCP/IP series of protocols was not designed for its current purposes (let alone, future demands) and has a number of inherent weaknesses that produces serious security insufficiencies.

### *Collecting more and more data*

With increasing connectivity, possibilities of collecting large bodies of data for numerous purposes (e.g., surveillance, market analysis) are expanding as well. Data analytics techniques are nowadays used to analyze big data, and commercial organizations and governments are already using them widely. Obviously, privacy could be jeopardized by the technical ability to collect data.[9] Or as one scholar puts the issue: "Data is the pollution problem of the information age and protecting privacy is the environmental challenge."[10]

On the other hand, given the potential value and various uses of these data, the organizations responsible for collecting, maintaining and transporting data could also become targets of attacks, economically or politically inspired.

There is a trend identified regarding the adoption of big data analytics techniques for criminal purposes. The same analytics approach business, police, or intelligence services use, can be copied by a perpetrator. For instance the use of social networking analysis, to select the persons of interest in an organization who can be most efficiently targeted by spear-phishing. This approach will create all sorts of new opportunities for cyber criminals, such as the extraction of data of interest or ID information enhancement.

## 2.2 Approaches to cybersecurity

### *Developing an encompassing response*

Cyber-attacks and ICT failures provide potentially economic, security, social, and political risks. Consequently, efforts to respond to these risks have become multilayered. Where in the 1990s responding to cyber crises was considered a technical question first and foremost, more and more the operational, policy, and strategic levels of response are recognized. Most governments have developed cybersecurity strategies and policies. Cybersecurity has become a topic which has been receiving increasing media attention. Also, government officials have publicly and repetitively expressed the need to take cybersecurity to the "board room".

In the European Union, 25 member states have a National Cybersecurity Strategy (NCSS) (either completed or under preparation). The following figure provides an overview of cyber threats addressed in 18 strategies developed across the world:

| | CYBER THREATS TO: | | | | | | |
|---|---|---|---|---|---|---|---|
| COUNTRY | CRITICAL INFRASTRUCTURE | DEFENSE CAPABILITIES | ECONOMIC PROSPERITY | GLOBALIZATION | NATIONAL SECURITY | PUBLIC CONFIDENCE IN ICT | SOCIAL LIFE |
| AUS | ● | ● | ● | | ● | | ● |
| CAN | ● | ● | ● | | ● | | ● |
| CZE | ● | | ● | | ● | | ○ |
| DEU | ● | | ● | ● | ○ | | |
| ESP | ● | | ● | | ● | ○ | |
| EST | ● | | ● | | ○ | | ● |
| FRA | ● | ○ | ● | | ● | | |
| GBR | ● | | ● | | ● | ● | ● |
| IND | ● | | ● | ○ | | | |
| JPN | ○ | | ● | ● | ● | | ● |
| LTU | ● | | ○ | | ○ | ● | |
| LUX | ● | | ● | | | ○ | |
| NLD | ● | ○ | ● | | ○ | ● | ● |
| NZL | ● | | ● | | ● | ○ | |
| ROU | ● | ● | ○ | | ● | | |
| UGA | ● | | ● | | | ● | |
| USA | ○ | | ● | | ● | ● | |
| ZAF | ● | | ● | | ○ | ● | |
| Count | 18 | 5 | 18 | 3 | 15 | 9 | 7 |

NOTE: ● – EXPLICITLY DEFINED; ○ – IMPLICITLY REFERENCED

TABLE 2. CYBER THREATS IN NCSS
SOURCE: LUIIJF, E., K. BESSELING, AND P. DE GRAAF. "NINETEEN NATIONAL CYBER SECURITY STRATEGIES."
INTERNATIONAL JOURNAL OF CRITICAL INFRASTRUCTURES 9, NO. 1 (2013): 3-31

For all these cyber threats, response options are being developed. Parallel to approaches in other security areas, these options range from focusing on preventing cyber-attacks and failure, to mitigating attacks or post-attack stabilization (e.g., a National Detection Centre). The phases of conflict that these options target go from pre- to post conflict.

### *Governance of the Internet and governance on the Internet*

Security is increasingly appearing in governance discussions related to the Internet.

On the one hand, there is governance and security *of* the Internet. The fact that the Internet is currently supporting functions in society for which it was not designed is affecting the overall security. This is especially related to the earlier mentioned TCP/IP series of protocols, which has a number of weaknesses.[11] The development and implementation of alternatives requires additional effort and, by some, is considered very urgent. The multi-stakeholder mechanism of governance, which allows representatives from technical communities, users, NGOs, and the private sector to be involved in open fora for debate and decision-making, has been the dominant model since the emergence of the Internet. However, the transition of technological to political dominance of Internet activities is also starting to apply to the governance of the Internet and its supporting operations and services. So, questions about how to redesign parts of the Internet do attract increasing attention by government and economic actors as well. The result is that increasingly national governments are trying to assert their power and interests, stressing the perspective that they are the primary representatives of the needs and interests of populations and that the multi-stakeholder mechanism is not effective.

The governance *on* the Internet on the other hand is quite a separate dimension. While the multi-stakeholder mechanism is also in place here, the intergovernmental approach is, for instance, appearing at the UN level at the General Assembly level through the 15-member Group of Governmental Experts (GGE), which is trying to develop norms of Internet behavior by states, confidence building measures, ways to exchange information, and capacity building opportunities. Within the UN family, there are at least 15 to 20 additional bodies that deal with governance issues as well.

### *Legal tools*

As more and more human conduct appears online, questions often arise concerning whether and how to apply to the Internet the legal principles developed for the offline world. This has triggered considerable debate whether cyberspace and cybersecurity issues within require dedicated or adjusted bodies of law. This still applies to various issues such as privacy, intellectual property, liability (both for software as well as content), and so on, but also to the bodies of law such as International Law, Law of Armed Conflict, and International Humanitarian Law. Also, enforcement of legal articles, such as through take-down notices, surveillance, or declarations of protected zones are questioned in their efficacy.

### *Non-binding measures*

Although some scholars claim that most current legislation could be applied to the cyber domain as well, there is still no widespread consensus on legal definitions or on its enforcement. Confidence-building measures (CBMs) are an instrument of interstate relations aimed to strengthen international peace and security by reducing and eliminating the causes of mistrust, fear, misunderstanding, and miscalculations that states have about the military activities of other states. Various confidence building measures aimed at reducing the risk of conflicts are being discussed in regional fora, such as the Organization for Security and Co-operation in Europe (OSCE).

China, Russia, Tajikistan and Uzbekistan collaborated on a potential General Assembly resolution on an international code of conduct (CoC) for information security and called for international deliberations within the UN framework on such an international code, with the aim of achieving the earliest possible consensus on international norms and rules guiding the behavior of states in the information space. Proponents of the CoC argue that it is an open and sustained process of building international consensus, that the draft CoC is not an end product, but the beginning of the process. Adversaries claim this is a development toward providing more power to governments in cyberspace.

# 3 Dutch Strategic Cybersecurity Context

Governments have developed cybersecurity strategies that outline their overall plans aimed at understanding the risks in cyberspace and developing response options. These strategies often stress the interrelated nature of various types of cyber threats, the wide range of possible societal impacts, and the cascading effects of risks. As a result, governments call for a comprehensive approach, including various type of actors such as businesses, citizens and researchers.

This is apparent in the second Dutch **National Cybersecurity Strategy (NCSS2),** dating from 2013 and published by the Ministry of Security and Justice. One of its objectives is to "strengthen research and analysis capabilities to gain more insight into threats and risks in the digital domain."[12] It stresses the importance of a multi-stakeholder approach, with public-private partnerships, where relevant cooperating internationally.[13] Specifically, it highlights the value of a multidisciplinary approach, "in which the non-technical sub-areas are also included and needed to promote cybersecurity innovation."[14]

Many of these points are echoed in the **National Cybersecurity Research Agenda II**, which provides a framework for cybersecurity research projects. The NCSRA II supports the concrete implementation of the fifth goal of the NCSS2: "The Netherlands has sufficient cybersecurity knowledge and skills and invests in ICT innovation to attain cybersecurity objectives". The research agenda was initiated by the public private platform on security and privacy IIP-VV and embraced by the Dutch Cyber Security Council (CSR) and synchronized with the EU Cybersecurity Strategy. It focuses on two topics: 'Security and Trust of Citizens'[15] and 'Security and Trustworthiness of Infrastructure'.[16] The agenda:

- has an intermediate term in mind ("security challenges of the next 6-12 years"),
- explicitly mentions economic benefits of research ("stimulate the Dutch security economy and promote innovation in this sector"[17]);
- highlights the importance of cooperation with "knowledge institutions and relevant public and private organizations"[18];
- aims to, in line with our observation that cybersecurity affects the whole of our society, fund a broad range of research: "while traditional computer science plays an important role, it also considers the roles of α and γ disciplines."
- stresses that effective research will depend, to a large extent, on inter-disciplinary research. Different disciplines often operate in a somewhat stovepiped manner, "with radically different backgrounds and traditions. Stimulating collaboration between them is important: combining insights from different fields will be crucial for addressing some of the challenges in cybersecurity."[19]

Based on the National Cyber Security Research Agenda, two trajectories of research and innovation were set up. Simultaneous calls for short term and long term research proposals were held in 2012 and 2014, financially supported by several Dutch ministries and disciplines within the Dutch research council NWO. Funding ministries of the second call are Defence, Economic Affairs, Interior, Security and Justice, Finance, Infrastructure and the Environment. Long term research in this call is funded by NWO physical sciences, social sciences and technical sciences. Currently 20 long term research projects are running, as a result of this competition. In addition 14 second phase Small Business Innovation Research

(SBIR) short term R&D projects are running as a result of competitions organized by the Netherlands Enterprise Agency (RvO).

