National Cyber Security Research Agenda

— Trust and Security for our Digital Life —

Version 1.2

Editors:

dr.ir. Herbert Bos	(Vrije Universiteit Amsterdam)
prof.dr. Sandro Etalle	(Technische Universiteit Eindhoven)
dr.ir. Erik Poll	(Radboud Universiteit Nijmegen)

Contents

About this document

This document is the result of a series of discussions about the best shape, form and content of a national research agenda in line with the National Cyber Security Strategy (NCSS). It formulates, in concrete terms, common thoughts and promising directions for a research agenda in cyber security. While all contributors firmly believe that a realisation of the agenda requires ambitious funding, as well as solid governance and embedding, this document addresses only the research directions.

Acknowledgments This document has been edited under the coordination of the *ICT Innovatie Platform Veilig Verbonden*, with a broad involvement of researchers from various disciplines (computer science, law, public administration, cyber crime sciences and police studies) and from several universities and research centres (RU Nijmegen, VU Amsterdam, TU Eindhoven, University of Twente, TU Delft, Tilburg University, TNO, Novay). Discussions have extensively involved experts from the industry as well as from (semi-)government organizations.

1 A National Research Agenda for Cyber Security

As our reliance on the ICT infrastructure increases, so do concerns about its security. The growing complexity of ICT systems means that bugs and vulnerabilities are harder to avoid, creating new opportunities for increasingly sophisticated attackers.

The recent attack on a uranium enrichment facility in Iran by the Stuxnet worm shows that strategic interests can attract cyber-attackers[1]. Unfortunately, the Netherlands is an important player in the world of cyber crime. As the country with the highest broadband penetration and the best quality broadband in the world, the Netherlands is a prime target for botnets. As we cannot afford to let cyber criminals erode the trust we and others have – and need to have – in the ICT infrastructure, or at least in the services provided through this infrastructure, research is needed. *Trust* is a *conditio sine qua non* for normal economic transactions and inter-human communication. It is at the core of social order and economic prosperity, and in an increasingly ICT-dependent world, the security of ICT plays an ever more important role here.

Figure 1: President Ahmadinejad of Iran visits the uranium enrichment facility in Natanz. The plant was targeted by the Stuxnet worm (see page 14)

There are several reasons to set up a National Research Agenda for Cyber Security:

- Security in our ICT-dependent world is crucial, both to protect Dutch society from cyber-attacks, and to provide the confidence and trust in ICT that is necessary for its use.
- Investing in security expertise provides strategically essential knowledge for decision makers to act wisely in complex cases such as electronic passports and online IDs, e-health, cyber-crime, cyber warfare, smart electricity grids, public transport, smart cars and roads, critical infrastructure, etc.
- Services and products that provide improved ICT security open concrete economic opportunities that can be reaped by stimulating security research (Ernst&Young, 2011).

This document proposes an ambitious National Cyber Security Research Agenda (NCSR) to boost ICT security expertise in the Netherlands through research at universities and knowledge centers, government agencies and companies active in ICT security, and to foster partnerships between these domains. The NCSR Agenda positions itself alongside the NCSS and complementary activities focused on more short-term and operational goals, such as the establishment of legal and law-enforcement frameworks to deal with cyber crime, response teams to handle cyber security incidents, threat analyses and protection of existing ICT infrastructure, awareness campaigns, etc.

[1] See the Stuxnet sidebar in Section 4.2.

2 Focus and objectives

The NCSR Agenda concentrates on two areas:

Security and Trust of Citizens This includes privacy protection, security of mobile services, data and policy management, and accountability.

Security and Trustworthiness of Infrastructure This 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.

This fits well with the National Cyber Security Strategy (NCSS), and also with the recent 'Digitale Agenda.nl' Ministerie EL&I (2011), that has 'Digital security and trust' as one of its action lines. Moreover, it is in line with the recommendations of the EU advisory board on Research & Innovation on Security, Privacy, and Trustworthiness in the Information Society (RISEPTIS, 2008).

The **objectives** of the NCSR Agenda are to

- Improve the security and trustworthiness of the ICT infrastructure.
- Prepare the Netherlands for the security challenges of the next 6-12 years.
- Stimulate the Dutch security economy.
- Strengthen and broaden Dutch security research by fostering cooperation.

There is a potential for tremendous benefits by bringing together the different sectors and stakeholders: government, industry, knowledge centers, interest groups and universities. Stimulating research will also have a big impact on higher education and help in training the next generations of security experts, incl. PhD students trained as part of research projects, and many more Bachelor and Master students that come into contact with the field. More fundamentally, highly visible research projects and groups help to attract students to the area.

A useful role model for the NCSR Agenda is the Sentinels research program, that was launched in 2004 and is now in its final stages. Sentinels has proven to be an important catalyst in creating a vigorous ICT security community in the Netherlands. This community spans the private and public sectors and links researchers at universities, knowledge centres, companies and government agencies. Through the academic partners involved it has also provided a boost in education in ICT security. (More information about Sentinels in Appendix C) . Where Sentinels was largely technical in focus, for the NCSR Agenda to be a success it will also include the wider community of alpha and gamma researchers needed to address the challenges of cyber security, as discussed below.

Figure 2: Wikileaks routinely demonstrates the consequences of information leakage.

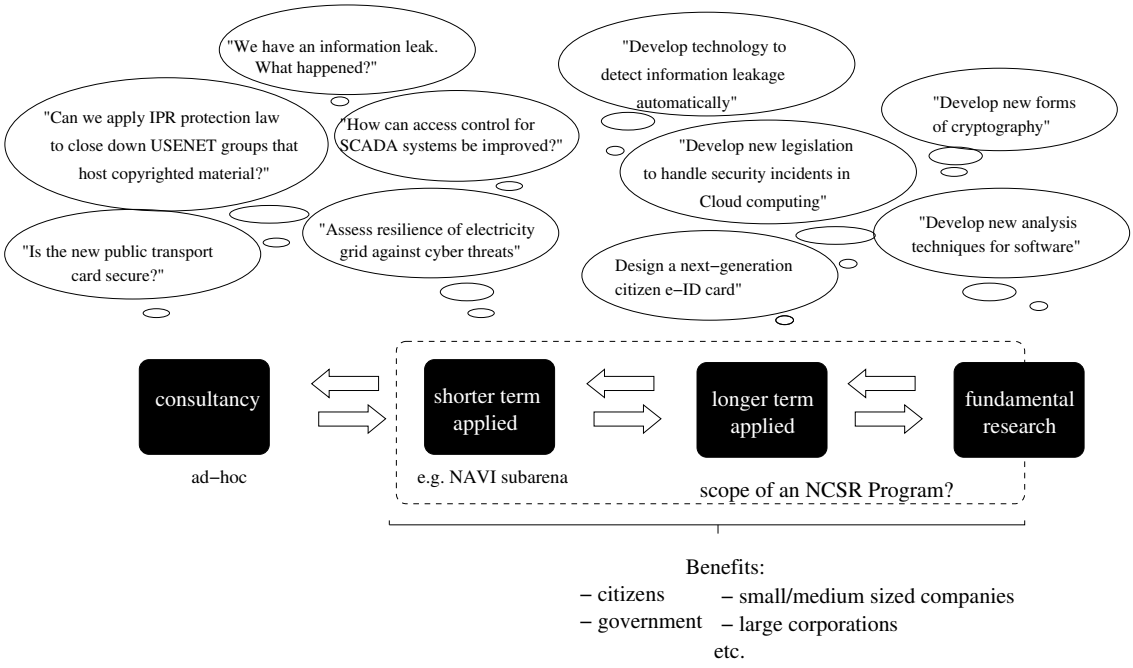

Figure 3: The spectrum of ICT security research problems – with examples

Take home message:
The NCSR Agenda sets the strategic research agenda for cyber security research and education in the Netherlands, involving stakeholders from several fields and several organisations. The NCSR Agenda endeavours to improve cyber security through research, leading to the creation of new, high-quality jobs.

The NCSR Agenda *focuses* on the following research topics:

1. identity, privacy and trust
2. malware
3. forensics
4. data & policy management
5. cybercrime/underground economy
6. risk managing, economics, legislation
7. secure design & engineering

3 The many aspects of cyber security

Cyber security issues are no longer limited to traditional computer systems, such as PCs and laptops. Rather, they surface everywhere, from electricity and water supply systems to the health service, from public transport to smart cars, from implants to supply chains, and from banking and logistics to the emergency services.

