NCSRA II

National Cyber Security Research Agenda II

Contents

Editors:
prof.dr.ir. Herbert Bos (Vrije Universiteit Amsterdam)
prof.dr. Sandro Etalle (Technische Universiteit Eindhoven)
ir. Frank Fransen (TNO)
dr.ir. Erik Poll (Radboud Universiteit Nijmegen)

September 30, 2013

About this document

The NCSRA II is the updated version of the National Cyber Security Research Agenda (NCSRA), which was drafted in 2011 and served as the guiding document for the 2012 calls for cyber security research proposals in the Netherlands.

This document, like the previous version of the NCSRA, has been edited under the coordination and responsibility of the *ICT Innovatie Platform Veilig Verbonden* (IIP-VV)[1]. NWO and four ministries (EZ, V&J, Def, BZK) requested the IIP-VV to produce an update of the NCSRA, in order for them to use this as a basis for a new cyber security research call in 2014.

This research agenda is a strategic document that provides a frame of reference for the research challenges and opportunities for the wider field of cyber security, so that it may help to align and synchronise the various ICT security research initiatives in the public and private sector in the Netherlands. It has been produced with a broad involvement of researchers from various disciplines (computer science, law, public administration, cybercrime sciences, and police studies), including experts from universities (incl. RU Nijmegen, TU Delft, TU Eindhoven, University of Tilburg, University of Twente, and VU Amsterdam) and other knowledge institutes and centres of expertise (incl. TNO, NCSC, WODC, NSCR, Novay, and NFI), and through discussions with experts from industry and (semi-)governmental organizations. For validation, three meetings have been held with representatives of three clusters of applications domains to solicit feedback, discuss comments, and get input on draft versions of this agenda.

There were several reasons for publishing a new version of the Research Agenda for Cyber Security. Where the previous agenda focused almost entirely on defense, we now incorporate more offensive operational cyber activities also. Moreover, in the previous research agenda, some research themes lacked both a clear separation and a more precise and complete description.

Finally, we added a new `addendum', as a (separate) companion document to provide concrete examples of research topics and questions.

1 http://www.iip-vv.nl

NCSRA II

A National Research Agenda for Cyber Security

As our reliance on ICT increases, so do concerns about its security. This is explicitly recognised and addressed by the Dutch government in its first National Cyber Security Strategy (NCSS, 2011) and the updated version, the NCSS II. The growing complexity of ICT systems means that vulnerabilities are harder to avoid, the increased use creates new opportunities for increasingly sophisticated attackers, and chain dependencies between systems and services mean that any disruption can quickly escalate.

Rising worries about state-sponsored cyber attacks have led to military cyber task forces in most advanced countries. In 2012 we have seen that the military-grade Stuxnet attack on Iran's uranium enrichment facility was not an isolated event. Similar, equally complex malware such as Flame, Duqu and Gauss have shown that cyber attacks are weaponized to an incredibly advanced level. For example, for Gauss, discovered in the summer of 2012, we still do not know what it does, more than a year later, despite massive efforts by the world's best malware research labs!

Unfortunately, the Netherlands is an important player in the world of cybercrime. As the country with the highest broadband penetration and the best quality broadband in the world, the Netherlands is a prime target for botnets. The 2013 version of the Cyber Security Assessment Netherlands[2] (NCSC, 2013) provides a good insight into our country's interests, the threats that may harm these, and our resilience to defend against these.

Its main conclusions can be summarized as follows: a) the dependence on ICT for individuals, organisations and society has grown, b) the number of cyber threats has increased (in particular the threats posed by nation states and professional criminals), and c) the resilience has remained about the same because new initiatives and measures do not keep up with vulnerabilities, and basic measures are not always taken.

As we cannot afford to let cyber criminals erode the trust we have – and need to have –

Figure 1: Unit 61398 is the Chinese army's advanced persistent threat unit that has been alleged to be the source of Chinese computer hacking attacks.

2 http://www.ncsc.nl

Figure 2: The Stuxnet attack on the uranium enrichment facility in Iran was only the start of a wave of military-grade malware that includes Flame, Duqu and Gauss. For Gauss, researchers are still trying to discover its exact functionality more than a year after its initial discovery.

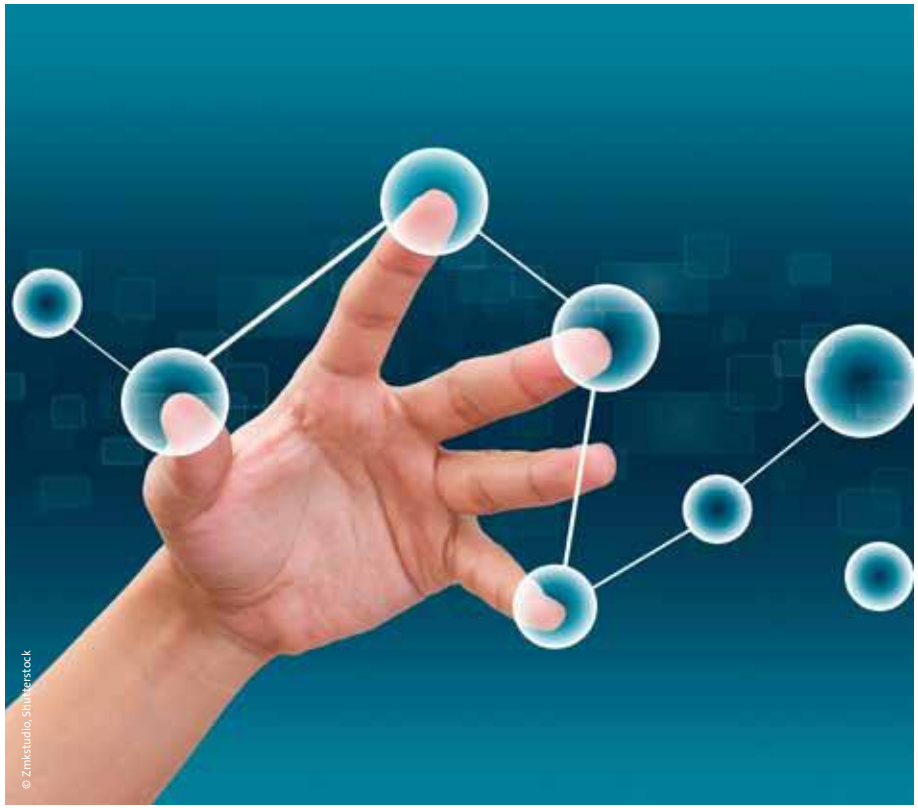
in the ICT infrastructure and the services it provides, research is needed. *Trust* is a *conditio sine qua non* for normal economic transactions and inter-human communication. It is at the core of social order and economic prosperity, and in an increasingly ICT-dependent world, the security of ICT plays an ever more important role here.