The long-term Cyber Security Research Program set up by NWO focuses on the development of products, services and knowledge for the security of the digital society, encouraging collaboration between the business community and science, with the business community as both supplier and customer.

In addition to the projects funded in this national program, NWO Physical Sciences (NWO-EW), the Ministry of Security and Justice and the U.S. Department of Homeland Security (DHS) jointly fund research in the field of cybersecurity. Three cybersecurity research projects with Dutch and American scientists receive grants adding up to a total amount of approximately 1.3 million Euros. The Netherlands and the U.S. each pay half. Currently running projects focus on malware on smartphones, notification regimes against cybercrime, and the defense of SCADA and ICS.

# 4 Analysis of NWO's Cybersecurity Research Portfolio

## 4.1 Approach of the analysis

This sections focuses on the 23 NWO funded research projects. We have examined these projects granted in three different rounds of the NWO cybersecurity long term research program. In our analysis, we have zoomed in on the following six dimensions of research:

- ➔ **Content**: what overarching NCRSA research theme does the project address?
- ➔ **Application domain**: what areas of society and/or what critical infrastructures does the research target?
- ➔ **Output**: what response-level does the research provide input for?
- ➔ **Stages**: What phase of a cyber-crisis does the research target?
- ➔ **Disciplines**: What disciplines are involved in the research?
- ➔ **Collaborating partners**: What type of actors (public-private etc.) are involved?

By scoring all projects on a number of elements related to the six dimensions introduced above, we generated charts that give an idea of the scope of research covered. The scoring has been done on the basis of the available project summaries (abstracts). The scoring is on the basis of the number of projects involved rather than the budgets available to the project.[20]

Subsequently, the first draft of this paper served as input for a roundtable discussion, held 3 March 2015, which included participants from the Dutch cybersecurity research community and representing different research disciplines. Supported by the input of the roundtable and verified by additional interviews with three Dutch Internet community experts, the analysis of the NWO research portfolio was complemented and suggestions for next steps in cybersecurity research programming were formulated and included at the end of this paper.

For the entire duration of this analysis, we had close cooperation with NWO and IIP-VV representatives.

## 4.2 Main observations

We first summarize the main observations:

- The current NWO research portfolio covers all research themes defined in the NCSRA I and II.
- There is a strong focus on four research themes:
  - Malware and malicious infrastructures
  - Attack detection, prevention, and monitoring
  - Secure design and engineering
  - Risk management, economics, and regulation.
- Offensive cyber capabilities and forensics have received the least attention.
- Most research focuses on providing benefits to governmental actors or the private sector.
- About half of all projects target a specific critical infrastructure sector, with most attention on public order and safety; legal order; and telecommunications.
- Projects predominantly are targeted at the policy or operational level. Almost all policy-focused research contains a 'risk management' focus. Other aspects of policy responses, such as doctrine development, are not explicitly considered.
- Only a few projects focus on the tactical and strategic levels of response.

- Most projects are aimed at preventing cyber threats from materializing. Almost all projects focus on prevention and detection, with hardly any research addressing implementation of lessons learned, stabilization or attack mitigation stages.
- Most involve β-disciplines computer sciences and/or engineering.
- While β-disciplines are very dominant, there is a great number of projects that involves at least two different disciplines. As such, the research projects can certainly not be considered monodisciplinary.
- γ-disciplines such as Psychology, Law, Policy or Economics are somewhat involved in the projects, primarily in those related to risk management-like approaches.
- Almost all projects involve collaboration with multiple actors. Half of them involves collaboration between knowledge institutes, the government and the private sector, around a third involves collaboration between knowledge institutes and the private sector.

## 4.3 Research process deployed

Up to now, NWO has deployed two national rounds, i.e. two calls for cybersecurity research proposals, the first in 2012 and the second in 2014. The cybersecurity program was positioned as a thematic program soliciting research project proposals not restricted to computer science, welcoming proposals from other disciplines or with a on multidisciplinary approach.

Applicants had to adhere to a number of criteria:

- Projects should be strategic, long-term research
- Proposals are expected to be prepared by a consortium, i.e. Public-Private Partnership
- The research topic should be based on any of the research themes described in the NCSRA (I or II)
- Project should at least employ one PhD for four years or postdoc for a period of two or three years.
- The maximum total funding requested from NWO is € 500.000.
- The maximum co-funding from consortium partners is 100% of the total funding requested from NWO.

As indicated before, a total of 20 projects were selected and financed after these two national rounds. These two were complemented by a third (international) round in which 3 projects were rewarded. Each of these third-round projects is jointly executed by researchers from a university in the US and The Netherlands. This type of cooperation is possible based on an Agreement between the Government of the United States of America and the government of the Kingdom of the Netherlands on cooperation in science and technology concerning homeland and civil security matters.

## 4.4 What overarching research themes do the projects address?

In developing its National Cyber Security Research Program, NWO used various criteria in determining what the substantive direction should be of cybersecurity research (see above). First of all, the NCSRA was chosen as the frame of reference, with the full set of research themes. Thus, as a research program, it took a broad approach aiming to cover the full range of research themes, all considered relevant.

We examined a number of issues related to the themes as defined in the agendas:

- Are all themes considered relevant and are they addressed in similar ways?
- Are there any thematic blind spots in the overall coverage of the selected research projects?
- How do the themes and selected projects balance between the need for broad coverage and focus?

The NCSRA II lists 9 research themes:

| Themes | Description |
|---|---|
| **Theme 1: Identity, Privacy and Trust Management** | Identity management, privacy protection and managing trust in the online world are essential functions for adaptation of information technology in our society. These functions are to be applied and tailored to the needs of many different application domains. |
| **Theme 2: Malware and malicious infrastructures** | Malware and Malicious Infrastructures focuses on analysing malware and the criminal infrastructures, to develop better and more effective defences against the malware threats. Research in this area is important since malicious software is the essential means for many types of attacks, thereby generating social and economic power for the attackers. |
| **Theme 3: Attack detection, attack prevention, and monitoring** | This research theme focuses on the challenges to prevent and detect cyber attacks, including large-scale denial-of-service attacks, epidemic virus distribution, and stealthy and dormant attacks on high-value targets (i.e. Advanced Persistent Threats). Since these attacks continuously get more complex and more sophisticated, the preventive and detection techniques have to get better. |
| **Theme 4: Forensics and incident management** | The goal of cyber forensics is to identify, collect, preserve, analyse and present digital evidence of criminal activity, and to find those responsible, often in the aftermath of an attack. Incident management focuses on containment, recovery and becoming operational again at minimal cost and as quickly as possible. In particular, forensics research needs to balance on one hand the need to re-bootstrap the infrastructure after an incident, and on the other side the need to keep the traces left by the attack that can be used for forensics research. |
| **Theme 5: Data, Policy and Access Management** | Data, Policy and Access Management is concerned with research on novel access management and compliance monitoring techniques to preserve confidentiality, availability, and integrity of data according to well-defined security policies. Given the current trend toward cloud based data storage, with the associated ambiguities regarding ownership and access, this problem is getting increasingly complex and important. |
| **Theme 6: Cybercrime and the underground economy** | Research in this theme focuses on understanding the modus operandi of perpetrators of cybercrime, their motivations – which may be financial or ideological – and understanding the underground economy which they form. In practice, there are very different actors engaging in illegal activities, ranging from online vandals, hacktivists, criminals, organized crime, to nation states. The goal is to become more effective against cybercrime, e.g. by finding the effective ways to intervene, or by improving cooperation between (private and governmental, national and international) parties against cybercrime. |
| **Theme 7: Risk Management, Economics, and Regulation** | The focus of this research theme is on improving risk management, a better understanding of cybersecurity economics, and what the role of government(s) both in national and international context should be in cybersecurity. Ultimately, good risk management should provide the basis for allocating resources to improve cybersecurity in the optimal way. Such risk management can be carried out at corporate level, but also across sectors, over value chains, or at (inter)national level. Taking into account the many chain dependencies between ICT systems and services poses an additional challenge here. |
| **Theme 8: Secure Design and Engineering** | Security engineering is a relatively new field and still lacks the methods and tools to design, build and cost-effectively test secure systems. Recent events have revealed core components and services we thought could be trusted to be insecure, drawing attention to the basic need to secure digital communications, and showing that current approaches to assess security are inadequate.<br>This research theme focuses on developing methods, tools and techniques to improve security engineering. Particularly challenging is the design and engineering of secure systems of systems, in which the interaction of heterogeneous unit plays an important role in the security of the whole system. Also, raising awareness and attention for security in the design phase is a challenge. |
| **Theme 9: Offensive Cyber-Capabilities** | Offensive cyber capabilities are becoming essential for defense organizations, but also in law enforcement and for prosecution. Law enforcement agencies have indicated an interest in offensive technology, not so much for 'striking back' at attackers, but with an eye on observing, disrupting and stopping criminal activities, as well aiding the apprehension of the perpetrators. This research theme focuses on improving the knowledge position and the operational cyber-capabilities in the widest sense. |

**Table 1 NCSRA-II themes.**

Figure 1 below shows the theme distribution among the 23 projects. We note that:

- All NCRSA themes are addressed at least once.
- A few themes have received considerably more attention
    - Theme 2: Malware and malicious infrastructures ;
    - Theme 3: Attack detection, attack prevention & monitoring;
    - Theme 8: Secure design & engineering; and
    - Theme 7: Risk management, economics & regulation.
- Only a few projects touch upon
    - Theme 6: Cybercrime and the underground economy; and
    - Theme 5: Data, policy & access management.
- Almost none of the projects look at
    - Theme 9: Offensive cyber capabilities; and
    - Theme 4: Forensics & incident management.