Addressing cyber security involves many domains of expertise, or *disciplines*. We do not just need technical expertise to detect and stop attacks – or better still, prevent them. We also need laws and regulations that better fit computer crime, and we need to better understand the forms and causes of cyber crime, the effectiveness of measures, including law enforcement, the underground economy, and see where economic drivers for implementing security measures are lacking and regulation may be needed.

In the disciplines involved in cyber security, we can make a rough distinction between:

- technical aspects: the β disciplines of computer science and engineering, and neighbouring areas of mathematics (notably cryptology) and electrical engineering.
- human (or non-technical) aspects: the α and γ disciplines of law, criminology, (business) economics, (information) management, applied ethics, psychology and sociology.

These disciplines involve very different communities, with radically different backgrounds and traditions. The NCSR Agenda will stimulate collaboration between them: combining insights from different fields will be crucial for addressing some of the challenges in cyber security. For example, law enforcement will require a combination of technological, criminological, and legal aspects, while some technical security measures, e.g. Deep Packet Inspection, raise important ethical and legal questions. The NCSR Agenda provides a real opportunity where the Netherlands can show the way forward by establishing serious collaboration between these communities.

The dimensions of the NCSR Agenda
The NCSR Agenda covers the central research challenges in cyber security across its many dimensions:

- the different **disciplines**: the β disciplines of computer science and engineering, and neighbouring areas such as cryptology, and the α and γ disciplines such as law, criminology, (business) economics and (information) management.
- the different **application domains**, such as critical infrastructures, internet and telecom, finance, e-government.
- the different **stages**: prevention, detection, analysis, response+recovery, governance.
- the different **layers**: the basic infrastructure of networks, hardware, and software (e.g. for internet, cloud computing, or pervasive systems); the applications, services, and service providers; the content, content providers, and users.

The research will involve and benefit the entire field: industry, knowledge centers, and the various levels of government. Similarly, research will comprise both visionary, long-term aspects of cyber security (how do we prepare for the security issues in 2020 and beyond?), and more immediate goals (how do we deal with a future Stuxnet-like attack on a power plant in the Netherlands, and guarantee sufficient resilience?).

Short vs long term research

Cyber security research spans a broad range from short-term to long-term, applied to fundamental, and focused to broad, as illustrated in Fig 3. At one end of the spectrum are short-term consultancy-type projects, e.g., to evaluate security concerns or proposed solutions. Because of their urgent and ad-hoc nature, these do not easily lend themselves to synchronisation in a broader research program. At the other end of the spectrum is fundamental scientific research, carried out at universities. Longer term research, both applied and fundamental, often involves training of PhD students.

Intermediate forms are carried out internally inside many companies and organisations, but also occur as separate projects across organisations, for example projects funded for the NAVI Sub-arena, which focuses on vital ICT infrastructure, and the EZ/STW/NWO/ICTRegie 'Sentinels' program, which has a broader scope of pre-competitive security research in public-private partnership between industry and knowledge centres.

Although different types of organisations may typically be involved in more short-term or long-term research, these do not form separate and isolated communities. This is important for sharing

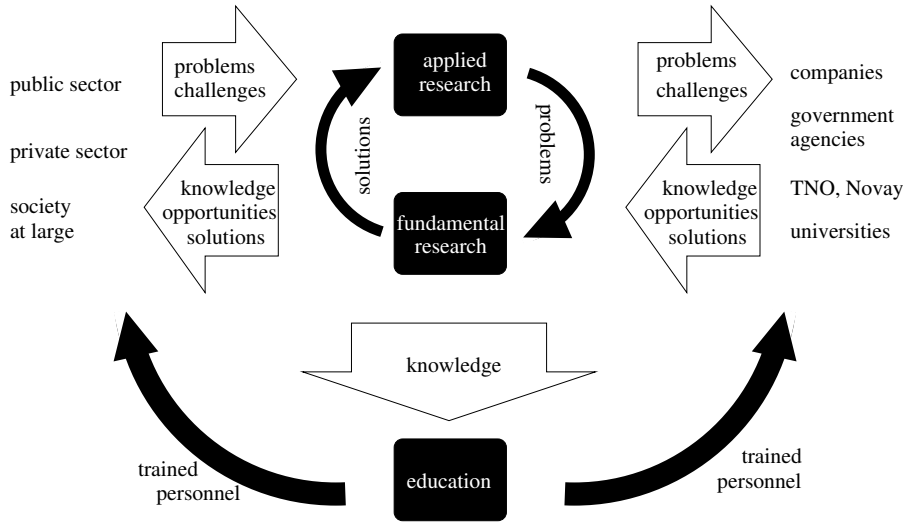

Figure 4: ICT security research

knowledge and expertise, but also for sharing challenges and problems – a practical immediate problem may pose an interesting scientific challenge and inspire and stimulate more fundamental research – and to see to it that the right knowledge is delivered in education, as illustrated in Fig. 4.

Security successes and failures in the (semi)-public sector.

Some of the big security initiatives in the public sector show how things can go right or wrong.

The ov-chipkaart was introduced without any cooperation with the academic community, resulting in some very unfortunate choices. The sector has learned from this and now keeps in close contact with the wider community via the e-ticketing forum.

The electricy sector has learned from this and has been cooperating with academics from an early stage in the introduction of smart electricity meters. As a consequence, the Netherlands is now regarded as a 'thought leader' in Europe on issues of security and privacy for smart electricity meters.

4 Setting the research agenda

This research agenda identifies the generic research themes and application areas that are crucially important to the Netherlands as a knowledge economy. The agenda describes the Dutch research scene in the area of cyber security, sets out the research subprograms which can give the Netherlands the edge and outlines options for attaining valorisation by setting up channels of communication between knowledge institutes and companies. The agenda can be translated into actual research proposals in close consultation between the knowledge institutes, the universities, the industry concerned, the government and social institutions.

In the remainder of this document, we flesh out the research themes and application areas in more detail–see Figure 5 for a high-level overview.

4.1 Contexts

Concrete research questions typically arise in a specific context, which may involve a certain technology (e.g. cloud computing), a particular application domain (e.g. finance), or combination

of the two. Still, similar research questions arise across different context, representing broader research topics. Below we make an inventory of the most important contexts, both regarding technology and application domain. The next section then lists the underlying research topics that represent the central challenges for security across these contexts.

Technologies

A central technology that is at the heart of most applications is of course Internet, fixed or mobile. **Telecommunications and the Internet** are merging more and more to become an all-IP environment, where traditional telephony (voice), television (video) and data exchange are integrated into a multi-channel system. Services can be provided to large groups of users (broadcasting and information sharing), specific groups (narrowcasting and user communities) as well as single users. As many critical applications have come to rely on Internet, the Internet itself has become an ever more critical infrastructure.

An important technology that builds on top of this is **cloud computing**. Cloud computing uses the communication infrastructure provided by internet to provide on-demand computation resources, in the form of raw computing power or more specialised services, by offering infrastructure, platforms or software 'as a service'. Cloud computing is increasingly used by individual citizens and companies to outsource their ICT needs. Cloud computing may offer economic benefits, by exploiting economies of scale and releasing users from maintenance tasks. However, cloud computing also introduces extra (communication) costs, and raises serious challenges for security.

Another important technological trend is **pervasive systems**: we are rapidly moving away from the desktop-model, and increasingly interact with ICT technology that is integrated into everyday objects and activities, that make up the *Internet of things*. Some of these devices are fully connected to the wider Internet, but many are not (e.g., wearable computing, or smart insulin pumps). In some respects, cloud computing and pervasive systems are polar opposites: cloud computing relies on massive centralisation of data and processing power, whereas pervasive systems rely on a massive distribution of processing power. As we are surrounded by ever more devices with embedded electronics, the digital and physical worlds are rapidly converging to form one cyber-physical reality – in our homes, our workplaces, in semi-public places such as care homes and hospitals, in public spaces such as the (public) transport systems, and ultimately at a global level. Pervasive systems have important implications for privacy, security, trust and have a deep impact in our social lives. Also, some of the devices, for instance RFID tags, have only very limited capabilities when it comes to information storage, processing and communication, so that traditional methods for providing security are not feasible.