Continued investment in security expertise provides up-to-date and strategically essential knowledge for decision makers to act wisely in complex cases such as electronic passports and online IDs, e-health, cybercrime, cyber warfare, smart grids, public transport, smart cars and roads, and other critical infrastructures. On the positive side, ICT security presents significant economic opportunities, through services and products that provide improved security, and by enabling the continuous growth in the use of ICT (Ernst&Young, 2011). The demand for solutions in this area is huge and growing. Bringing together the key organisations and research groups fosters a community that can address this demand and provide a strong economic impulse.

Policy Context

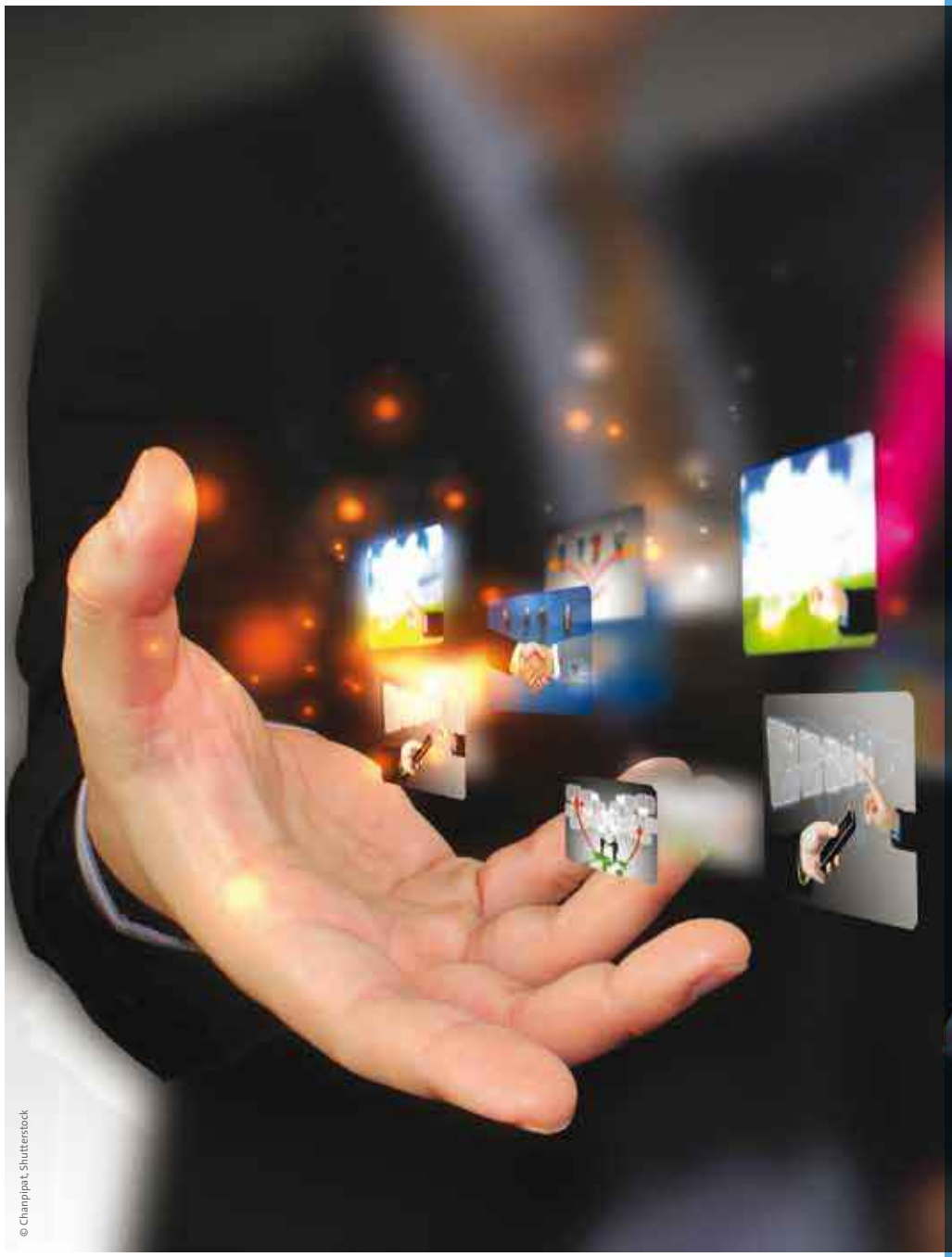
This research agenda aims to provide a frame of reference to align and synchronise the various ICT security research initiatives in the public and private sector in the Netherlands, and to help in boosting Dutch ICT security expertise through research at universities and knowledge centers, government agencies, and companies, and to foster partnerships between these various partners.

In its Top Sector policy, the Dutch government focuses on innovation in nine economic top sectors for growth that have been identified. The aim of this agenda is to serve as leading for all cyber security research, regardless the top sector the research is associated with. At least two top sectors, High Tech Systems and Materials (HTSM) and Energy, directly deal with cyber security, as does the Roadmap ICT which cuts across all Dutch top sectors in recognition of the role of fundamental and strategic ICT research in many domains. The Security Roadmap under HTSM, the Smart Grids Innovation Contract under Energy, and the Roadmap ICT under the theme 'ICT one can rely on' all refer to the NCSRA.