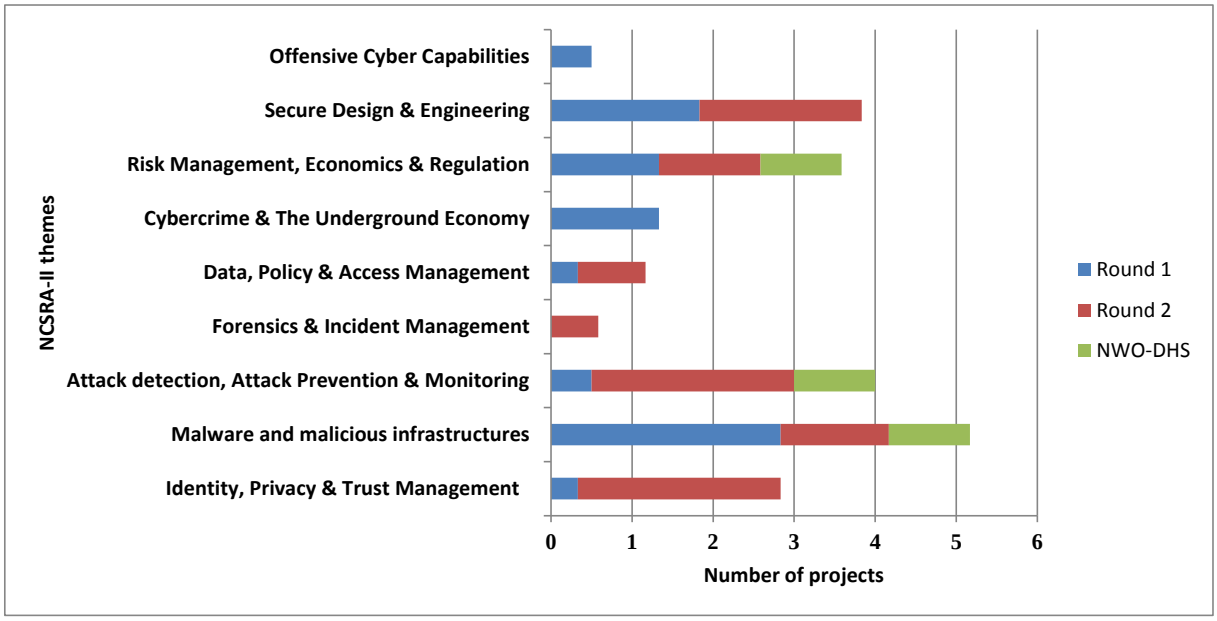


**Figure 1 NCRSA-II themes addressed in NWO research projects. If a project touched upon multiple themes, these received a weight equal to their importance. For example, one project that focused mostly on theme 1, and partly on theme two, received a weight of 0,75 for the first theme, and 0,25 for the second.**

The process of the identification of the NCSRA research themes can be considered diligent. The IIP-VV has involved the broader cybersecurity community, consulted during the NCSRA development process. Therefore, these 9 themes as such were not debated during the roundtable discussion. The fact that all themes were addressed met with approval and the fact that some themes were more addressed than others could have had rather inconspicuous reasons than a structural bias in the research community. In addition, one could argue that theme 9 and 4 are more specifically focused to the defense domain and investigatory process, while the other themes have much broader implications. Cybercrime (theme 6) is becoming an increasingly prominent issue, which could be emphasized more.

Given some of the broader trends presented in the previous section, it would be useful to assess to what extent the current themes can comprehend the new developments as well.

During the roundtable discussion participants gave examples demonstrating the multi-disciplinary character of cybersecurity (research): money muling (i.e., laundering money that

is illegally acquired through fraud), malware that could be targeted more effectively. Or, cyber risk assessments which could raise more awareness if they were also addressed from the victim's perspective, rather than purely threat-based. Also, because of the increased prominence of state actors, in several roles, attention in risk management could be directed at modalities of public governance other than legislation or regulation, for instance in setting standards. Another topic that is emerging, as described in the previous section, is that of big data analytics. While privacy issues are dominant regarding this topic, there are many other issues involved that make it a complex matter that might deserve dedicated focus. And, related to the Privacy theme, a broader name such as Protecting Fundamental Rights could be used, which would include freedom of expression among others.

Finally, the question of the cohesiveness of the themes and the subsequent projects selected for NWO funding was also raised. As indicated before, the NCSRA I and II have had a rather broad approach to the cybersecurity domain. As a result, it is rather logical that the 23 projects sparsely cover this wide spectrum. Thus, the debated issue is whether there should be more focus (possibly different per funding rounds) in which bigger projects could be supported, more tuned into future needs rather than accommodating the current existing research base in the Netherlands or covering the entire spectrum of topics.

### 4.5 Where will the research results be applied?

The application domain perspective considers, first, the type of actors that would benefit from the research, and , second, what (if any) critical infrastructures the research is focused on.

We defined 4 types of actors, that can be distinguished on the basis of different responsibilities and interests within the cybersecurity domain: private sector, government, academia, civil society, and other (unspecified). Each of these actors considers ICT as an increasingly asset for itself, including Academia, and each have their own role, responsibilities and challenges in addition to many shared ones.

Figure 2 below presents which actors can be supported by the research, which clearly indicates that most research is focused on addressing the issues of government and private sector companies. This is not a surprising result as they represent the majority of the interests. Civil society is still lagging despite the increased emphasis that is being put on, for example, enabling NGOs to contribute to the development of cybersecurity norms.

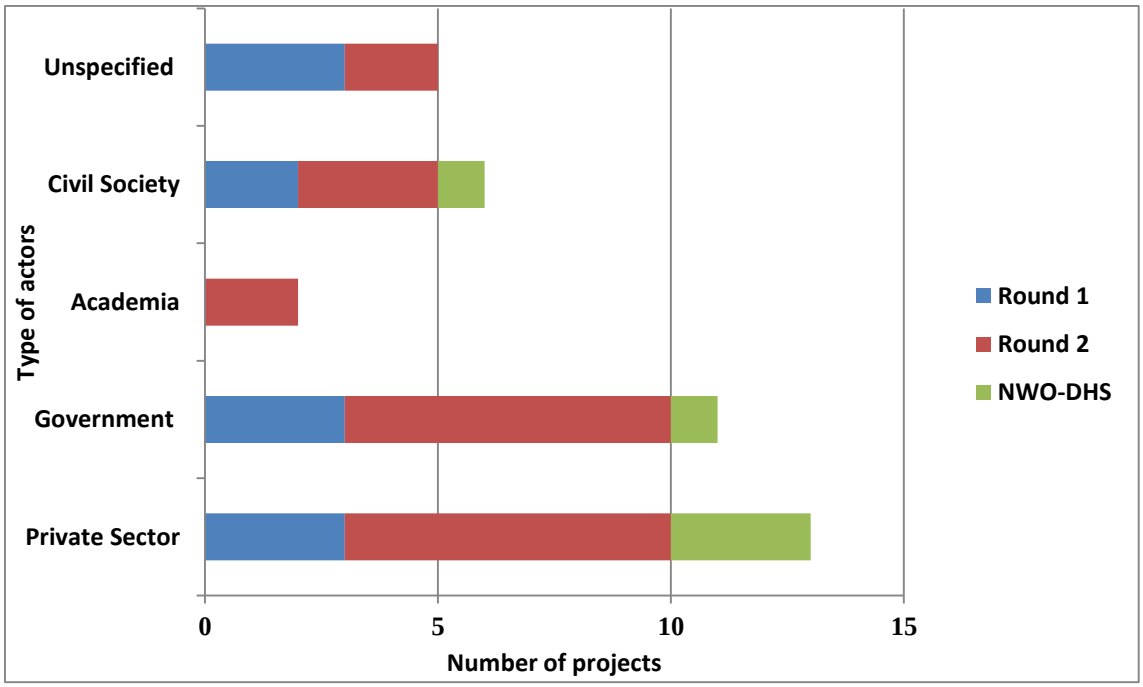


**Figure 2 Type of actors envisioned in NWO research projects to benefit from research, distinguishing private sector; government; academia; civil society; and unspecified. Some projects aim to produce benefits for multiple actor types.**

We also examined the possible research focus on critical infrastructure (CI) sectors. The CI sectors appear dominantly in discussions about cyberspace and national security, especially regarding potential attacks on energy or telecom grids by both state actors and non-state actors, and the impact that outages may have on broad parts of society.

Figure 3 below indicates that:

- A total of 10 projects (43%) target a specific critical infrastructure sector
- The focus is predominantly on three sectors, i.e.: public order and safety; telecom; and legal order
- The remaining sectors are all specifically addressed once, while the chemical and nuclear industry sector is not explicitly targeted in the research projects.