Application areas

ICT technologies are used for many applications, ranging from generic use of ICT in the office or at home, to more specific applications in industry, each with their own security requirements and threats. Below we highlight some of these application areas.

- **Domestic**. ICT and ICT networks play an increasingly important role in people's private lives, as the way to communicate and socialize (e.g. through social network), as source of information and entertainment (e.g. with gaming, and internet taking over the role of television). This clearly has important security and privacy implications. Also, huge ICT infrastructure collectively provided by the Dutch citizens, with its excellent broadband connections, in itself has proved to be an interesting target for botnets.

- **Commercial**. Nearly all companies also make use of ICT and internet on a daily basis, and rely on its security just as the private individuals do Trust in ICT and internet is vital for its ongoing and increasing use, and for companies to reap the economic benefits that this brings.

Online commerce is increasingly important, and lack of trust in ICT and internet could undermine its growth: Ernst&Young (2011) estimates that increased trust in internet by consumers could provide an additional 1.4 billion euro of online trade by 2014.

Just as private individuals are concerned with privacy, companies are concerned with their intellectual property and confidential information. Companies are faced with a rapid rise of ever more sophisticated cyber attacks aim at corporate espionage.

- **Industrial Control Systems**. SCADA (Supervisory Control and Data Acquisition) systems monitor and control large industrial systems, such as chemical and nuclear plants, and large parts of the national critical infrastructure, such as the water, gas and electricity supply. Disruptions in SCADA systems can have disastrous consequences, but their increasing reliance on ICT – including internet – has made them vulnerable to remote attacks. Stuxnet is the most famous one among numerous examples here. This is especially worrying as these systems are attractive targets for hacktivism, cyber terrorism, and cyber war.

  Improving the resilience of the ICT-dependent critical infrastructure requires research on these infrastructures as they exist today, to understand their interdependencies and judge their reliability in the face of attacks, and research on more secure components (hardware, software, or communication protocols) that may be needed to build a secure infrastructure.

- **Smart grid**. A new piece of technical critical infrastructure very much under development today is the smart grid, the next-generation electricity and utilities network that uses ICT technology to provide two-way digital communications between suppliers and appliances at consumers' homes, including smart meters and in the near future also batteries in electric cars. Smart grids are being promoted as a way of addressing energy independence, global warming and emergency resilience issues, but the increased reliance on ICT also introduces new threats, both for the security of the overall network an privacy of individual users.

- **Finance**. Financial institutions or their customers are increasingly often victim of targeted cyberattacks, carried out by well-funded criminal organisations, that are becoming ever more sophisticated. These attacks are costing millions to consumers, retailer, and financial institutions (e.g. through skimming, stolen credit-card numbers, DoS attacks on payment infrastructure) and undermine the trust that is crucial for the financial system.

  Present security solutions (firewalls, intrusion detection systems) cannot cope with this level of sophistication. There is a clear need for new defensive approach that can deal with targeted attacks and exploits of zero-day vulnerabilities. Identity fraud is also a major issue here. New payment schemes (e.g. using NFC mobile phones) may offer new technical and commercial possibilities, but also raise new security and privacy concerns.

- **Transport & Logistics**. Cars and transportation systems are increasingly making use of sophisticated software to carry out safety-critical processes such as braking in cars. Drive-by-wire is already a reality, and in the near future intelligent transportation systems will make use of large-scale communication to optimise fuel consumption, reduce traffic jams, increase safety and implement smart tax charges, also brings high security risks; e.g. it has been demonstrated that malware in a car may turn off the braking system. Moreover, the communication means that are needed to implement the smart mobility paradigm will turn the car in an open system which is by definition open to cyber-attacks.

  In logistic, the main challenge in the domain is to ensure business continuity while making the value chains as short and responsive as possible. A shorter chain has fewer participants and thus lower cost. A responsive chain delivers goods and payments faster, again lowering costs. However in a shorter chain the risks of interruption of the logistics and transport services will increase and thus business continuity risks will increase.

- **e-Health**. Processes in the health sector are increasingly being supported by ICT. ICT is also the key enabler of new methods of providing care, as exemplified by ambient assisted

Secure trade lanes

The Netherlands derives more than two-thirds of its GDP from merchandise and services trade[†]. With strategic hubs like Schiphol and the port of Rotterdam, and import and export valued at approximately 430 and 480 billion euro respectively, the country is strongly dependent on secure trade lanes. While physical protection is a first step, cyber security plays an increasingly important role.

Research in security in logistics and the international supply chain aims to enhance trust between trading partners and government. Doing so requires cooperation between all kinds of business and governmental partners to work together and share data, and requires both technical and non-technical viewpoints.

For example, criminologists, sociologists, and psychologists are needed to understand the threats to secure international trade. The objects of study include problem posed by criminal organisations and their motives and means for attacking data records related to international transport (e.g., to enable smuggle), but also tax evasion by means of data manipulation in (electronic) transport-related documents. We need economists to calculate the risks involved in terms of money, based on estimations of probabilities and impacts, and policy makers, management experts and institutional economists, to provide organisational measures, the legislation and decision-making, as well as to organise supervision structures.

[†]US State Department Background Note: The Netherlands, `http://www.state.gov/r/pa/ei/bgn/3204.htm`

living. However, patient data is often spread across many care providers, such as the general practitioner, dentist, specialist, physiotherapist, hospital, pharmacy and, of course, the patient. Care providers must be able to access relevant information that is created and maintained by colleagues (such as medication records), must be able to take action in case of emergencies and still guarantee the privacy of the patient's data. The security of patient data is essential to ensure that doctors obtain the correct information at the right time. The retention period for patient data is long (up to 70 years) and this poses a significant challenge for the technical infrastructure that supports the healthcare system.

- **e-Government**. The government plays different roles as far as cyber security is concerned. On the one hand, the government is a major user of ICT technology, with the increasing use of online information and services to citizens. Here the government is an important role model, and its conduct sets a standard. Also, ICT technology may provide new ways to promote democracy, e.g. through e-voting and local referenda.

  On the other hand, the government is responsible for the security and the protection of privacy for citizens, not only through legislation and law enforcement, but also through promoting awareness, by providing knowledge and expertise (e.g. via GOVCERT.NL), and stimulating (inter)national collaboration. Just as governments already provide identities and means of identification for use in the physical world, they will increasingly do so in the online world, which may be crucial in combatting identity theft as ever more services go online. Indeed, the introduction of an national electronic ID, the eNIK, is stated as one of the objectives in the NCSS. Finally, cyber espionage is a growing concern for government.

- **Military/defense**. In 2010, Cyberwarfare became frontpage news, as well as a conspicuous reality with the Stuxnet attack on Iran (see page 14). Cyber security is crucial to the military and the Department of Defense both in terms of defensive/reactive capabilities, and in pro-active capabilities. Cyber defense is strongly related to resilience of the various critical

Figure 5: Application domains and research topics

infrastructures already mentioned above (Clarke and Knake, 2010). Additionally, forensics and attribution are fertile grounds for research involving many disciplines. However, in most advanced countries interest in a pro-active strike force is growing and more research and study is needed in this area.

4.2 Research Topics

Within the application domains listed above, the research agenda covers research topics in activities that range from the secure design of new systems, to coping with the aftermath of attacks on existing systems. Again, each topic requires contributions from multiple disciplines: technical, legal, economical, etc. To structure the discussion on a potentially infinite list of research topics, NCSR Agenda distinguishes the following research topics:

1. **Identity, Privacy and Trust Management**

   Managing the (digital) identities, protecting user's privacy and managing the trust in the online world are essential functionalities of the *future internet*[2], which are required in each of the application areas listed above. The application areas concern important but distinct aspects of the digital life of the citizen. In each of these, different authorities, and different numbers of authorities – sometimes one (e.g. the government), sometimes many, sometimes none – will be responsible for providing and controlling identities, and different authentication mechanism will be used. Therefore, different identity management solutions are needed to cater for the various needs. Research sub-areas include the computer science and crypto techniques to ensure privacy and to handle identities securely, organisational rules and guidelines to delegate trust, and rules and legislation to deal with identity theft, privacy and anonymity rights, as well as private data retention and corresponding access rights.