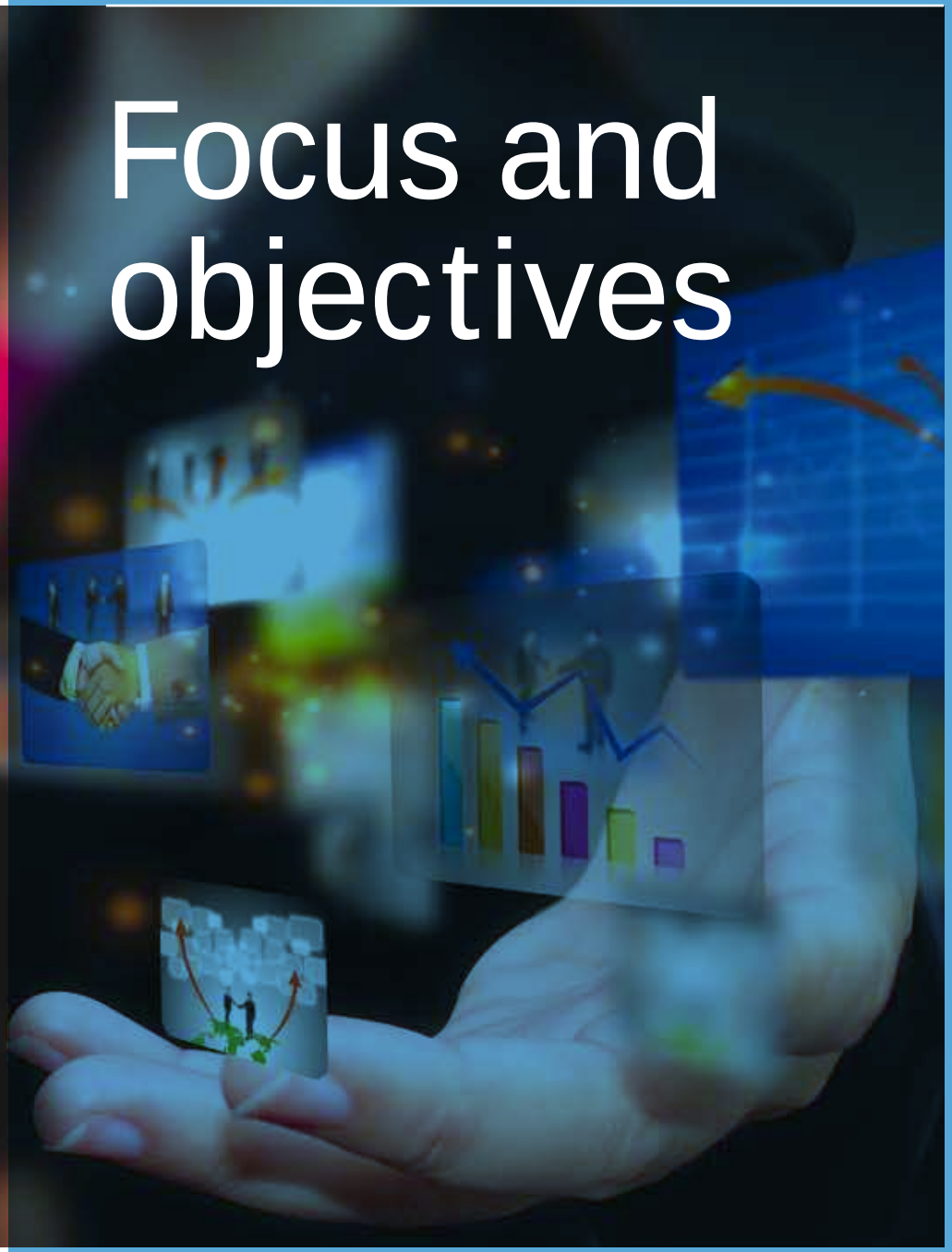


This agenda can also help to position the Dutch research community and industry in the international context, in the EU (European Commission, 2013; Council of the European Union, 2012) and beyond, notably in the US (US Department of Homeland Security, 2009). International collaboration is crucial, since cyber security problems transcend national borders, and new developments in ICT take place in a global research community. The NCSRA II positions itself alongside the NCSS II and complementary activities focused on more short-term and/or operational goals, such as improvements in the legal and law enforcement frameworks to deal with cybercrime, response teams to handle cyber security incidents, threat analyses and protection of existing ICT infrastructure, awareness campaigns (such as Alert Online), etc. Here the goal is to continue the thrust of the research programmes started with calls for proposals in 2012, handled by AgentschapNL for short term applied research in SBIR projects and by Netherlands Organisation for Scientific Research (NWO) for long term applied and fundamental research, which in turn had a precursor in the Sentinels programme[3].

3 http://www.sentinels.nl



Focus and objectives



The NCSRA II 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, and the earlier '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) and the newer "Red Book" produced by the European Network of Excellence SysSec (SysSec, 2013).

The objectives of the NCSRA II based research programmes are:

- To improve the security and trustworthiness of the ICT infrastructure and ICT services.
- To prepare the Netherlands for the security challenges of the next 6-12 years.
- To stimulate the Dutch security economy and promote innovation in this sector.
- To strengthen and broaden Dutch security research by fostering cooperation between knowledge institutions and relevant public and private organizations.

This agenda contributes to these objectives by defining themes for cyber security research and education, both in a public and private context.

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.

Like the previous version, this version of the NCSRA considers cyber security in the broadest sense. Thus, while traditional computer science plays an important role, it also considers the roles of α and γ disciplines.

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

The NCSRA II identifies the following research themes:
1. Identity, privacy, and trust management
2. Malware and malicious infrastructures
3. Attack detection & prevention, monitoring
4. Forensics and incident management
5. Data, policy and access management
6. Cybercrime and the underground economy
7. Risk management, economics, and regulation
8. Secure design and engineering
9. Offensive cyber-capabilities

The NCSRA II chooses a broad perspective, knowing that innovative cyber security solutions are mainly driven by inspiration, not by orchestration. It leaves putting emphasis on one or more research themes to those who provide funding for research programs, formulate research proposals, etc.

© Chanpipat, Shutterstock

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. They range from Advanced Persistent Threats, perhaps initiated by governments, to much simpler but still costly cyber vandalism, for instance by 'script kiddies'.

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 cybercrime, the effectiveness of measures, including law enforcement, also across international borders and legal jurisdictions, 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. Stimulating collaboration between them is important: 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 NCSRA II provides a real opportunity where the Netherlands can show the way forward by establishing serious collaboration between these communities.