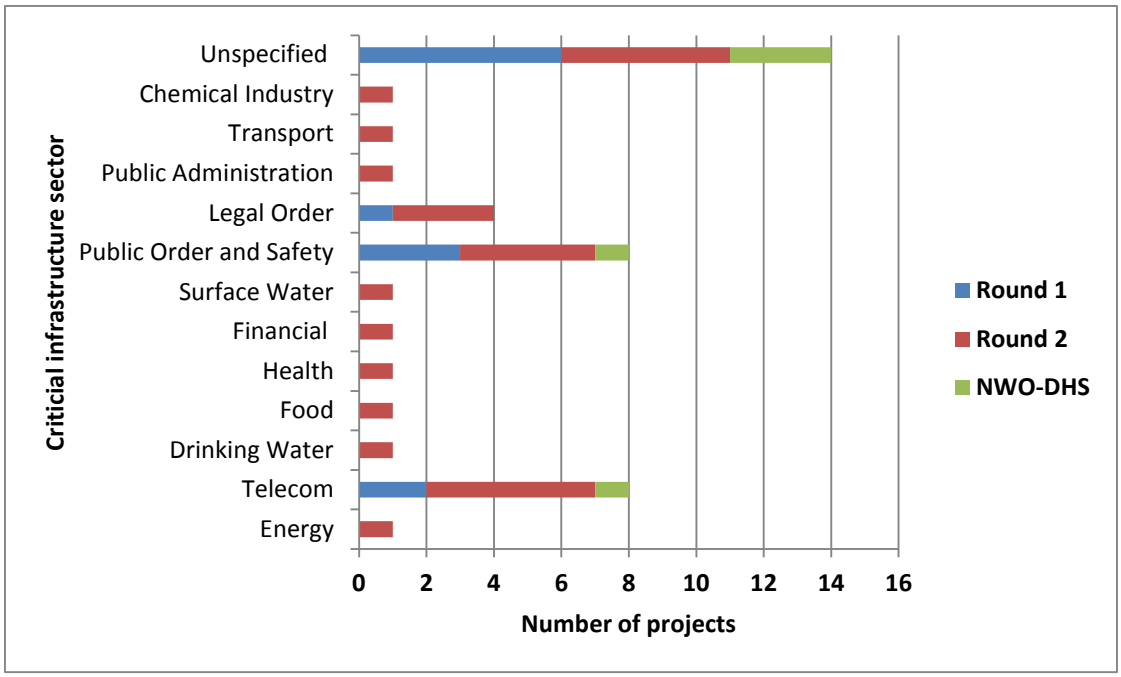


**Figure 3 Critical Infrastructures addressed in NWO research projects. Some projects address multiple critical infrastructures.**

While the heavy focus on and involvement of the telecom sector as one of the most crucial critical infrastructures (and also provider of much of the supporting infrastructure for the Internet) in society is easy to explain, the very limited explicit consideration on the energy, financial, and water management sectors can be considered remarkable. But we need to be careful here drawing conclusions, since dividing 23 projects into 13 disciplines means we deal with some statistical insignificance, that can only be solved by looking at a larger number of projects.

## 4.6 What decision-making level will benefit from research results?

ICT has become an enormous push for growth in our economies and has supported various types of innovation and transformation in society. This also requires an increasing need for secure products, services, and procedures. It also means that states, companies, researchers, and individuals need to protect their assets. Thus, research projects are focused on understanding underlying problems and developing solutions at various decisionmaking levels, from technical and operational (e.g., finding new methods to find traces in mobile devices) to strategic ones that focus on conceptual, long-term, and broad adaptations to current practice (for example, how to understand the concept of deterrence in cybersecurity).

For purposes of examining the current NWO cybersecurity research project portfolio, we distinguished four decision making levels and within each level a number of functions that are commonly executed at these levels:

1. **Operational**: Detection, Identification & Authentication; Risk Assessment; Intervention & Neutralization; Impact Reduction; Incident Response; Training and Exercises; Operations.
2. **Tactical:** Information Management**;** Communication.
3. **Policy:** Doctrine**;** Situational Awareness & Assessment; Risk Management**;** Command and Control.
4. **Strategy:** Policy & Governance; Legislation & Regulation.

Based on Figures 4-6, we note that:

- Most research projects target the operational and policy decision making levels (over € 4 million on a total of about € 10 million spent on research projects thus far), with few projects focusing on tactical (€ 1,3 million) and strategic levels (around € 0,4 million).
- Of all research projects looking at the policy decision-making level, almost all fell in the category of the 'Risk Management' function. Functions as 'Command & Control', 'Situational Awareness & Assessment', and 'Doctrine' were (almost) not represented.
- Research projects aimed at providing operational support look primarily at Detection, Identification & Authentication, Impact Reduction, and to a lesser extent Risk Assessments functions. Operations, Training and Exercises, Incident Response and Intervention & Neutralization are (almost) not addressed.

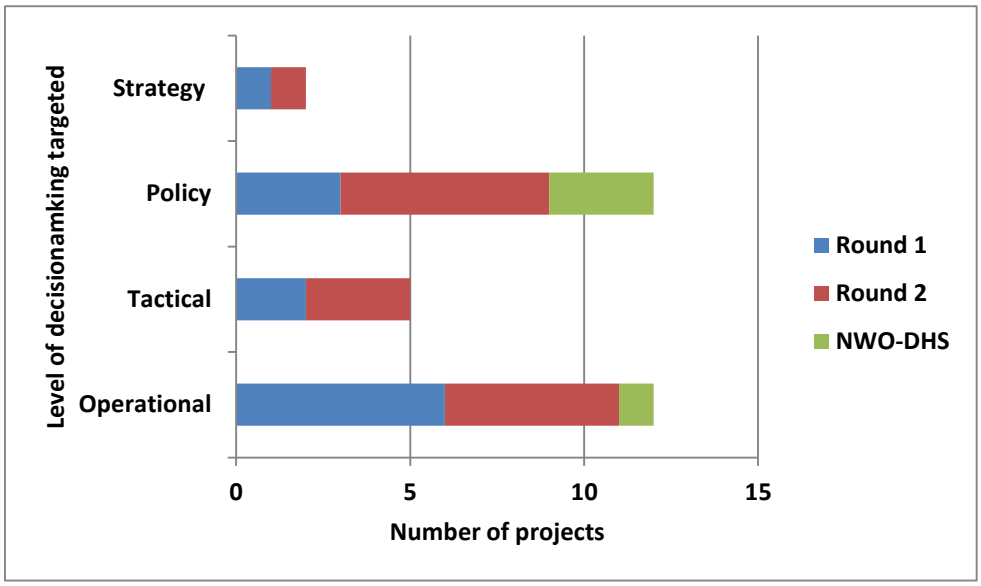


**Figure 4 Level of NWO research projects, distinguishing 4 levels: strategy, policy, tactical and operations. Some projects target multiple levels.**

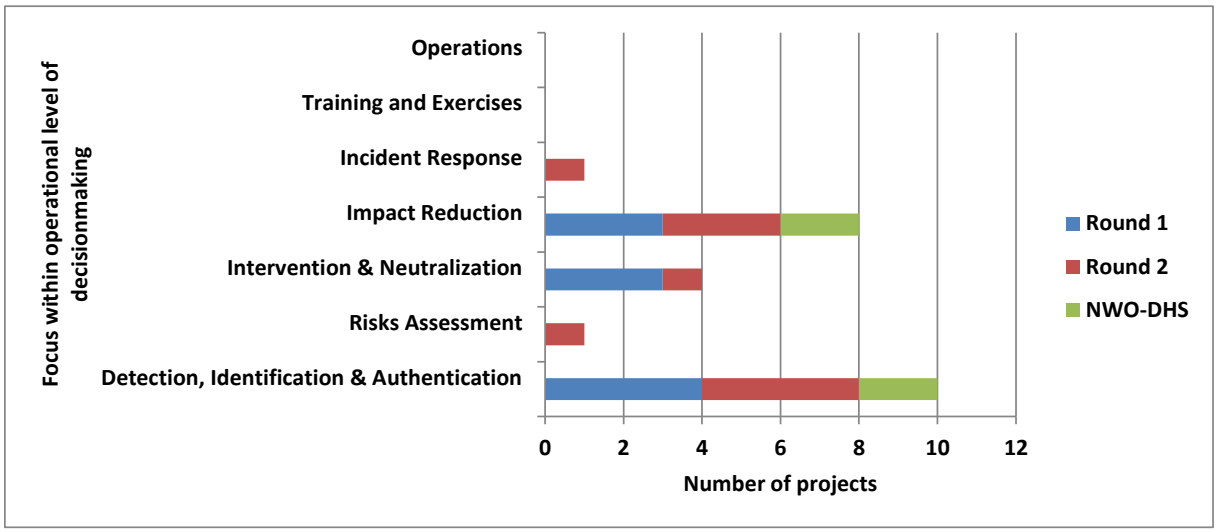


**Figure 5 Specific application areas for all NWO projects addressing the operational level.**

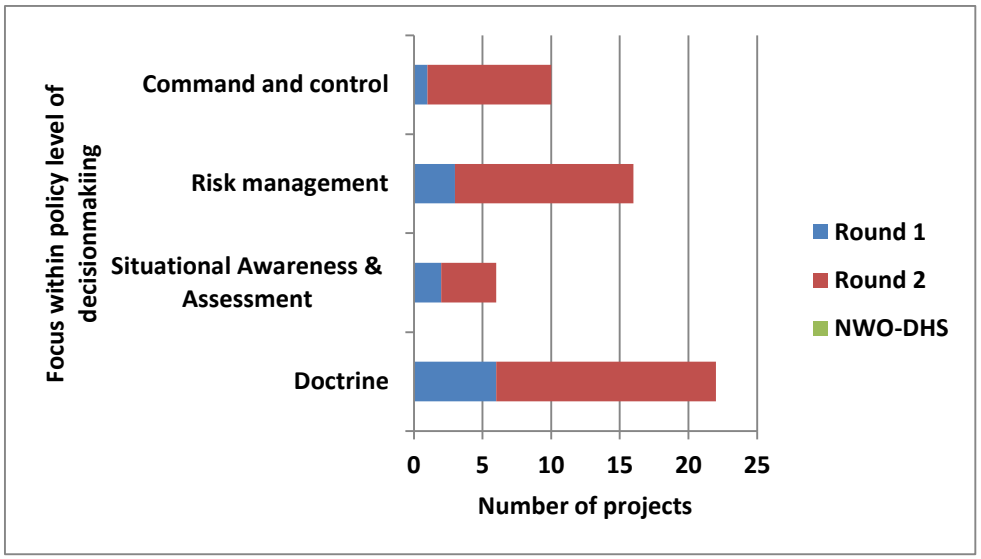


**Figure 6 Specific application areas for all NWO projects addressing the policy level.**

During the roundtable, there was widespread acknowledgment of the rather lopsided (asymmetrical) distribution of projects at the operational and technical levels. Concurrently, participants were stressing the clear need for research on the more strategic levels.