[2]See Future Internet Assembly: http://www.future-internet.eu/

2. **Malware**

   Malware, short for malicious software, denotes all forms of hostile, intrusive, or annoying software or program code. The ability to run malware is essential for many types of attack, serving as a *conditio sine qua non* for generating social and economic power for the attackers.

   Thus, the threat of malware will remain critical for the foreseeable future. Currently, we experience the threat of malware most saliently in the form of botnets – millions of infected machines tied together in networks at the disposal of attackers. But malware evolves with the ICT infrastructure. We are already seeing malware on social networks, in cloud computing and on mobile devices.

   In terms of research, it poses an interdisciplinary challenge. We need advances in technology, as well as arrangements to shape the socio-economic forces that fuel or mitigate the spread and impact of malware. Unless these issues are researched jointly, we will be stuck with partial solutions of limited value.

   Technological advances include attack detection and prevention, incident recovery, reverse engineering, and attack analysis. For instance, to detect and prevent attacks, we need techniques and tools to spot and remove vulnerabilities from software, and monitoring systems to raise an alarm when a program behaves in an anomalous manner.

   Analysis of malware requires reverse engineering techniques to help us understand what it is doing, as well as methods to estimate the number of infected machines and the effectiveness of counter-measures. From an historical perspective, we should study trends in malware–as doing so prepares us for new threats in time.

   While originating in criminal behaviour, the magnitude and impact of the malware threat are also influenced by the decisions and behaviour of legitimate market players such as Internet Service Providers (ISPs), software vendors, e-commerce companies, hardware manufacturers, registrars and, last but not least, end users. Here, critical questions focus on economic incentives for the variety of market players. These can be shaped by self-regulation, state regulation and liability assignment. At the organizational level, we need policies to govern the management of hardware and software (including purchase, configuration, updates, audits, decommissioning), and guidelines regarding the management of information.

   In addition, we often lack understanding about the socio-cultural context of the malware. Why is it doing what it is doing? The threat posed by Anonymous (the loose group of netizens and hackers that attacked companies that interfered with WikiLeaks) is very different from that of criminal organisations herding massive botnets, and that of state-sponsored cyber espionage and warfare. Studying the origin of attacks and the nature of the victims, as well as the language and socio-cultural references in malware help linguists and sociologists to profile the attackers.

3. **Forensics**

   The goal of cyber forensics is to examine digital media in a sound manner to identify, preserve, recover, analyse and present facts and opinions about the information. Forensics, and, more generically, Computer Security Incident Response (CSIR), is an important part of cyber security. It operates on the corrective or repressive side of security, i.e. it comes into play after a security breach has occurred and attempts either to correct the problem as quickly as possible, or to find evidence to be able to identify and prosecute the culprit.

   The first decision after an incident is an economic one. How essential is the compromised system? For example, in a critical infrastructure setting such as a power station, it may be more important to get things up and running (without running the risk of a repeat) than to gather forensic evidence. If, however, the decision is made to consider the compromised system a crime scene, highly skilled digital forensics expertise is needed on-site as quickly as possible to collect evidence, in a way that provides evidence that is admissible in a court of law. This process requires deeply technical as well as legal knowledge. Legal expertise about

digital forensic evidence is also very important in getting more visible cases where cyber criminals are successfully prosecuted. Live forensics (forensics on a system that cannot be switched out, as in critical systems) and the attribution question (linking the criminal activity to the criminals behind it) are examples of issues that urgently require additional research. Forensic evidence has been used in a number of high profile cases and is becoming widely accepted as reliable within US and European court systems. However, this may be hampered by a lack of official standards for digital forensic evidence, especially with multiple parties providing digital forensic evidence.

4. **Data and Policy Management**

   In the application areas a variety of data plays a key role. However, the confidentiality, availability, authenticity and integrity requirements for different kinds of data can vary greatly, both in the technical as well as in the legal sense. For example, health records must be kept for 70 years, and therefore require strong security, whereas other data is almost ephemeral, such as the data kept by RFID tags. In this area, we need computer science research to develop data management techniques, but also organisational procedures, to ensure correct handling of sensitive data, and research to make sure that technical policies match with the user's mental models and understanding.

5. **Cybercrime and the underground economy**

   There is organised cyber crime, such as skimming, botnets, provision of child pornography and advance fee fraud, and unorganised (common) cyber crime, such as simple frauds, downloading child pornography, uttering threats, etc. In both cases we need to understand the (explaining) factors that lie behind the crimes, the modus operandi and the criminal careers of cyber criminals, and, in the case of organized crime, how their organisations work. We need to know more about patterns in cybercrime, who the victims are and how victimisation can be explained. Since money (and as a result of that goods and information with a monetary value) is a key factor in many crimes, it is important to better understand the underground economy, its size, its characteristics and how it is intertwined with the legal economic system. Also we need to know more about the effectiveness of measures against cyber crime and the cooperation between (private and governmental; national and international) parties against cybercrime. What works and why? Do law enforcement agencies use their special powers for crime fighting in a digital world and, if so, with what result? The aim of research into the cybercrime area, is to design crime prevention strategies and measures to effectively disturb/block criminal activities.

6. **Risk Management, Economics, and Regulation**

   Risk management aims to assess the economic value of security, to provide a rational basis for allocating resources to improve security after identifying and assessing risks – and to determine if we are doing enough, or too much, and if we are spending resources on the right things. One central problem here is that concrete data is often lacking, and more research could provide a more solid basis.

   A much more fundamental problem is that risk assessment is typically done by an individual party, one of the many parties that collectively provide a complex value chain. For an individual party in such complex value chain there may not be any economics incentives to fix a problem. Indeed, in cyber security there are many *externalities*: costs that borne by other parties and hence not incorporated in price. For example, someone whose home PC is part of a botnet might not notice any adverse effects, and hence not be motivated to go through all the hassle of cleaning it. Perverse incentives may be a more important cause of security problems rather than the lack of a suitable technical protection mechanisms. A better understanding of the economics of security – and the economic (dis)incentives that occur – is needed for more structural solutions of security problems.

   Understanding economic drivers – and where these fail – is also crucial to determine where regulation is needed, and more generally what the government's role should be in cyber

security. Different regulatory frameworks may apply in the various application domains, and at different levels: national, EU, and international.

7. **Secure Design, Tooling, 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. ICT systems in use today are typically not designed and built with security in mind. As a result, security is often dealt with retrospectively, only after security problems arise. Security problems then have to be solved by an add-on in the design, when bad initial design decisions can no longer be reversed. When it comes to the software, fixing the problems requires costly bug fixes to patch implementations.

   Ideally, systems should be designed with security and privacy in mind from the start – ensuring **Security by Design** or **Privacy by Design**. They should then be implemented and tested using good engineering principles and analysis techniques to avoid security problems or detect them at an early stage. While considerable progress has been made in some niche areas, such as security protocol analysis, sound engineering methods for security are still a long way off, especially when it comes to providing secure software.

   Besides software engineering, the field of economics plays an important role in this area. The cost of a secure design may be initially higher and requires a trade-off between risks and expenses. In addition, the cost over time for a secure design is likely to be quite different from that of less secure systems.

Even if initially aimed at one specific application domain, research on the topics above can provide generic solutions that will apply to many application domains. For this to happen it is important that NCSR Agenda helps to disseminate of knowledge and project results across these application domains.

Cyber warfare: or how a digital bomb targetted Iran's nuclear programme

Up until the summer of 2010, the threat of *cyber warfare* was not considered too serious – a threat that would perhaps emerge in the future, but not just yet. Sure, some used the term to refer to the Russian cyber assaults on Estonia in 2007 and on Georgia in 2009, but experts agreed that it was a misnomer in both cases. While the incidents were serious, they were hardly the result of a serious, advanced, state-sponsored attack. More like a large number of disgruntled citizens participating in low-tech assaults.