© Carlos E. Santa Maria, Shutterstock

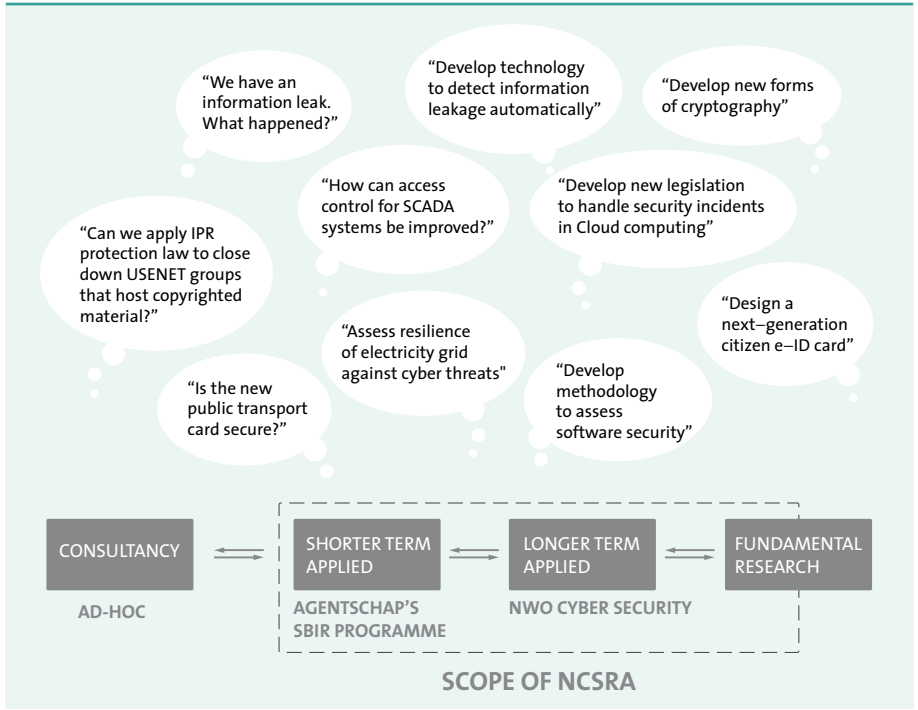


Figure 3: The spectrum of ICT security research problems – with examples

The many aspects of cyber security
Cyber security is a complex issue, affecting many application domains and straddling many (scientific) disciplines and fields. Many different dimensions could be used to classify and categorize the research challenges in cyber security, for example:

- the different scientific **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, and psychology.
- the different **application domains**, such as finance, commerce, government, telecom, transport and logistics, which includes some critical infrastructures.
- the different **stages**: prevention, detection, analysis, response & recovery, governance, with risk assessment as the overarching activity to balance these.
- 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 different **technologies**: tools, techniques, systems, and methods to build solutions and applications, cloud computing, mobile devices, embedded systems, pervasive computing, internet of things, etc.

All these classifications or dimensions have their pros and cons: no matter which is chosen, there are always some research questions that span multiple categories. After considering the alternatives above (and others), a thematic classification (with nine research themes) mapped on a number of application domains (resulting in a two dimensionial representation), as will be presented in Sections 4.2 and 4.3, was chosen for this agenda as the preferred approach.

The research will involve and benefit the entire field: industry, knowledge centers, education, 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, and from applied to fundamental, 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 scientic 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. Good examples are the projects funded in the 2012 SBIR call for proposals in cyber security supported by AgentschapNL and earlier programs such as the NAVI Sub-arena (which focused on vital ICT infrastructure).

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 knowledge and expertise, but also for sharing challenges and problems – a practical immediate problem may pose an interesting scientic 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.

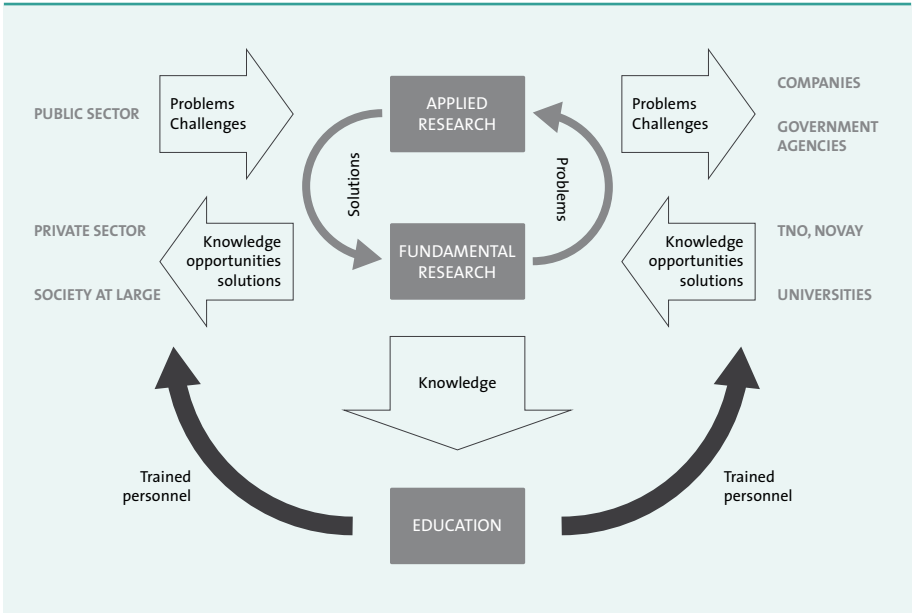


Figure 4: ICT security research

© Chanpipat, Shutterstock

Technologies, application domains, and research themes

NCSRA II

Concrete research questions typically arise in a specific context, which may involve a certain technology (e.g. cloud computing), or a particular application domain (e.g. finance), or a combination of the two. Still, similar research questions arise across different contexts, representing broader research themes. The next two sections make an inventory of the most important contexts, both regarding technology and application domain. The last section then lists the underlying research themes that represent the central challenges for security across these contexts.

4.1 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 the 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.

© Rafal Olechowski, Shutterstock

Challenges are also raised by the sheer amount of data. More and more organizations are amassing data sets that are so large and so complex that they cannot easily be processed by conventional means of data processing. Finding anomalies that point to security incidents in Big Data is a difficult problem.

Another important technological trend is **pervasive systems**: we are rapidly moving away from the desktop-model, and increasingly interact with ICT 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 (e.g. smart phones), but many are not (e.g. wearable computing, or smart insulin pumps). The security of machine to machine (M2M) interactions as seen in modern cars, and manufacturing, is becoming an increasing concern.

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.

Figure 5: Application domains (outer ring) and research themes (inner ring)

Besides the location of computation and hardware capabilities, we distinguish a myriad of technologies in the nature of the software that have heavy implications for security. Information exchange no longer has a predominantly client-server nature. Information is exchanged in peer-to-peer fashion, more and more information is shared via social networks, and security sensitive operations (related to banking, health-care, taxes, etc.) all occur via the Internet with a variety of technologies for things like authentication and protection. A research program in security should find its place in this moving technology landscape.

© Rafal Olechowski, Shutterstock

4.2 Application domains

ICT is used in 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. Many of these domains are interdependent and incidents in one sector will have cascading effects. Below we highlight some – but by no means all – of these application domains. Several of these can be considered as critical infrastructures.