There seem a number of obstacles that currently prevent a more balanced approach:

- The lack of supply of strategic-research project proposals
- The limited size of projects and available budgets
- Some of the funding conditions (need for valorization of the research results, requirement to connect to top sectors)
- Technology push nature of some of the cyber research work

## 4.7 What stage of cybersecurity does the research target?

Next, we looked at the stage of cybersecurity which was addressed in the research projects. There are various ways of splitting up the so-called security chain, basically ranging from Prevention (or even Pre-emption) to Response. Obviously, there is no right or wrong in stressing a particular stage or not. On the one hand, focus on Prevention could be preferred as such approaches can often save many costs. On the other hand, given the fast technological advances, it is hard to continuously keep up with new threats and trends. It is also said that many private companies often rather run the risk of attack than having to invest in costly security (preventive) measures. In these instances, adopting resilient approaches to recover from attacks or to have some built-in redundancy into organizations might be advisable. An entire other direction would actually be to develop offensive capabilities. However, this topic is specifically addressed within one of the research themes of the NWO program and thus not considered here.

For purposes of this analysis, we distinguished the following stages: Prevention (i.e., everything focused on not being harmed, including Detection), Mitigation and crisis management, Stabilization, and Implementation of lessons learned.

As the figure below shows, almost all NWO projects focus on Prevention and Detection, with hardly any research addressing Implementation, Stabilization or Attack Mitigation stages.

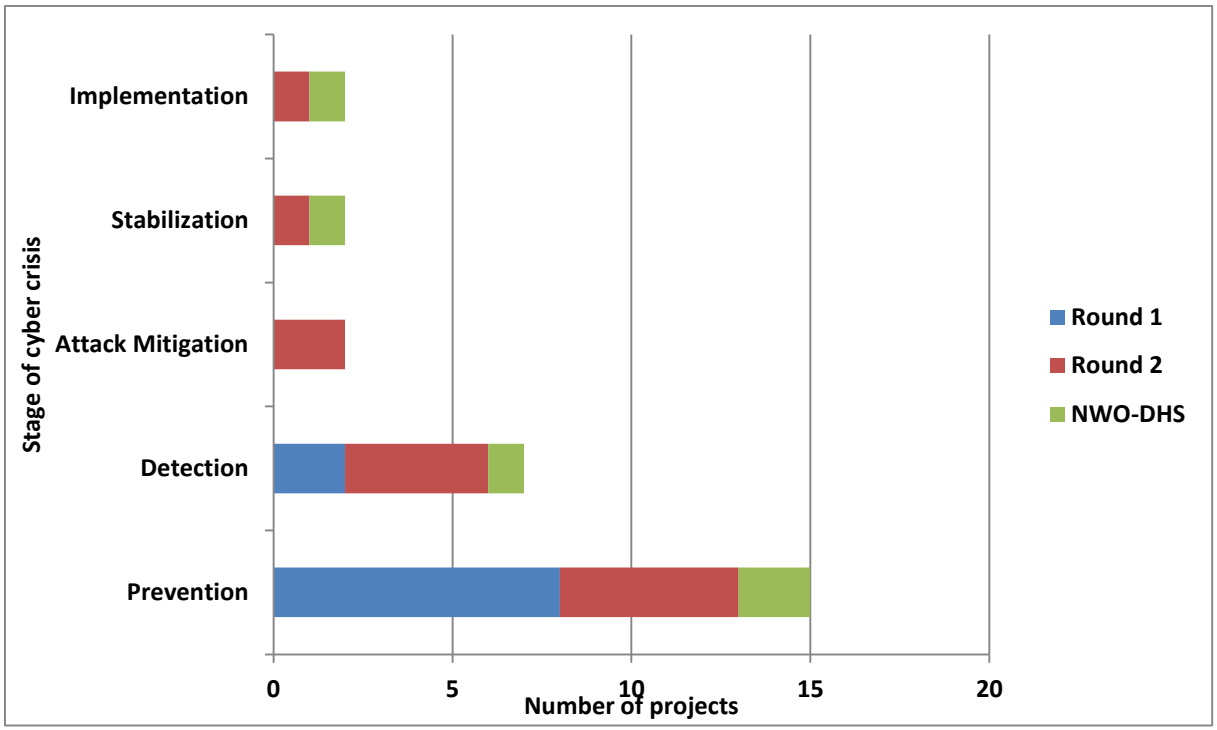


**Figure 7 Stages of cyber crises addressed in NWO research projects. Some projects target multiple stages.**

Again, preference for one approach over another is not straightforward, but some more emphasis on the resilience phases (Mitigation, Stabilization) of a cyber crisis could help in making more informed decisions about the effectiveness of these various ways to deal with cybersecurity.

## 4.8 What research disciplines are involved?

Multidisciplinary approaches in cybersecurity are deemed important as cybersecurity threats often have multi-dimensional characteristics. In addition, the range of topics that are addressed within cyberspace in general and cybersecurity in specific is wide. Beyond the technical aspects of security, for instance the secure operations of internet protocols or the Domain Name Server system, there are many behavioral (e.g., how can awareness of cybersecurity be raised), organizational (e.g., what governance model is most effective to the various subsystems of cyberspace), legal problems (e.g., what constitutes a cyber crime or are existing bodies of international law also applicable in cyberspace) that need to be better understood. But given the interaction across many of these aspects, next to multidisciplinary it is also necessary to conduct true interdisciplinary research.

Which disciplines are involved in the current research projects? And to what extent is research 'interdisciplinary', that is are multiple disciplines involved in a research project? We assessed disciplinary involvement of the projects using the following classification of academic research fields.[21]

There are various ways of classifying different (sub)disciplines within bigger domains. Given that many debates are addressing the chasm between alpha/gamma studies on the one hand and beta on the other, we have taken this division as a starting point. The disciplines mentioned in the table below are not meant to be exhaustive, but should cover the main areas of research that may be relevant for cybersecurity studies.

| Alpha Sciences (Humanities) | | | | Beta Sciences (Formal/Natural) | | | | | Gamma Sciences (Social Sciences) | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Cultural Studies, Linguistics | History | Media | Philosophy | Computer Sciences | Engineering | Life sciences | Mathematics | Physics | Economics | Law | Policy/political sciences | Psychology | Sociology |

Figure 8 below show what academic disciplines are involved in the currently ongoing research projects. We observe that:

- γ-disciplines such as Psychology, Law, Policy or Economics are somewhat involved in the current NWO cybersecurity research program, primarily related to risk management-like approaches.
- Most current research projects involve β-disciplines computer sciences and/or engineering.
- α sciences like philosophy or history are entirely absent. One research projects looks at the ethical aspects of software defined networking systems, but this is not the main focus of the project.

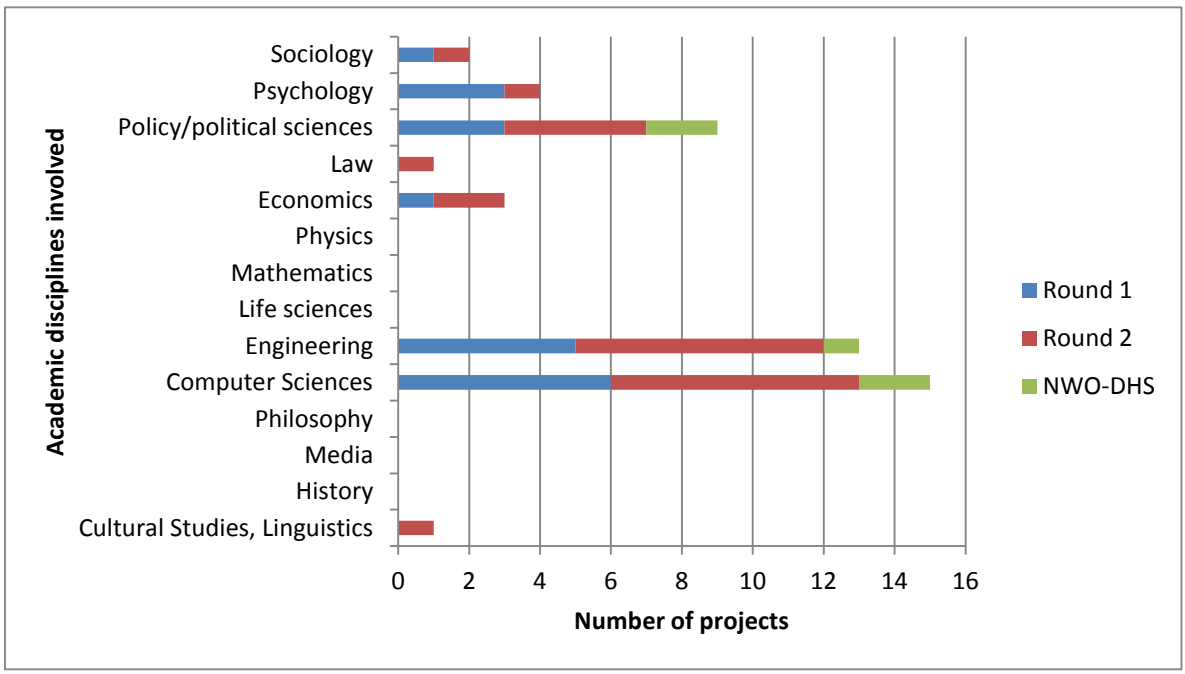


**Figure 8 Disciplines involved in NWO research projects.**

While β-disciplines are very dominant, there is a great number of projects that involves at least two different disciplines. As such, the research projects can certainly not be considered monodisciplinary.