Stuxnet All this changed in June 2010, when a security firm in Belarus discovered a highly sophisticated worm that infects and reprograms industrial systems. The worm, popularly known as *Stuxnet*, is dubbed the most sophisticated virus ever written. It is not just any old virus: it targets very specific sites – a uranium enrichment facilities in Iran. According to news reports the worm might have damaged Iran's nuclear facilities in Natanz and eventually delayed the start up of Iran's Bushehr Nuclear Power Plant. Most experts agree that Stuxnet is a cyber weapon probably created by a technologically advanced nation state. For instance, Kaspersky Labs concluded that it could only have been created "with nation-state support", making Iran the first target of real cyber warfare.

The attack is incredibly sophisticated. Initial infection occurs via USB sticks. This may not sound terribly sophisticated, but it is a very clever idea, since it also allows attackers to 'cross the air gap': to infect machines that are protected by firewalls, and even those not connected to the Internet at all. Next, it spreads to other Windows machines on the same network as the initial victim.

Why is Stuxnet so frightening? Well, the first thing that is unusual about this attack is the number of completely new, unknown attack vectors (so-called 'zero-day Windows exploits') employed by Stuxnet. Such exploits are highly valued by attackers and it is rare to see them waste more than one zero-day exploit in a single attack. Stuxnet has four.

Second, it loads (driver) software into the very heart of the victim systems. The Windows operating systems is actually fairly careful about loading software in its most privileged levels – the only way to do so without raising suspicion is by making sure the code is signed by a trusted vendor. The digital certificates used for this purposes are typically well-guarded secrets, but Stuxnet uses two compromised digital certificates to do so.

Finally, the attack spreads and looks for specific machines that control industrial systems. Industrial control systems consist of Programmable Logic Controllers (PLCs), which can be thought of as minicomputers that can be programmed from a Windows system. These PLCs contain special code that controls critical processes like the machinery in a plant or a factory. Again, even if these systems are not on the network, Stuxnet may well reach them using the USB flash drives. Incredibly, Stuxnet not only reprograms the PLCs, but also uses rootkit tricks to hide the changes. In the words of Jarrad Shearer of Symantec: "Stuxnet isn't just a rootkit that hides itself on Windows, but is the first publicly known rootkit that is able to hide injected code located on a PLC."

Stuxnet is a high-tech weapon, delivered by no fewer than seven different ways to propagate, four zero days, one known exploit, three rootkits, two stolen certificates, and two Siemens security issues. It has but one target: Iran's uranium enrichment facility. The modified PLC code causes the facility's centrifuges to spin at damaging frequencies. This brings up another interesting issue. To pull this off, the makers must have had detailed knowledge of the target systems – a complex and costly affair.

Lessons to learn Despite its size (1.5Mb), it took many months to detect the Stuxnet attack, and despite a huge international effort, it took another few months to analyze it. Stuxnet changed the threat landscape–until last year, attacks on PLCs were considered science fiction. Like Iran, the Netherlands today would not be ready for such 'threats of tomorrow'–the expertise is simply lacking. Longer term vision and development of such expertise requires research and education. More than anything, Stuxnet has taught us that cyber warfare is real *now*.

References

Cho, A. (2008). University hackers test the right to expose security concerns. *Science*, 322(5906):p.1322–1323.

Clarke, R. A. and Knake, R. (2010). *Cyber War: The Next Threat to National Security and What to Do About It*. HarperCollins.

Ernst&Young (2011). Groeien door veiligheid – onderzoek naar de waarde van een veilige en betrouwbare ict infrastructuur voor de nederlandse economie. Report for Ministerie van Economische Zaken, Landbouw & Innovatie.

Grossman, W. M. (2007). Jam session - an design to block RFID tags. *Scientific American*, page 2.

Ministerie EL&I (2011). Digitale Agenda.nl - ICT voor innovatie en economische groei.

RISEPTIS (2008). Trust in the information society. EU RISEPTIS (Research & Innovation on Security, Privacy and Trustworthiness in the Information Society).

Appendix A. The cyber security research community in the Netherlands

Below we present an inventory of the main actors in security research in the Netherlands, in industry, at university and knowledge centres, and government agencies. Thanks to the stimulus of the Sentinels research program, there is a good level of cooperation between industry, universities, and knowledge centres, notably through the IIP Veilig Verbonden.

Universities

Security research at universities in the Netherlands mainly takes place at the universities listed below, listed below in alphabetical order. For completeness we also include relevant lectorates in Higher Vocational Education institutes (HBO), where the focus is more on training than research.

- **Centrum for Wiskunde en Informatica, CWI (Cramer)**

  The Cryptology and Information Security group at CWI headed by prof. Cramer carries out research in cryptography, cryptanalysis, and applications to information security. This includes research on public key infrastructures, secure computation, post-quantum security, leakage-resilience, quantum cryptography, and number theory.

- **Haagse Hogeschool (Spruit)**

  Prof. Spruit (`www.marcelspruit.nl`) is lector in Information Security at the Haagse Hogeschool, which also provides a degree programme in Information Security Management.

- **Open Universiteit (Stol, van Eekelen)**

  Prof.dr. W.Ph. Stol (www.wouterstol.nl) holds the chair in Cyber Safety, which is a collaboration between NHL Hogeschool and the Dutch Police Academy, and the chair Police Studies with a focus on Cyber Safety, at the Open University. Prof. Stol and prof. van Eekelen perform multi-disciplinary cyber crime research, in particular for the digital payment infrastructure.

- **Radboud Universiteit Nijmegen, RU (Jacobs, Hoepman, Poll, Hildebrandt, van Eekelen)**

  The Digital Security founded by prof. Jacobs in 2003 has quickly grown to one of the largest in the Netherlands. The group carries out research into security protocols and applied crypto, smartcards and RFID, and software security. Research in the group ranges from very applied and practical work (e.g. into RFID systems, smart grid, and GSM) to more societal aspects of security, especially in the area of privacy, for instance through the research of prof. Hildebrandt on social, ethical and legal implications of the new ICT infrastructure. The group carries out a lot of security consultancy, also for Dutch government.

- **Technische Universiteit Delft, TUD (Brazier, van Eeten, Lagendijk, van der Lubbe, van den Berg, Tan)**

  In the Information Security & Privacy Lab of the Faculty of Electrical Engineering, Mathematics and Computer Science, the group of prof. Lagendijk carries out research into multimedia content security (fingerprinting, watermarking, secure signal processing). Research in this group led by dr. van der Lubbe focuses on cryptographic techniques for security and privacy.

  In the Faculty of Technology, Policy and Management (TPM), prof. van Eeten researches governance of infrastructures, including economic incentives and market failures regarding cyber security and prof. Brazier researches mobile agent systems. In the same faculty, the Information and Communication Technology section, led by prof. Yao-Hua Tan, carries out research on secure trade lanes and e-government. The newly established Centre for Risk

and Trust, led by dr. van Gulijk and dr. van den Berg,researches risk assessment in socio-technical systems, trust and privacy management, and intelligent data analysis for security & forensics. Here in cooperation with prof. Miller and prof. van den Hoven there is also research on applied ethics of security and privacy.

- **Technische Universiteit Eindhoven, TU/e (Tilborg, Etalle, Lange, Schoenmakers)** Security research in Eindhoven is carried out by EIPSI (Eindhoven Institute for the Protection of Systems and Information), which was formed in 2007 from the Coding and Cryptology group in Mathematics and the recently established Security group in Computer Science. Prof. van Tilborg's has a long-standing international reputation in coding and cryptology. The Security group in Computer Science headed by prof. Etalle looks at a broad range of issues, including trust and identity management and security of embedded systems.

- **Vrije Universiteit Amsterdam, VU (Tanenbaum, Bos, Crispo, Fokkink)**

  The VU has two closely collaborating security groups: one led by prof. Tanenbaum and one led by dr. Bos. The Systems and Security group headed by prof. Tanenbaum, KNAW professor and winner of an ERC Advanced Grant, carries out work on secure operating systems. His group also carries out research on Security Protocols and RFID.

  The group led by Bos works primarily on systems security, detecting and fingerprinting attacks at the lowest layers: the kernel, or even the (emulated) hardware. Their Argos honeypot system used by many organisations around the world. The current research focus lies in the protection of mobile devices, retrofitting security on legacy binaries. In 2010, dr. Bos won a European ERC Starting grant to start a new team on the topic of reverse engineering.

  Also at the VU, in the Theoretical Computer Science prof. Fokkink carries out security research into protocols and distributed algorithms.