- **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.** 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, or e-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 aimed 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 the 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 inter-dependencies 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 grids.** 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 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 Grid and the privacy of individual users.

- **Finance.** Financial institutions or their customers are increasingly often victim of targeted cyber attacks, 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, but this change 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 into an open system which is by definition open to cyber-attacks.

  Cars are only one example. White-hat hackers have shown that new air traffic protocols are susceptible to a wide range of attacks. Several incidents in the past have shown that train services are vulnerable to software problems. There is no doubt that this is true for most modern forms of transport.

In logistics, 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.

- **Healthcare.** Processes in the health sector are increasingly being supported by ICT. ICT is also the key enabler of new 'e-health' methods of providing care, as exemplified by ambient assisted living. However, patient data is often spread across many care providers, such as the general practitioner, dentist, specialist, physiotherapist, hospital staff, pharmacists 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), to 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.

- **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, with the increasing use of online information and services to citizens in e-government. Here the government is an important role model, and its conduct sets a standard. Also, ICT 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 the NCSC), 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 National Cyber Security Strategy. 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. 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 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, including the Netherlands, interest in a pro-active strike force is growing and more research and study is needed in this area.

- **Law enforcement.** Similarly, the use of ICT has become a crucial tool in many tasks related to tracking down, monitoring and apprehending criminals. Research is needed into improving these abilities without jeopardising the safety and privacy of citizens. Some of these capabilities are extensions to existing capabilities like tapping, while others are entirely new. The research challenges include many different fields: technical, legal, sociological, etc. Again, attribution in particular is a difficult but hugely important research task.

- **Telecom.** Underlying the networked systems and of crucial importance to the dependability of our ICT infrastructure (and society in general) are the network services provided by the Telecom sector. Attacks on telecom equipment may lead to serious privacy leaks and disruption of services that affect millions of people. It is important to study the risks and possible security measures for this sector.

- **Media and news outlets.** News outlets and mass media are important channels for disseminating information and (thus) attractive targets for attackers. Both the news outlets and the threats are increasingly digital. In the past, we have witnessed the compromises of the websites of governments like that of Syria by Anonymous, but more traditional television and radio broadcasts and printed media are possible targets also. Besides these traditional media, the domain also includes new media outlets like blogs, social networks, tweets, etc.

4.3 Research Themes

To structure the discussion on a potentially infinite list of research topics, across many disciplines and many application domains, the NCSRA II distinguishes nine research themes, listed and discussed below.
The themes have been chosen to cover the whole spectrum of research challenges, across scientific disciplines, across applications domains, and across the stages from prevention, through detection to response. This presentation in research themes was chosen because it seemed the best way to reflect the complexity and interdisciplinary nature of cyber security, where other classifications, for example along the dimensions discussed in the text box on page 17, might create unnatural boundaries. Each theme listed requires contributions from multiple disciplines: technical, legal, economical, etc. We emphasize that in all themes, we should work on new methodologies and approaches, as existing methodologies often no longer suffice or even apply. For instance, legislation developed for the physical world often matches awkwardly to cyber incidents.

© Rafal Olechowski, Shutterstock

1. **Identity, privacy and trust management**
   Managing the (digital) identities, protecting citizen's privacy, and managing the trust in the online world are essential functionalities of the *future internet*[4] , which are required in each of the application domains listed above. The application domains 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 mechanisms will be used. Therefore, different identity management solutions are needed to cater for the various needs. Research sub-areas include the computer science and cryptography 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. **Malware and malicious infrastructures**
   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.

4 See Future Internet Assembly: http://www.future-internet.eu/

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.

© Rafal Olechowski, Shutterstock

In terms of research, it poses an interdisciplinary challenge. We need advances in technology, for instance in reverse engineering, de-obfuscation, botnet tracking, analysis of criminal infrastructures, and classification and clustering of malware. Likewise, we need reliable methods to estimate the number of infected machines and the effectiveness of counter-measures.

At the same time, we need arrangements to shape the socio-economic forces that fuel or mitigate the spread and impact of malware. From a historical perspective, we should study trends in malware – as doing so prepares us for new threats in time. Unless these issues are researched jointly, we will be stuck with partial solutions of limited value.

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.

3. **Attack detection, attack prevention, and monitoring**
   Cyber attacks by malware and human attackers range from large-scale Denial-of-Service attacks, epidemic virus distribution, to small-scale attacks on high-value targets. Sometimes attacks are stealthy or even dormant, for instance in the case of backdoors, while in other cases, attacks are very noisy. Monitoring systems and networks helps to detect and prevent the attacks as early as possible, but even here, the sheer volume of information in the age of Big Data often make it difficult to detect anomalies that indicate security issues.

   Technological research challenges include binary hardening, network monitors, IDS and IPS systems, 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 system behaves in an anomalous manner. Likewise, compliance monitoring is important to spot vulnerabilities (in systems and organisations) as early as possible. From an organisational and management perspective, we need research into policies and protocols for monitoring, auditing, etc. From a legal perspective, we need clear rules for what is and what is not permitted in monitoring (and by whom), as well as ways to enforce these rules.

4. **Forensics and incident management**
   Forensics and incident management are related but different activities that follow in the aftermath of an attack. Incident management consists of recovery (e.g. salvaging as much of the compromised system as possible), but also restoring systems and state, and becoming operational again at minimal cost. Part of the non-technical side of incident management consists of setting up protocols and organizational structures for handling the incidents (who is in charge, who answers to whom, what role do various parties play, etc.) – all in the light of rules and regulations (such as the general obligation to report information leaks). Another part will be the assessment of things like: what was compromised, how badly was it compromised, can the data manipulation be reverted, what needs manual inspection, etc.? At the same time, it requires organisational procedures to deal with reviewing security protocols, disclosure to press and public, assembling teams to deal with the recovery, etc.

   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.

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. In a crime scene, however, highly skilled digital forensics expertise is needed on-site as quickly as possible to collect evidence, in a secure way so that it that is admissible in a court of law. This process requires deeply technical as well as legal knowledge. The fact that cybercrime often spans international borders poses an important additional challenge here. Live forensics (forensics on a system that cannot be switched off, 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. The same is true for the legal side: what is admitted as what sort of evidence under what circumstances? Forensic evidence has been used in a number of high profile cases and is becoming more accepted as reliable within US and European court systems. However, this is hampered by a lack of standards for digital forensic evidence, especially with multiple parties providing digital forensic evidence. Again, research is needed into developing such standards and methods. Finally, there are open issues related to liability, possible insurance and limitations thereof.