The number of disciplines involved in each project is listed in the figures below.

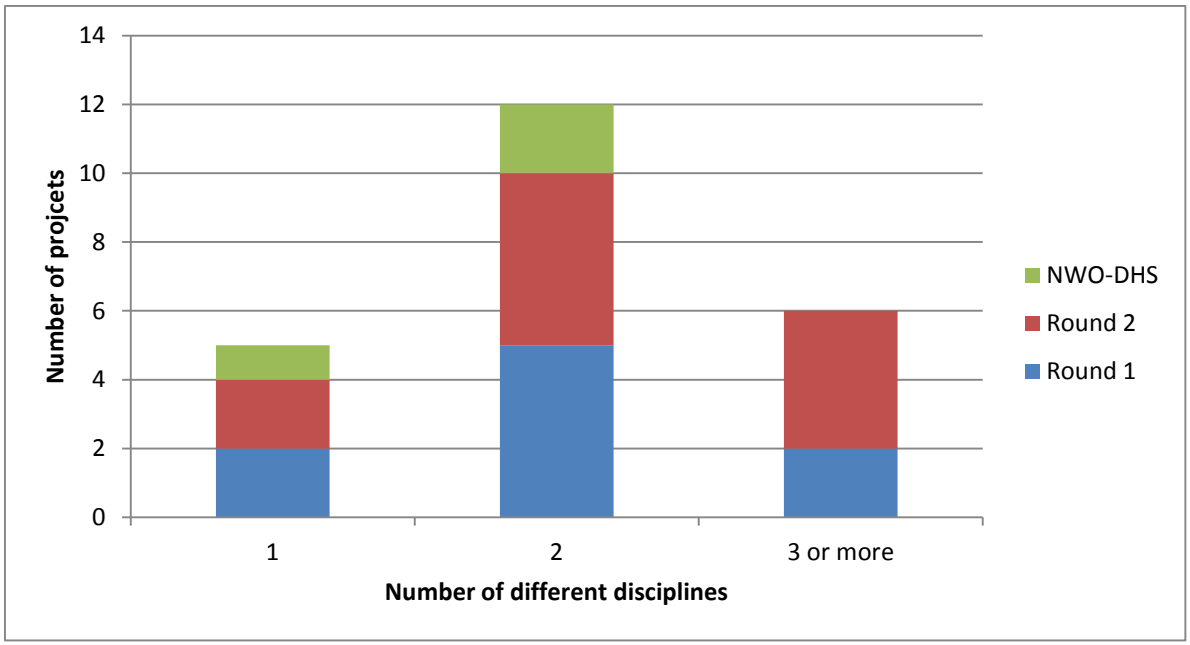


**Figure 9 Number of disciplines involved in individual NWO research projects.**

While the interdisciplinary nature is for the majority within the gamma or beta research domain, there is quite a number of beta and gamma crossovers within projects, almost half of the total (10 projects). In the second round, this has become even more visible than in the first call for projects. This is represented in Figure 10.

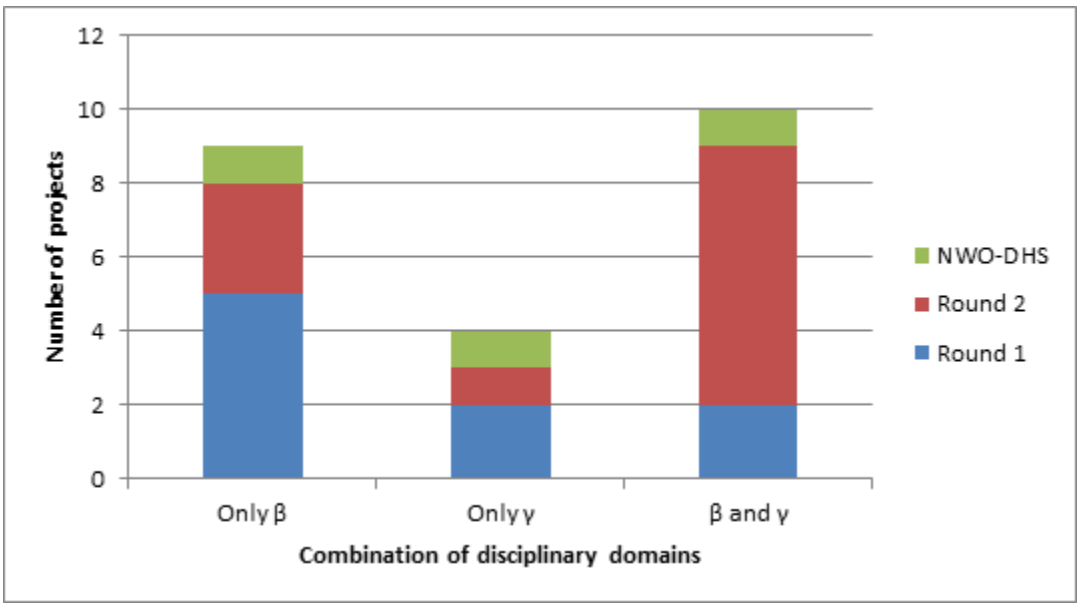


**Figure 10 β, α-and γ-disciplines addressed by NWO research projects.**

Representatives of the Dutch research community largely recognize the outcome of these classifications and the dominant technology-orientation (i.e., computer sciences and engineering) of the project portfolio.

The translation of the technology on various behavioral levels (e.g., of states, societies, individuals) is not yet sufficiently addressed. There is a need to involve other disciplines to address issues more comprehensively. Examples of these are:

- (Media) communication sciences: informing public opinion in better interpreting actual cyber events, which is currently without sufficient background knowledge.
- Philosophy / Humanities: addressing some of the issues from another perspective
- Criminology: to better understand the behavior of people in cyberspace. Who are guilty of hacks and cybercrime and what are their reasons for operating this way?
- Public Administration: how can we shape governance issues?
- Economy: what are the costs of cyber (in) security, how can criminal business models be countered?
- Other behavioral sciences: what is the social behavior of states, how can we create better integration of new tools?

Also, integration of the various knowledge domains can improve understanding of the various challenges in cybersecurity. Now, there is a tendency to get too deeply involved in subdomains of cybersecurity. Crossovers can be created by consolidating research through:

- Concentration by location (e.g., in the UK much of the cyber research projects are concentrated around Cambridge);
- Funding through combining resources for broader oriented projects;
- Stimulating and stressing the connecting cybersecurity elements across disciplines. Requires sharing resources between NWO-domains;
- Allowing man on the moon type of projects being part of the research program.

An important obstacle to interdisciplinary research is the lack of opportunity to publish research results in journals which still tend to be strictly disciplinary confined. While creating dialogue across disciplines is important, the actual outcomes need to be packaged in mono-disciplinary terms.

### 4.9 Research collaboration partnerships

As cybersecurity becomes a key issue to all, the various stakeholder groups (including governments, the private sector, the technical community, civil society and international organizations) should play an active role in ongoing discussions about its governance, management, and security. The multi-stakeholder approach in these debates should also be reflected in research. Some issues might actually warrant less or more representation of types of stakeholders, but the overall objective in assessing this dimension is whether there were specific voids or biases in NWO's research portfolio.

We looked at actors involved in research collaboration within the set of current NWO projects. Is there cooperation between two or more knowledge institutes? Between a knowledge institute and a governmental actor? Between a knowledge institute and the private sector? Or between all three?

Figure 11 below indicates that half of all projects involve collaboration between knowledge institutes, the government and the private sector, followed by knowledge institutes collaborating with the private sector.

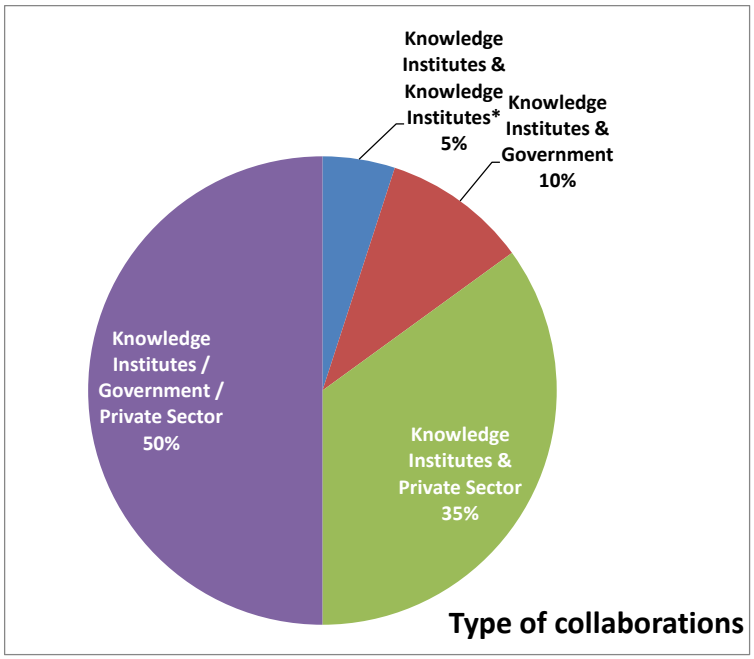


**Figure 11 Research collaboration across all NWO research projects. It can be stated that there seem to be no obstacles in setting up collaborative research proposals in cybersecurity.**

Given the fact that collaboration with at least one partner other than a knowledge institute was compulsory, this is not a surprising observation.