- **Universiteit Twente, UT (Hartel, Kargl, Jonker, Veldhuis, Junger)**

  In the Computer Science Department, the Distributed and Embedded Security research group (DIES) headed by prof. Hartel carries out research into the analysis and design of secure distributed and embedded systems. The research considers at a variety of applications, ranging from smart guns, via smart surroundings to smart homes and vehicles. The Electrical Engineering department has a successful research group that focuses on biometrics (Veldhuis).

  ICT security research at Twente is intimately connected with research in other disciplines; betas and gammas work together on the prevention and detection of crime and disorder, and more specifically cyber crime (prof. Junger).

- **Universiteit van Tilburg (Prins, Koops, Leenes)**

  The Tilburg Institute for Law, Technology, and Society (TILT), part of the Faculty of Law, carries out multidisciplinary research into the legal and social implications of emerging technologies. A key feature of the research program is the interaction between legal, technological and social perspectives

  Much of the research of TILT touches on ICT, on issues such as e-government, privacy, cybercrime, and intellectual property rights. Here there are research lines on Cybercrime & Cybersecurity, which deals with the legal and social issues raised by ICT developments in criminal law, anti-terrorism, and critical infrastructures, and a research line on Privacy and Data Protection.

- **Universiteit van Amsterdam, UVA (de Laat, Hugenholtz, van Eijk)**

  In the Faculty of Science, the System and Network Engineering Science group of prof. de Laat carries out research on optical networks and generic AAA (Authentication, Authorization, Accounting) architectures for the Grid. The group is also active on research on data privacy

and security, and has for instance investigated the proposed Dutch scheme for electronic health records (EPD).

The Institute of Information Law, part of the Faculty of Law, engages in research into fundamental and topical aspects of information law, and provides a forum for critical debate about the social, cultural and political aspects of regulating information markets.

- **Universiteit van Leiden, UL (Lenstra, Zwenne, van Wilsem)**

  In the Faculty of Law, the e-Law institute carries out research into the role of the law in the information society and the institute for Criminal Law and Criminology researches ICT from a criminological point of view.

  At the Mathematical Institute, the Number Theory and Algebra headed by prof. Lenstra carries out fundamental research on cryptography.

- **Universiteit van Utrecht (Grijpink)**

  At the Institute of Information and Computer Sciences of Utrecht University, economist and lawyer prof. J. Grijpink investigates identity issues in information society.

The academic excellence of Dutch security research is demonstrated by the international recognition. Prof. Tanenbaum of the VU received an ERC Advanced Grant by European Research Council (ERC) for research into secure operating systems. As a follow-up to the Sentinels De-Worm project, dr. Bos of the VU was awarded the prestigious ERC Starting Grant in the field of computer security. Scientific American did an article on the RFID Guardian project at the VU (Grossman, 2007), and the security group at the RU was the subject of a special article in the top scientific journal Science (Cho, 2008), all the more extraordinary as top science journals rarely pay attention to computer science research. For his PhD thesis on intrusion detection in high-speed networks, Willem de Bruijn of the VU won the Eurosys Roger Needham Award for best PhD thesis in systems in Europe – Eurosys is the European Chapter of ACM SIGOPS. The VU was invited to join a high-profile EU FP7 project FORWARD [3] on identifying future security threats and needs, and setting directions for security research at a European level.

Apart from academic and economic impact, Dutch ICT security research can also lay claim to real societal impact. On several occasions Dutch security research made grabbed the international headlines, for instance with research on

- RFID viruses (e.g. 'Scientists: RFID chips can carry a virus', CNN, 15/3/2006),
- Mifare cards (e.g. 'Details of Oyster card hack to be made public', The Times, 21/7/2008),
- and electronic identity cards (e.g. 'E-passport security flaw allows remote ID of nationality (The register', 8/4/2008).

On a national level, security experts from universities have been involved in – or even sparked off - debates on topic such as the ov-chipkaart, electronic voting, electronic patient records (EPD), and the biometric passport, for instance serving as experts in Parliamentary hearing, serving on committees (e.g. the Adviescommissie inrichting verkiezingsproces), or performing security research for government agencies and ministries (e.g. on the new Rijkspas, the EPD and Digid, the RIES internet voting system, the biometric passport, smart electricity meters, electronic roadpricing, and the electronic driving license). This only underlines the fact that given the growing role of ICT in the information age – and the associated growing threats – it is crucial that the Netherlands has expertise in ICT security.

In the light of the above, it is not surprising that on three occasions the annual ICT I/O Award, awarded by IPN (ICT-onderzoek Platform Nederland) for the best achievement in bringing ICT research to the attention of the general public, went to security-related research: in 2005 to prof. Jacobs of the RU for research on electronic voting, in 2006 to dr. Rieback of the VU for the RFID Guardian project, and in 2008 to the Mifare team of the RU for their research on Mifare Classic and the OV-chipkaart.

[3] `http://www.ict-forward.eu`

Other Knowledge Centres

Apart from the universities, TNO and Novay (formerly the Telematics Institute) are important knowledge centres for ICT security research. The Netherlands also boasts two independent, PNP (private non-profit) organisations involved in ICT security research, both focussed on Internet, namely SURFNet and NLNet Labs.

- **TNO** Starting in 2011, the research at TNO is clustered in the following 7 themes
  - Healthy Living
  - Industrial Innovation
  - Integral Security & Safety
  - Energy
  - Mobility
  - Built Environment
  - Information Society

  The two themes most relevant within the context of the NCSR Agenda are Defence Safety & Security (led by drs. H.G. Geveke), and Information Society (Erik Huizer). The first covers the innovation area Secure & Safe Society, comprising e.g., Cyber Operations (warfare) R&D and the Dutch Centre for Protection of National Infrastructure (CPNI.NL) – formerly known as the NICC.

  The second covers the innovation areas Future Internet, Use Societal impact of ICT and Vital ICT Infrastructures. These four innovation areas have strong relations with the research agenda of the Sentinels II programme. They cover diverse areas such as critical infrastructure protection, risk perception and risk analysis, security & safety management, privacy enhancing technologies and identity management, intelligence provisioning, RFID and the Internet of Things, applied cryptography, smart cards and trusted computing, labelling and release mechanisms, to name but a few. TNO is a major player in FP7 IST & security areas as well as in NATO Research & Technology Organisation/Agency working groups. Power companies, KEMA, and TNO are working on Smart Grids and their security. The total number of TNO researchers involved in these topics are 50+ people. Senior scientists in these areas are, among others, prof.dr.ir. Wessel Kraaij, ir. Eric Luiijf, dr. Jaap-Henk Hoepman, dr.ir. Thijs Veugen, ir. André Smulders, and prof. Robert Kooij.

  TNO is a member of the International Security Foundation (ISF), ECP.NL and participates in the Permanent Stakeholders Group of the European Networking and Information Security Agency (ENISA).

- **Novay** Novay's research program focuses on the role that ICT plays in networked innovation. Security and trust are important aspects that make or break innovative solutions as soon as they are deployed in the real world. Novay is organized in two departments, one focusing on Human Centric Services and one on Networked Enterprises. Most of the security related work is carried out in the Identity & Trust theme within the Human Centric Services department, although multi-disciplinary experts from both departments work within high profile security and trust related projects such as GigaPort3 (on eScience collaboration) and cidSafe (on high trust consumer identity).

- **SURFNet** is a subsidiary of the SURF organisation, in which Dutch universities, universities for applied sciences and research centres collaborate nationally and internationally on innovative ICT facilities. Security is an important area of attention for SURFNet. SURFNet has its own Computer Emergency Response Team, **SURFCert**, and carries out research into network security and identity management, with the aim of providing innovative new services for its users, including payment services (SURF internetpinnen) and new ways for

identity management. In the past SURFnet pioneered an intrusion detection system for its clients based on the Argos honeypot technology, developed by the VU in the Sentinels project 'Deworm'.

- **NLNet labs**, funded by Foundation NLNet, is a research centre that focuses on new developments in internet technology, especially the next generation internet with IPv6 and the secure domain name service DNSSEC.

Government

Many different ministries and government agencies are involved with ICT security research and security projects. The government is not only an important user of ICT security, but also has an important role as provider of ICT security, in gathering and disseminating technical know-how and raising public awareness, and as regulator.