5. **Data, Policy and Access Management**
   In the application domains 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 (possibly over very long time scales), 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. Likewise, need to develop methods (both technical and non-technical) to protect data better.

   Security in systems that handle sensitive information requires the enforcement of information flow according to well-defined policies. We need research in novel access management techniques to help regulate who gets access to what information and under what circumstances. Given the current trend toward storing more and more data into the cloud, with the associated ambiguities regarding ownership and access, this problem is increasingly important. We need research that helps us decide how data should be managed, where it should be stored, how it will be maintained, who can do what with the data, and so on. And we need new technology to enforce these policies.

   This theme, which centers on data, has a close link with research theme 1, which centers on users. After all, any form of access control presupposes some notion of identity for users, and so access control solutions researched in this theme may use the identities provided by schemes developed in theme 1.

© Rafal Olechowski, Shutterstock

6. **Cybercrime and the underground economy**
   There is organised cybercrime, such as skimming, botnets, provision of child pornography and advance fee fraud, and unorganised (common) cybercrime, 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 nature and background of perpetrators, 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 study the underground economy, its size, its characteristics and how it is intertwined with the legal economic system. Also we need to investigate and assess the effectiveness of measures against cybercrime 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.

   In addition, we often lack understanding about the socio-cultural context of the attack. 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.

7. **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. A scientific basis for establishing such facts is currently missing. One central problem here is that concrete data is often lacking, and more research could provide a more solid basis. For instance, we need to know what does and does not work in

prevention, deterrence, and regulatory counter-measures. Likewise, the role of regulation and legislation should be analyzed deeply, vis-a-vis other measures.

© Rafal Olechowski, Shutterstock

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 a complex value chain there may not be any economics incentives to fix a problem. Indeed, in cyber security there are many *externalities*: costs that are 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 suitable technical protection mechanisms. New studies into the incentives and externalities are needed, to get a better understanding of the economics of security – and the economic (dis)incentives that occur – and 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 and legal constraints may apply in the various application domains, and at different levels: national, EU, and international.

8. Secure Design and Engineering

System and software engineering still lack the methods and tools to design, implement, 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, after security problems arise, with awkward add-ons if bad initial design decisions can no longer be reversed. Moreover, even if a design is flawless, in implementing it many security flaws will be introduced in the software, only some of which will be caught in testing, leaving many to be dealt with by patching only after their discovery, if ever. Finally, the secure system should be usable.

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, and only released into the field after rigorous and reliable assessment. While good 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.

Better techniques are needed for testing and verification to discover bugs prior to release. Besides software engineering, economics can play an important role in this area. After all, the cost of a more secure system may initially be higher but lower in the long run. However, turning this into an economic incentive requires better techniques to assess risks and costs.

© Rafal Olechowski, Shutterstock

9. Offensive Cyber Capabilities

In some domains, it is important to develop techniques to strike back at attackers (both physically and by means of a cyber-attack). Besides the cyber-technical advances (often collectively referred to 'hacking back'), these include ways to disrupt financial and other support infrastructures on which the adversary relies. Offensive cyber capacities are equally essential in testing the defenses of existing systems – for instance in penetration testing.

Research challenges include the development of reliable techniques to penetrate other systems, evade defenses, and escalate privileges. Non-technical challenges include the development of legal guidelines to determine when offensive capacities may be used and by whom, and against which targets. Decision procedures and command structures for the use of offensive cyber force are also areas that require research.

Even if initially aimed at one specific application domain, research in the themes above can provide generic solutions that will apply to many application domains. For this to happen it is important that the NCSRA helps to disseminate knowledge and project results across application domains, and the different communities involved.

References

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

Council of the European Union (2012). Proposal for a Council decision establishing the Specific Programme implementing Horizon 2020 - The Framework Programme for Research and Innovation (2014-2020). Available from http://register.consilium.europa.eu/pdf/en/12/st17/st17029.en12.pdf.

NCSC (2013). Cyber Security Assessment Netherlands (CSAN-3). Annual trend report of the Dutch National Cyber Security Centre. Available from http://www.ncsc.nl.

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.

© Skovoroda, Shutterstock

European Commission (2013). Cybersecurity strategy of the European Union: An open, safe and secure cyberspace. Available from ec.europa.eu/information_society/newsroom/cf/dae/document. cfm?doc_id=1667.

US Department of Homeland Security (2009). A roadmap for cybersecurity research. Available from http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf. Ministerie EL&I (2011).

Digitale Agenda.nl - ICT voor innovatie en economische groei. Beleidsnota.

NCSS II (2013) Nationale Cyber Security Strategie editie II, Ministerie van Veiligheid en Justitie.

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

SysSec (2013). The Red Book – the SysSec Roadmap for Cyber Security Research. European Network of Excellence SysSec (Systems Security Research). Available from http://www.red-book.eu.

Websites

http://www.iip-vv.nl
http://www.sentinels.nl

© Everything possible, Shutterstock

Addendum to the NCSRA II

Editors: prof.dr.ir. Herbert Bos (Vrije Universiteit Amsterdam)
prof.dr. Sandro Etalle (Technische Universiteit Eindhoven)
ir. Frank Fransen (TNO)
dr.ir. Erik Poll (Radboud Universiteit Nijmegen)

September 30, 2013

About this document

This addendum to the updated National Cyber Security Research Agenda (NCSRA II) aims to help readers of the NCSRA II in getting a better understanding of the context and scope of the cyber security research themes. To do this, this addendum gives, for each of these research themes, examples of more concrete research topics, considers the scientific disciplines involved, and provides examples of existing research projects and of research questions for possible future projects. N.B. the lists of example research questions are *not* meant to be exhaustive.

The examples of existing research projects include projects awarded in the Cyber Security calls in 2012 funded by NWO and the ministries of Security and Justice, Economic Affairs, Defence, and the Interior: both short-term projects awarded in the SBIR call organized by AgentschapNL[1] and the long-term projects awarded in the Cyber Security call organized by NWO[2]. The list of examples has been compiled during our field consultation. This addendum thus also provides an (not necessarily complete) overview of the Dutch cyber security research landscape, augmented with needs and research questions as formulated by public and private users of (future) results of research projects.