However, it remains unclear what the nature of collaboration is during the research process and whether private sector partners remain sufficiently involved. Some researchers have argued against the mandatory participation of private companies as it would lead the results of the research too much to the needs of the private partner rather than to the broader research agenda. In addition, co-funding constructions are perceived to be a restriction of multidisciplinary research.

Collaboration across (NL-US) borders is currently taking place within the three NWO-DHS projects. For some researchers, a strict focus on the Netherlands is actually sensible, especially regarding experiences across legal systems which hardly translate. Some researchers have the idea that international connections of academia are well developed, while others indicate that especially in such a broad domain as cybersecurity, many research activities in other places in the world go unnoticed, which could lead to duplication of effort.

# 5 Conclusions and Recommendations

The Netherlands has one of the most well structured approaches toward cybersecurity in Europe and the rest of the world. An overall national cybersecurity strategy which is used to guide both public and private sector initiatives is being kept up to date in an environment which is very dynamic. Based on its principles, a cybersecurity research agenda aims at developing research excellence in the cyber domain as well as developing solutions to the challenges faced by governments, businesses, and citizens alike. Short-term and long-term research programs have been established in a coordinated effort.

Developments in this field are fast paced. Almost coming out of its infancy, cyberspace is growing its commercial activities, attracting criminal intentions, increasing threats to users at a societal and individual level, and drawing in forms of regulation and the like.

NWO's cybersecurity research program and the SBIR fund for cybersecurity R&D have given an important stimulus to cybersecurity research in the Netherlands. A total of 7 different Dutch universities, 3 different American universities, 6 Dutch knowledge institutes (TNO, NSCR, WODC, NFI, NCSC, AIVD), and 34 public and private organizations (mainly businesses) are currently partnering in the execution of the 23 NWO long term research projects. Two rounds of SBIR resulted in the development of 14 different prototypes by 13 different companies.

However, it is debatable whether the current stream of projects is able to provide enough answers to the problems cyber is facing. Our assessment is that these projects are bi-disciplinary at best, technically-oriented, and very operational in approach. While undoubtedly many relevant technical matters are being considered, the bigger, conceptual, shaping powers are only addressed in a minimal way.

The past two thematic calls for proposals within the NWO cybersecurity research program have resulted in a portfolio of projects with the following characteristics and needs for improvement:

**Content**

- There are a number of biases in the orientation of the current research portfolio:
  - Skewed consideration of critical infrastructures
  - Little focus on resilience in cyber crises
  - No inclusion of alpha studies

These biases should be further analyzed, for instance, by also taking into consideration the larger cybersecurity research portfolio across the Netherlands. It also raises questions about whether preferred research orientations or a certain balance in our national research orientation spectrum should be created.

- Consideration of including a broader, international orientation might be worthwhile. This could be done in supporting exchange programs, setting up bilateral research programs, and the like.
- Despite the cross-sectoral approach of the program, there is no sufficient inclusion of topics outside of the technical domain. As such, it encourages expert researchers within the cybersecurity domain to develop proposals, which are primarily focused at the

operational, technical levels. The involvement of other disciplines needs to be encouraged. Systems-oriented research as well as the policy and strategic dimensions of cybersecurity are underrepresented.

- Cybersecurity is a domain that is increasingly overlapping with issues of governance, economy, and law. The novelty of the domain means that perspectives on these issues are constantly in flux. Synchronized calls for long term fundamental research and short term product innovation routes in the area of cybersecurity turned out to be a successful combination. Simultaneous matchmaking prior to announcing these two call types resulted in fruitful cross fertilization. Three different target groups are equally motivated to seek matches. Businesses get a better understanding of the research that is going on and get an opportunity to pitch their needs. Researchers could become inspired by entrepreneurial needs and get to know suitable companies they could interest to join their consortia. Governments, as (launching) customers, are looking for solutions improving (national) cybersecurity, etc. The importance of this mechanism of combining short term and long term research should be emphasized and thus the continuation of this approach is recommended.

**Finance**

- The coherence of the portfolio can be significantly improved. Within a wide spectrum there are now a relatively small number of projects awarded without much connection. Question is whether there should be a focus within the program to be able to find a better balance among projects or whether one can create more synergy and holistic view by connecting the different projects wherever applicable during their execution, e.g. via yearly NCSRA symposia, periodic meeting between applicants and consortium members, or whether an entirely different approach (man on the moon type project) would provide more visible synergy and impact.
- There is need for a funding scheme that can support the multidisciplinary dimension of the program in order to address the underrepresentation of certain areas of interest.

**Assessment/Objectives**

- While it is too soon to comment on the results of the various projects, the output indicators are more focused on research factors than in addressing the various problems and challenges that these projects would need to address. Also, the size of the individual projects is considered too small to make enough of an impact.
- The objectives of the program are currently targeted at developing awareness and research excellence. This prevents big push research as it is not specifically targeted to reaching objectives with bigger societal challenges. It is not unimaginable that cybersecurity research could contribute to these as well.
- Interdisciplinary research is partially hindered by the lack of publishing vehicles. A special multidisciplinary cybersecurity research program could stimulate publication of interdisciplinary studies. Worthwhile mentioning here is the initiative taken a few years ago to start “Crime Science” an international, interdisciplinary, peer-reviewed journal, with an applied focus. This Journal has a broader scope than cybersecurity, but might serve as an example to the cybersecurity community.

Overall, this analysis has been performed on a statistically low number of projects (23 projects, and 9 different research themes). An extension of the analysis which includes non-NWO funded projects as well as the results of future calls is recommended.

## Appendix I: Abstracts of Ongoing Research Projects in NOW's Cybersecurity Program

### Abstracts of 23 NWO-funded cybersecurity long term research projects

Refer to the IIP-VV website, i.e. https://www.iipvv.nl/nl/content/programs

## Appendix II: Original NWO Calltext for Round 1 and 2

1. Call for Proposals Cyber Security Research (first tender) 2012 (ref. 12-NROI-058), NWO-EW

2. Call for Proposals Cyber Security Research (second tender) 2013-2014 (ref. 13-NROI-138), NWO-EW

Refer to the IIP-VV website:
https://www.iipvv.nl/en/content/programs
or to the proper links on the NWO cybersecurity website:
http://www.nwo.nl/onderzoek-en-resultaten/programmas/cyber+security/achtergrond

## Appendix III: List of Experts Consulted

The following people have provided input, before, during and/or after the roundtable meeting, March 3rd 2015, Utrecht

- Drs. J.P. Barthel, NWO/IIP-VV
- Prof. dr. ir. H.J. Bos, Vrije Universiteit Amsterdam
- Dr. D. Brandt, IIP-VV
- Drs. J.C.E. Brouwers, NWO/IIP-VV
- Dr. K. Clark, NCSC, Ministerie van Veiligheid & Justitie
- Prof. dr. P.A.L. Ducheine, Universiteit van Amsterdam
- Dr. J.H. Hoepman, Radboud Universiteit Nijmegen
- Drs. E. Hubers, NWO
- Dr. ir. H. Jonker, Open Universiteit
- Prof. dr. M. Junger, Universiteit Twente
- Prof. dr. E.J. Koops, Universiteit van Tilburg
- Dr. E. Kosta, Universiteit van Tilburg
- Prof. dr. ir. R.L. Lagendijk, Technische Universiteit Delft
- Prof. mr. A.R. Lodder, Vrije Universiteit Amsterdam
- H.A.M. Luiijf MSc., TNO
- Dr. ir. E. Poll, Radboud Universiteit Nijmegen
- Dr. H.J.G. de Poot, SIA
- Prof. Mr. J.E.J. Prins, Universiteit van Tilburg
- Ir. D.B.J.M. Riksen, Ediction
- Dr. R. Rijswijk van-Deij, SURFnet
- Dr. W. Segeth, STW
- Mr. H. de Vries, NCSC, Ministerie van Veiligheid & Justitie
- Drs. H. Wesseling, Berenschot

The following people were interviewed:

- Dr. ir. C.A.M. Neggers, CEO SURF
- Prof. dr. ir. E. Huizer, CTO SURFnet, Universiteit van Utrecht
- Mr. O. Kolkman, CTO, Information Society (ISOC)

## Appendix IV: Summary of the Roundtable Meeting (Dutch)

**Multidisciplinariteit in Cybersecurity Research**
**Een eerste terugkoppeling in de vorm van gebundelde uitspraken opgetekend tijdens de ronde tafel gesprekken op 3 maart 2015 te Mammoni in Utrecht.**

De huidige benadering van cybersecurity vraagstukken is nog steeds 'technology push'/aanbod gedreven. De β benadering overheerst, terwijl de γ wetenschap in een aantal projecten wordt benut om de techniek te laten landen.

Over multidisciplinaire insteek van een maatschappelijk probleem: Is *money muling* geen groter probleem dan malware? Ofwel, is de aanpak van het eerste niet tevens een effectief middel om het tweede te bestrijden?

Hoe kunnen we media/gebruikers helpen om veel beter ontwikkelingen op waarde in te schatten? Denk bijvoorbeeld aan de SONY hack. Tegenwicht bieden aan de *culture of fear*.

Benadering vanuit elkaar aanvullende disciplines. We leren collectief niet voldoende (snel) van incidenten. Internet criminelen leren sneller. Ethische aspecten verdienen zeker aandacht: *Het moet normatief worden dat je je veilig gedraagt. We need to think about basic rights in the digital world. We need to be able to feel safe in the digital world. There is an accountability issue.* Ethiek omvat ook de methodologie van het cybersecurity onderzoek zelf. In de academische opleiding moet de cyber technicus met ethische en juridische kwesties kennismaken. Betrek juristen bij de start van onderzoeksprojecten, om *legal issues* af te dekken.