Within the Ministry of the Interior, Logius (formerly GBO.Overheid) is now the central service for ICT and the overall infrastructure for e-government. As such, it is responsible for DigID and PKIoverheid. GOVCERT.NL, the Computer Emergency Response Team for the Dutch Government, is now also part of Logius. The AIVD, in particular its unit NBV (Nationaal Bureau voor Verbindingsbeveiliging), supports the Dutch government in protecting its (digital) information. The NBV is the government agency responsible for evaluating information security products and solutions.

In 2004 the ministries of Security & Justice, the Interior, Economic Affairs, Agriculture, and Innovation (EL&I) and the National Police Services Agency KLPD have joined forces in the fight against cybercrime, by setting up a joint high-tech crime unit. The KLPD/THTC (Korps landelijke politiediensten - Team High Tech Crime), together with GOVCERT.NL and NCTb (Nationaal Coordinator Terrorismebestrijding), are responsible for the fight against cybercrime, and also internet-based terrorism. The Ministry of EL&I also supported the NICC (Nationale Infrastructuur Cyber Crime), now incorporated by TNO. The Ministry of Security & Justice incorporates the NFI (Netherlands Forensic Institute), which has digital forensics and cybersecurity as one of its areas of expertise. The NFI works on cyber security in the broad sense, looking at threats such as malware, skimming, phishing and botnets, as well as crime facilitated through cyberspace such as fraud, and develops methods, software, and hardware tools to extract and analyse digital forensics.

In the Ministry of Infrastructure and the Environment, the National Road Traffic Agency (RDW) is active in security research, e.g. surrounding initiatives for electronic driving licences.

The Ministry of Defence sponsors defence-related security research, largely carried out by TNO. The Netherlands Defence Academy (NLDA) has been investing in more security expertise, for instance with the appointment of prof. T. Grant to head the group Operational ICT and Communications.

Commercial

The Dutch industry and service sectors include many companies that are active in ICT security research. This includes large industrial companies, some smaller companies provide security expertise in technical, legal, or criminological issues, and also a growing number of SMEs and young start-ups.It is beyond this document to try to list them all. Instead, we provide a more useful overview by categorizing them in broad classes.

Large industrial companies involved in ICT security research include Philips, NXP, FOX-IT, Irdeto, and Thales. Smaller industrial companies focussed on security include CHESS and NEDAP. CHESS develops hardware and software for security-critical for instance in the payment sector and industrial control. NEDAP is amongst others a major supplier of (physical) access control systems using smartcards and RFID.

In an EU-supported initiative, Philips is a founding member of Trust in Digital Life (TDL, `http://www.trustindigitallife.eu`), a consortium that aims to set out a vision for trustwor-

thy products relating to information and communications technology (ICT), including devices, applications, services, and infrastructures. Philips alone had three successful spin-out companies that are focussed exclusively on ICT security, namely

- Civolution (`http://Civolution.com`), that works on watermarking,
- Priv-id (`http://www.priv-id.com`), that works on biometrics, and
- Intrinsic-ID (`www.intrinsic-id.com`), that works on anti-counterfeiting.

Of these, Priv-id is a spin-off resulting from the Sentinels ProBite project. Intrinsic-ID won the ICTRegie Award 2010 for the best achievement in technology transfer from academia to society.

Fox-IT is one of the larger and most prominent companies specialising in ICT security, especially in supplying solutions for governments and other organisations with high security requirements, and expertise in digital and internet forensics. Madison Ghurka is another specialist in providing services to efficiently identify, mitigate and prevent IT security risks, including penetration testing.

The Netherlands boast two internationally leading companies that carry out security evaluations, namely TNO spin-off Brightsight – which is also certified to carry out Common Criteria security evaluations – and Riscure, and one company specialising in security testing, Collis.

The major Dutch software houses Logica CMG, CapGemini, Atos Origin, and Getronics all provide security expertise and develop ICT security solutions. In the software sector there are also more specialised firms that focus on ICT security, such as AET, a Dutch SME specialising in developing middleware for smartcards and USB tokens, and Consul (since acquired by IBM).

In the area of Identity Management, Morpho (formerly SAGEM and SDU Identification) is a major supplier of (electronic) identity cards and passports. Several young companies are active in biometrics, including Dartagnan-Biometrics, UniqKey, Priv-Id, Biometrics, and IDcontrol.

Research into Digital Right Management is not also carried out at Philips, but also at Irdeto (active in research for pay TV systems, also for mobile) and Civolution.

In the telecom sector, apart from KPN/Getronics, Vodaphone and Ericsson have research divisions in the Netherlands, in Maastricht and Gilze-Rijen, respectively.

In the financial sector, the major Dutch banks, such as ABN-AMRO, Rabobank, and ING, all have groups doing research on the ICT security of their financial infrastructure. In Europe, Dutch banks are seen as leading the way in internet banking (for instance with IDEAL, and as Chess and Rabobank coming in second place for the Excellence in Payments Innovation Award 2009 for Rabo SMS Betalen). The Dutch payment infrastructure is very efficient and has been a successful export product, giving rise to the companies Equens and Currence (formerly Interpay).

In the professional services sector, the so-called Big Four – PricewaterhouseCooper, KPMG, Ernst & Young and Deloitte – all have Dutch divisions that specialise in ICT security and provide information security services such as audits, penetration testing, and consultancy. SecurityMatters is a start-up that originates for Sentinels working on innovative solutions for the detection of attacks.

Several legal firms are specialising in ICT and law, e.g. ICTRecht, or in consultancy in the domain of privacy protection, e.g. Holvast & partner. Burea Beke (`beke.nl`) has a multi-disciplinary team of criminologists, psychologists, lawyers and sociologists that carries out scientific research and provides expertise to support decision makers in the area of crime and security. Hoffmann Bedrijfsrecherche is a leading company that carries out fraud investigation and provides forensic services and strategic risk management.

Appendix B: Ongoing ICT security research initiatives

Recent and ongoing ICT security research initiatives

The Ministry of Defence sponsors defence related security research, which is nearly all carried out by the Netherlands Organisation for Applied Scientific Research (TNO). This research is often of a highly confidential nature, which makes it difficult to include other partners into the research projects.

The Ministry of the Interior and Kingdom Relations supports civil security research (Innovatie voor Maatschappelijke Veiligheid, IMV) in 9 topical areas for a total funding of 21MEuro per annum. The areas are: Terrorism; Threat analysis and risk management; Criminality; Security of Critical Infrastructure Networks; Improving policing; Integrated systems; Equipment and materials; Education and training. One of these areas is strongly related to ICT security (Security of Critical Infrastructure Networks), but ICT security plays a role in most others too. The main partners in funded projects are the emergency services, TNO, a variety of businesses, and universities.

The Ministry of Economic Affairs, Agriculture and Innovation sponsors a large number of research programs (by means of instruments like Fonds Economische Structuurversterking, Pieken in de Delta), some of which are related to ICT security.

Together with STW, NWO, and ICTRegie, the Ministry of Economic Affairs supports the Sentinels research program for ICT related security research. This program is managed by STW, the research council for technical disciplines. A summary of the Sentinels program is given in Appendix C.

NWO recently had a 3.5 M€ scheme on Forensic Science, led by NWO Chemical Sciences, but with a broad scope where the focus was not on digital forensics. The NWO programme Maatschappelijk Verantwoord Innoveren (`www.nwo.nl/mvi`) funds some projects in the field of security and privacy by design.

Finally, most other ministries such as the Ministry of Security and Justice fund security related research as part of other research programs; unfortunately we have not been able to collect information on these programs.

Appendix C. The Sentinels research program

Sentinels is a national Dutch research program on security in ICT, networks and information systems. The program was designed to boost ICT security research and expertise in the Netherlands, and foster collaborations between universities, knowledge centres, and companies to build a national ICT-security research community. Sentinels was launched in 2004, financed by the Ministery of Economic Affairs, the Netherlands Organisation for Scientific Research (NWO), and the Technology Foundation STW, and at a later stage also the national ICT innovation authority ICTRegie. In three rounds, in 2005, 2007 and 2009, the program funded a total of 16 collaborative research projects between academia and industry.