During our consultation meetings, we explicitly asked the attendants to give priorities for the research themes and topics. While opinions varied, the dominant response by far to this request was that doing so in the field consultation would not be a good idea. Instead, the consensus was that while the priorities will be determined by the interests of the funding bodies, ideally they should not be too restrictive. After all, a good indicator of what the stakeholders find important is what topics they choose for their research proposals, and for which they are willing to provide a signicant investment.

1 See http://www.agentschapnl.nl/programmas-regelingen/cyber-security.

2 See http://www.nwo.nl/onderzoek-en-resultaten/programmas/cyber+security.

1 Cyber Security Research Themes

The NCSRA II presents nine cyber security research themes. For each of these themes we present in this section a non-exhaustive lists of research topics and of scientific disciplines involved, we briefly describe one or more existing national research projects, and we list both short and long term research questions. The content of this section has been established in consultation with national experts in the cyber security research field.

The examples of short term project are taken from the SBIR projects whose first phase was awarded in the 2012 SBIR Cyber Security call organized by AgentschapNL.

As the research themes are not disjoint, but several touch one another, some of the projects in fact straddle more than one research theme.

1.1 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.

Possible research topics	Disciplines
• Identity and Access Management technologies and infrastructures • Legal and socio-economic aspect identity and access management • Privacy Enhancing Technologies • Anonymous credentials • Anonymity and pseudonymity • Usability aspects of identity and privacy technologies • Privacy by design • Business issues related to trust and identity • Individual's rights concerning privacy and identity management • Trust management and reputation systems • Technologies for Building Trust • . . .	• Computer Science • Cryptography • ICT Law • Psychology

Existing long term research: Revocable Privacy

The Sentinels[a] project *Revocable Privacy* tries to resolve the possible tension between security and privacy in providing flexible techniques for Privacy-by-Design. The project investigates techniques that guarantee a user's privacy unless he breaks clearly defined rules that have been fixed in advance, in which case privacy is revoked and personal details can be released, say, to the police. Techniques that provide such guarantees can open up new possibilities to use privacy-sensitive information in a carefully measured way to fight cybercrime or terrorism, for instance information obtained using camera surveillance, road pricing, DigID, or the public transport card.

a The Sentinels research programme, see http://www.sentinels.nl, funded by the Ministry of Economic Affairs, NWO/ICTRegie, and STW, was a pre-cursor of the current Cyber Security Research programme.

An example scenario is the fight against so-called tarpaulin cutters, criminals that target lorries parked overnight at motorway car parks, cutting open the tarpaulin to steal any valuable cargo. An algorithm has been developed for a number plate detection system at these car parks to detect such criminals: If the same car is detected at more than four parking areas in a single day, then the number plate is released, but all other number plates are guaranteed to be kept confidential. The algorithm has been proposed to the KLPD which is now examining if and how this algorithm can be implemented.

Contact: Dr. J.H. Hoepman (TNO & Radboud Universiteit Nijmegen)
Partners: CWI, TNO, and ICTU

1.1.1 Example Research Questions

Short term research questions

- What are the privacy risks of cloud computing?
- How is privacy perceived by the general public and how can users be made more aware of the privacy risks in day to day life?
- What is the practical deployability of privacy by design?
- What are the alternatives for and enhancements of the certificate based trust model currently used on the Internet and how do they compare?
- How to correctly anonymize large amount of aggregated data?

Long term research questions

- How do individuals deal with their online identities and associated authentication mechanisms, in both their private and/or professional life?
- How can an individual manage their online identities throughout life?
- How can technology, regulation, and organisational structures contribute to privacy friendly systems?
- How can we establish a more reliable, secure, and resilient global infrastructure for establishing trust between systems then the current PKI certificate based infrastructure?
- How to protect the privacy in big data and internet-of-things?
- Can we get rid of passwords and what does such a password-free world look like?

1.2 Malware and malicious infrastructures

The research theme 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.

Possible research topics	Disciplines
• Malware reverse engineering • Monitor, localize and identify botnets and distribution of malware • Analysis of botnet command & control mechanisms • Study malware trends and future malware threats (e.g. social networks, cloud computing and mobile devices) • Technical, legal and other methods used to mitigate, investigate, dismantle or disrupt botnets • Security economics of malware and malicious infrastructures • Exploitation techniques • …	• Computer Science • Criminal & ICT Law • Criminology • Economics • …

Existing long term research: The Power of Obfuscation (Re-Cover)

Software vendors and cybercriminals alike rely on obfuscation techniques to protect sensitive information from the prying eyes of reverse engineers. Obfuscators transform both the control flow and data layout of a program to make it practically infeasible to reverse them. A program's control flow can be hidden by a VM, while data layouts are hidden by splitting variables over multiple memory locations, or generating a string at runtime rather than storing it explicitly in the binary, etc.

Over the years, much research was conducted in probing control obfuscations. Typically, it shows that most techniques are limited in the face of determined attackers. Surprisingly, we do not know any such probing attempts for obfuscated data and memory. This is remarkable, because for reverse engineers there is great value in the data and its layout. So far, the tacit assumption has been that data obfuscation is strong and cannot be automatically reversed in practice.

The research question is whether this assumption is justified. Specifically, the hypothesis behind the project is that it is false for current data obfuscators and that it is feasible to recover the data structures in a semi-automated way. If this is indeed the case, the research outcome will have far-reaching implications for software security – both when it comes to analysing malware or designing better obfuscation techniques for engineering secure application.

Internationally, this project collaborates in the EU FP7 project WOMBAT (Worldwide Observatory of Malicious Behaviors and Attack Threats).

Contact: Prof.dr.ir. H.J. Bos (Vrije Universiteit Amsterdam)
Partner: Irdeto

1.2.1 Example Research Questions

Short term research questions

- Can we profile the owners of the infected machines–are they mostly owned by home users, SMEs, big companies, etc.?
- Investigate the willingness of a selection of countries to tolerate "hacking" as a means to clean up infected machines.
- What are the interdependencies between different kinds of malware (and the corresponding infrastructures): how often do the criminals use pay-per-install services to spread their malware, how common is the use of independent proxy networks, etc?
- Investigate the trends in botnets: in what ways do new botnets protect their C&C infrastructure against take-downs and disruptions?

Long term research questions

- Can we develop new techniques to analyze strongly obfuscated malware?
- Develop legal and ethical frameworks for cleaning up infected machines.
- Develop techniques to dismantle very resilient botnets (like GameOver/ Zeus and Sality).

1.3 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.