We moeten af van het idee "Als we de eindgebruiker kunnen aanpassen (door training in cybersecurity) dan werkt de tooling wel!" Zo werkt het niet! De gebruikers moeten centraal staan. Producenten moeten niet zo snel mogelijk op de markt willen zijn met een product, waarbij niet is nagedacht over security.

Hoe managen en onderzoeken we dit? We moeten de risico's in kaart brengen en maatregelen nemen:

- Wat zijn de lifecycle management aspecten (social, technical en legal) van cybersecurity?
- Hoe stemmen we bovenstaande aspecten onderling beter op elkaar af ?
- Hoe rijgen we de effectieve 'saté-prikker' door verschillende disciplines heen?

We moeten begrijpen dat *there's pressure on making companies more liable. Focus is needed on 4 areas: state actions (1); fun hackers (2); large companies absorbing personal data and all problems related (3); cyber criminals (4). We need different solutions for different threats.*

Deelnemers constateren dat een strategische ambitieuze NWO programmering de onderliggende projecten meer cohesie kunnen geven. Dat zou wellicht kunnen door een 'man on the moon' achtige aanpak voor te staan. *The problem is not: things are not covered, but: too much! Focus is lacking, maybe we need "man on the moon" super ambitious projects.*

- Advies aan NWO: Zet een subsidie instrument in, waarmee je focus en coherentie kunt bereiken.

- Advies aan onderzoekers: maak relevante NWO gebiedsbesturen (naast Exacte Wetenschappen) bewust van interdisciplinair karakter van cyber *shared funding responsibility*.

*Wat moet er gebeuren om multidisciplinair onderzoek te stimuleren? V*an het begin af aan multidisciplinaire vraagstellingen in het voorstel opnemen, voorzien in verschillende AiO trajecten, *beide uitdagend*! Bijvoorbeeld "The Internet of Things"; Dit vereist in het onderzoek, management van zowel de technische als sociale, nationale en internationale aspecten.

*Over flexibiliteit in het subsidie instrumentarium:* Als er een nieuwe call komt, dan deze deels op andere wijze uitvoeren? Strategisch onderzoek en valorisatie gaan moeilijk samen. Een ander voorbeeld is het Amerikaanse DARPA programma, waar tussentijds onderzoekslijnen worden samengevoegd.

Multidisciplinariteit in cybersecurity onderzoek is geen doel op zich. Echter, daar waar een multidisciplinaire aanpak als noodzakelijk wordt gezien is de vraag of dit past in het huidige wetenschapsbedrijf: Interactie tussen aanpalende disciplines is goed, maar het blijft monodisciplinair onderzoek! Publicaties zijn het grote probleem. Er is geen gelegenheid "buiten je discipline" te publiceren. Kan een onderzoeksvraag voor meer dan één discipline voldoende interessant zijn, zodat er ook voor tijdschriften binnen verschillende disciplines belangwekkende publicaties uit kunnen voortkomen?

Big data is ook een onderwerp waar veel in samenkomt. Maar een call op het kruispunt van security en big data levert niet automatisch multidisciplinaire projecten op, want je wordt afgerekend op het feit dat je in je eigen koker scoort en zelfs als je over die grens gaat in je huidige setting, hoe garandeer je dan dat je scoort? Ook in de volgende (academische) baan waar je op solliciteert, word je beoordeeld op juist die monodisciplinaire resultaten!

*Is the focus too much on national level? Sometimes it makes sense to have a strict focus on the Netherlands in cybersecurity research (e.g. specific judicial context).* Set up/ speed up research exchange programs and send young researchers to top-uni's abroad.

## Appendix V: References


Advisory Council on International Affairs (AIV) & Advisory Committee on Issues of Public International Law (CAVV), 'Digital Warfare', 2011

NCSRA I (2011), NCSRA II (2013), https://www.iipvv.nl/en/content/programs (ref. 10i-NROI-240, 13i-NROI-029)

National Cyber Security Strategy 2.0 2013, NCTV, V&J

Corien Prins, Nederlands Juristenblad, Geheime handel in digitale lekken, May 2014

Input roundtable discussion by Prof. Mr. Corien Prins: "Zitten er gaten in de huidige NCSRA als het gaat om het alfa, bèta, gamma spectrum? Zitten er gaten in de huidige projecten portfolio?" (ref. 15i-NROI041a)

Internet Society. Internet Invariants: What Really Matters. Internet Society. Geneva. Feb. 2012

H.A.M. Luiijf, Setting the Scene: The Need for Cybersecurity 2.0, 2014? (ref. 15i-NROI-012)

HCSS. Assessing Cyber Security, A Meta-Analysis of Threats, Trends, and Responses to Cyber Attacks, The Hague Centre for Strategic Studies. The Hague, 2015

Luiijf, Besseling, De Graaf, "Nineteen National Cyber Security Strategies", International journal of critical infrastructures 9, no 1 (2013) 3-31

Export Controls of Surveillance Technologies, Centre for Internet and Human Rights, GCCS 2015

Global Conference on Cyberspace 2015. Chair's Statement of the GCCS2015, The Hague, April 2015

Joseph S. Nye, Jr. The Regime Complex for Managing Global Cyber Activities. Global Commission on Internet Governance. May 2014. Paper Series No: 1

National Cybersecurity Centre. Cybersecurity Assessment Netherlands (CSAN 4). NCSC, The Hague. October 2014. p.8

Bruce Schneier. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company. March 2015

Louise K. Comfort, Arjen Boin, and Chris Demchak, eds., *Designing Resilience: Preparing for Extreme Events* (Pittsburgh, PA: University of Pittsburgh Press, 2010).

Fred Goldstein and John Day, Moving beyond TCP/IP, Pouzin society, 2010

Verslagen ronde tafel discussies d.d. 3 maart 2015 (ref. 15-NROI-063a, b, c)

NOTES

[1] Joseph S. Nye, "The Regime Complex for Managing Global Cyber Activities," 2014, 5–7.
[2] Internet Society, "Internet Invariants: What Really Matters," February 2012, http://www.internetsociety.org/sites/default/files/Internet%20Invariants-%20What%20Really%20Matters.pdf.
[3] GCCS2015, "Global Conference on Cyberspace 2015, Chairs Statement," April 17, 2015, https://www.gccs2015.com/sites/default/files/documents/Chairs%20Statement%20GCCS2015%20-%2017%20April.pdf.
[4] The Hague Centre for Strategic Studies (HCSS), "Assessing Cyber Security: A Meta-Analysis of Threats, Trends, and Responses to Cyber Attacks.pdf," 2015, http://www.hcss.nl/reports/download/164/2938/.
[5] National Cyber Security Centre (NCSC), "Cyber Security Assessment Netherlands 2014," October 2014, https://english.nctv.nl/Images/cybersecurityassessmentnetherlands2014_tcm92-580598.pdf?cp=92&cs=65035.
[6] Louise K. Comfort, Arjen Boin, and Chris C. Demchak, eds., *Designing Resilience: Preparing for Extreme Events* (Pittsburgh, Pa: University of Pittsburgh Press, 2010). Page 6.
[7] Joseph S. Nye, "The Regime Complex for Managing Global Cyber Activities," 2014, 5–7.
[8] Cyber warfare can be defined as 'the conduct of military operations to disrupt, mislead, modify or destroy an opponent's computer systems or networks by means of cyber capabilities." Advisory Council on International Affairs (AIV) and Advisory Committee on Issues of Public International Law (CAVV), "Cyber Warfare," December 2011, http://aiv-advies.nl/download/da5c7827-87f5-451a-a7fe-0aacb8d302c3.pdf.
[9] National Cyber Security Centre (NCSC), "Cyber Security Assessment Netherlands 2014."
[10] Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, First edition (New York, N.Y: W.W. Norton & Company, 2015).
[11] See, for example, Fred Goldstein and John Day, "Moving beyond TCP/IP," Pouzin Society, (April 2010), http://rina.tssg.org/docs/PSOC-MovingBeyondTCP.pdf.
[12] Rapport Nederlandse Rijksoverheid, "Nationale Cyber Security Strategie 2 (NCSS2)," October 28, 2013, 2, http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2013/10/28/nationale-cyber-security-strategie-2/rapport-nationale-cybersecurity-strategie-2-2.pdf.
[13] For example, It mentions that "the government, the business community and the world of academia will launch a cybersecurity innovation platform where start-ups, established companies, students and researchers can connect, inspire one another and attune research supply and demand. The PPP implementation of the second edition of the National Cybersecurity Research Agenda (NCSRA) will also contribute to this development." Ibid, p 3.
[14] Ibid., p. 26.
[15] Rapport Nederlandse Rijksoverheid, "Nationale Cyber Security Strategie 2 (NCSS2).". This "includes privacy protection, security of mobile services, data and policy management, and accountability".
[16] Which "includes malware detection and removal, intrusion detection and prevention, trustworthiness of networks and hardware, software security, security of SCADA/industrial control systems (ICS), and secure operating systems".
[17] Herbert Bos et al., "National Cyber Security Research Agenda II (NCSRA II)," 2013, 12–16.
[18] Ibid.
[19] Ibid.
[20] Based on a comparison, the latter did not provide significantly different distributions.
[21] We realize that there are several ways of classifying the various academic disciplines and that none of these are necessarily comprehensive. We have selected those areas that currently appear the most relevant and distinguishable, leaving out disciplines such as Earth and Life Sciences, and Chemical Sciences, despite the fact that these domains might become more relevant to cybersecurity in the coming years.

*The Hague* Centre for Strategic Studies

Lange Voorhout 16
2514 EE The Hague
The Netherlands

info@hcss.nl
HCSS.NL