The Sentinels research program

The Sentinels research program aims to improve ICT, networks and information security, including PCs, corporate and home networks, hand held devices, smart cards, and wireless networks. It targets the technical aspects of security through scientific research in close collaboration by academia and industry

Sentinels uses the standard procedure of the Technology Foundation STW, which funds collaborative utilisation-oriented research projects that are pre-competitive and tackle long-term problems. Here collaborative means that research projects are carried out by a consortium consisting of at least one university and one industry partners. Industry partners participate in the research and contribute to the project costs, with additional funding for personnel from Sentinels for PhD students or post-doctoral researchers at universities. This means that projects typically run for 4 years, the duration of a PhD. Each project has a panel of End Users that follows the progress to ensure broader dissemination and provide additional steering of the research.

Project grants are awarded through an open competition within the scope of the program, where project proposals are judged both on scientific merit and on utilisation, i.e. the application of the results of the research.

In addition to the research projects, Sentinels funded a part-time position of a Sentinels ambassador (drs. A. Eisner) to promote the program and its results to wider Dutch audience, especially in industry and government. Sentinels also supports networking and knowledge exchange by organising its own events (the Sentinels Security Day and the conference STW.ICT), by taking part in events such as the ICT-Kenniscongres and ICT-Delta, and by sponsoring the SAFE-NL workshops on ICT security research.

The total budget for Sentinels was 10.75 M€. The public financing was 8.35 M€ (2.5 M€ each from Economic Affairs, STW, and NWO, and another 845 k€ from ICTRegie). Companies participating in projects contributed another 2.4 M€. The first call for proposals for Sentinels was launched in 2004, with subsequent calls in 2006 and 2008. The first generation of projects, which started in 2005, have all ended now. Projects awarded in the last round started in 2009 and will end around 2013.

In preparation to the third call, more emphasis was put on user participation. To increase industrial participation, for the first time a small part of the budget was allocated to directly funding industrial participation. This approach was made possible by ICTRegie, who contributed 845k€, and clearly paid off, as the user contributions increased to 32 %.

The Sentinels research projects

The 16 Sentinels projects span a range of topics such as biometrics, risk assessment, searchable data encryption, intrusion detection, worm detection, virtual security perimeters, identity management, smartcards, RFID, mobile devices, mobile phones, privacy-enhancing technologies, social networks, and smart metering. These projects involved

- six universities: (TUE, UT, TUD, VU, RU, CWI),
- the knowledge centres TNO and Novay (formerly Telematics Institute),

- 18 companies (Brightsight, Chess IT, Philips, NXP, STMicroElectronics, Rabobank, Corus, Akzo, DSM, Hoffman, AtosOrigin, BiZZdesign, Ericsson, GetronicsPinkRoccade, Fox-IT, Alliander, Irdeto, Civolution), and
- several government agencies (B/CICT, ICTU, RDW).

Many more companies are active as End Users in Sentinels project fora. Around 35 PhD students/post-docs are employed and trained in these projects.

Results of the first Sentinels round

The six projects in the first round (DeWorm IPID, JASON, PINPAS, Practical Approaches to Secure Computation, and ProBite) have now all ended, allowing there results to be assessed. These projects resulted in two patents and in two spin-off companies, namely SecurityMatters and Priv-ID. In addition:

- ProBite had a follow-up with UT participating in the EU FP7 project Turbine. ProBite also received the European Biometrics Forum Industrial Award 2009.
- DeWorm had a follow-up with VU participating in the EU FP7 project Wombat and provided the basis for ERC (European Research Council) Starting Grant of 1.3 M€ for dr. H. Bos the Rosetta project on binary reverse-engineering.
- Practical Approaches to Secure Cooperation saw a follow-up in the NWO Vici awarded to prof. R. Cramer to work on secure computation.
- IPID had three follow-up projects (HERMES, CASTOR, MIDAS) looking at security of industrial SCADA projects in collaboration with Fox-IT, ABB, Brabant Water, Waternet, Alliander and the GasUnie.
- PINPAS had a follow-up at the TU/e with a project where end user Riscure sponsored a research position. At the RU it had follow-ups in collaborations with Collis and PwC (e.g. for the EU agency FRONTEX) and a project where TransLinkSystems funds a PhD student on smartcard-based e-ticketing solutions.

Impact of Sentinels

The Sentinels program has provided and continues to provide an important catalyst for security research and expertise in the Netherlands. There is now a well-connected ICT security research community, that spans and links industry, academia, and the public sector. One concrete manifestation of this community is through the IIP Veilig Verbonden `www.iip-vv.nl`. Universities have also recognized the growing importance of computer security and invested in the area.

Apart from the direct impact of the research carried out in Sentinels, the highly skilled researchers trained in the projects are maybe the more valuable contribution. Here the PhD and post-docs trained in Sentinels projects represent only the tip of the iceberg of much larger numbers of Bachelor and Master students finding their way to the ICT security field.

Researchers active in Sentinels can also lay claim to real societal impact. They have been involved in debates on topics such as the ov-chipkaart electronic voting, electronic patient records (EPD), the biometric passport, smart electricity meters, and electronic roadpricing. Note that many of these topics were not foreseen when the Sentinels research program was first drafted in 2004, and are not the subject of any Sentinels project; still, they have been picked up by the security research community supported by Sentinels.

1. JASON, Generic and Secure Remote Management Infrastructure
   Project leader: dr.ir. E. Poll (RU)
   In collaboration with Chess.

2. IPID, Integrated Policy-based Intrusion Detection
   Project leader: prof.dr. Roel J. Wieringa (UT)
   In collaboration with Rabobank Nederland and TNO ICT.
3. Practical Approaches to Secure Computation
   Project leader: prof.dr. Ronald J.F. Cramer (CWI)
   In collaboration with Philips Research.
4. ProBiTe, Protection of Biometric Templates
   Project leader: dr.ir. Raymond Veldhuis (UT).
   In collaboration with Philips Research.
5. DeWorm, Worm monitoring on Internet backbones
   Project leader: dr.ir. Herbert J. Bos (VU)
   In collaboration with TNO ICT.
6. PINPAS JC, Program INferred Power-Analysis in Software for Java Card
   Project leader: dr. Erik P. de Vink (TUE)
   In collaboration with UT, RU, Brightsight (formerly TNO-ITSEF) and STMicroelectronics.
7. S-Mobile: Security of software and services for mobile systems
   Project leader:.dr. B. Crispo (VU)
   In collaboration with Philips Research, TUE, TNO ICT.
8. VISPER: The virtual security perimeter for digital, physical, and organisational security
   Project leader: Prof.dr.ir. P.H. Hartel (UT)
   In collaboration with Atos Origin, B/CICT (Belastingdienst/Centrum voor ICT), BiZZdesign, Fox-IT, and Getronics-PinkRoccade.
9. SEDAN: Searchable data encryption
   Project leader: prof.dr. H. van Tilborg (TUE)
   In collaboration with Philips Research.
10. VRIEND: Value-based security risk mitigation in enterprise networks that are decentralized
    Project leader: prof.dr. Roel J. Wieringa (UT)
    In collaboration with Akzo Nobel, Corus, DSM, Hoffmann Bedrijfsrecherche, and Philips International.
11. PEARL: Privacy enhanced security architecture for RFID labels
    Project leader: dr. S. Mauw (TUE).
    In collaboration with Philips Research and TNO ICT.
12. Secure metering
    Project leader: Prof.dr. M.C.J.D. van Eekelen (RU).
    In collaboration with RDW and Alliander (formerly Nuon).
13. CREST: Collusion resistant tracking
    Project leader: Dr. B. Skoric (TUE)
    In collaboration with Irdeto and Civolution.
14. Mobile IDM: Identity management on mobile devices
    Project leader: Prof.dr. S. Etalle (TUE).
    In collaboration with RU, TNO ICT, Ericson, and Novay.
15. Kindred Spirits: Privacy enhanced social networking Prof.dr.ir. R.L. Lagendijk (TUD)
    In collaboration with UT, TNO-CIT, Philips, Irdeto, De Waag, PAIQ, BPP, BL.
16. Revocable privacy
    Project leader: Dr. J.H. Hoepman (RU)
    In collaboration with CWI, TNO, and ICTU.