Possible research topics	Disciplines
• System hardening strategies • IDS and IPS systems • Anomaly detection • Security event correlation • Vulnerability management • Techniques for vulnerability monitoring • Self-protection systems, automatic attack containment and response • Cross-organisation and cross-border security monitoring and situational awareness • Legal perspective on attack detection and monitoring • Information sharing • Containment • Visual Analytics • . . .	• Applied mathematics • Computer science • ICT Law • Policy, Organisation & Management • Scientific visualization • . . .

Existing long term research: Visualization and deep protocol analysis to detect cyber espionage and targeted malware (Spy Spot)

Cyber-attacks have grown in number and sophistication, achieving unprecedented success in reaching their target. Advanced Persistent Threats (APTs) such as data exfiltration attacks are both dangerous and difficult to detect. These targeted and stealthy attacks using specifically developed malware circumvent classical detection systems based on signatures or statistical anomalies in network traffic. Only by looking in detail at the actual content of communication it would be possible to detect APTs. A method is thus needed to analyse the huge amount of data involved in an effective way.

SpySpot proposes a solution which combines deep packet analysis with visualization of the analysis results enabling an end user to easily spot anomalies created by APTs such as digital espionage. While automated analysis is needed to manage the huge amount of data, no automatic method can match the ability of the human mind in recognizing deviations and evaluating these. It is thus important to integrate automated analysis with visualization of results for human-based evaluation, allowing the user to interactively potentially harmful anomalies, get more in-depth information, tweak the analysis based on experience, and provide feedback on the discovered anomalies, such as discarding harmless ones in future traffic.

Contact: Prof.dr. S. Etalle (Technische Universiteit Eindhoven)
Partners: SecurityMatters, SynerScope, TNO, AIVD

Existing short term research: CyberDEW - A Distributed Early Warning System for Cyber Security

This project develops a system for malware detection, called CyberDEW, that combines data from multiple intrusion detectors, uses information from other sources (e.g. CERT alerts) and interrelate these through automatic reasoning processes. This combination (fusion) of heterogeneous information makes attacks visible that previously stayed "under the radar". The innovation consists of the use of multiple types of information, in which the relationship between these types of information is defined by means of causal models.

Contact: Thales Nederland B.V. Huizen
Partners: Hogeschool Rotterdam and WODC

Existing short term research: Realtime monitoring and Adaptieve Cyber Intelligence

This project intends to enhance BusinessForensics' existing platform for real-time analytics, monitoring, and investigation to be used for cyber security in the public sector, notably Defence. The vision is to develop an integrated detection and ranking environment based on advanced human-machine interaction. The solution will combine profiling, new Machine Learning algorithms, man-machine interaction and include business context to alerts.

Contact: Business Forensics
Partners: TNO, Texar Data Science, TU Delft, Microsoft, Waternet

1.3.1 Example Research Questions

Short term research questions

- How can we detect information leakage without the need of experts, both at corporate level and for individual citizens?
- How can we assess and quantify the severity of data leakages?
- What methods and tools (e.gv˙ isualisation techniques, modelling & simulation) can improve the efficiency and effectiveness of a Security Operation Centre?

Long term research questions

- How can we support effective misuse detection and situational awareness in complex systems (M2M systems, smart grids, systems of systems, . . .).
- How can we provide a frameworks that supports the three phases of incident response: misuse detection, attack containment and forensics?
- How can we rapidly share information about incidents while guaranteeing data confidentiality?
- How can we make (time-critical) ICT-based critical infrastructures more reliable by means of autonomous and dynamic cyber-attack mitigation and recovery?

1.4 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.

Possible research topics	Disciplines
• Digital Forensics Techniques and Tools • Digital Forensics Process & Procedures • Digital Forensics & Law • Handheld Device & Multimedia Forensics • Cloud Computing forensics • Methods for Attributing Malicious Cyber Activity • Visualization for Forensics • Incident Response Procedures and Methods • Incident Response Reporting Formats and Standardization • Tools supporting Incident Response • Simulations environments for training • Incident Analysis • CERTs/CSIRTs • Incident information sharing • Communication with (potential) victims • Research investigating the effectiveness of active interventions vs. (passive) forensics (e.g. in the case of botnets) • . . .	• Computer science • Computer forensics • Criminal law • Cryptography • Data mining • Digital watermarking • Financial forensics • Organisation & Management • Policy studies • Scientific visualization • . . .

Existing long term research: Learning Extended State Machines for MalwareAnalysis (LEMMA)

A central challenge in detecting and analyzing malicious behaviour on computer networks, e.g. due to intrusions or botnet infections, is how to make sense of the vast amounts of data generated in monitoring such systems. The LEMMA project will develop automated tools that can learn models from such data sets that can then be used to analyze patterns in the traffic of large and distributed networks, in order to detect suspicious activity, to locate infections, and to develop behavioural fingerprints of malicious (or normal) traffic.

The project tackles this by combining three innovations in learning technology: 1. automated learning methods for learning timed state machine models with parameters, 2. methods for learning these models from large amounts of streaming data, and 3. fusion of information contained in models learned at different network locations.

The consortium combines expertise in states machine learning at Radboud University, expertise in information fusion at Thales, and a vast experience in analyzing network traffic at Madison-Gurkha, Thales, and NCSC. The research is centred around two main representative case studies; additional use cases are available from end-users SURFnet and the WODC at the Ministry of Security and Justice.

Contact: Prof.dr. F.W. Vaandrager (Radboud Universiteit Nijmegen)
Partners: Thales (TRT-NL/D-CIS lab), Madison Gurkha, NCSC, WODC (Wetenschappelijk Onderzoek- en Documentatiecentrum at Min. V&J), SURFnet, Polytechnic University of Catalonia, University of Texas

Existing short term research: Operating System Computer Memory Analysis (Mammal)

Computer memory frequently contains information useful for digital investigation. This information may include open network connections, active processes, crypto keys and command line details. The main focus in memory analysis has been on operating systems and kernel memory. Although there has been prior research regarding support for Windows, Linux and Android operating systems, there are a number of challenges to tackle.

The project objective is focusing on tool automation, flexible support, research regarding memory artefacts, and the analysis of application behaviour. This effort build on a memory analysis Java library, named Mammal, developed by the Netherlands Forensic Institute which will address the relevant areas above to advance memory analysis.

Contact: dr. Zeno J.M.H. Geradts (NFI)

1.4.1 Example Research Questions

Short term research questions

- Develop a trustworthy way for a bank to communicate with its clients after an incident (when the clients may no longer trust email and phones).
- What is a reliable way to estimate the damage due to an incident?
- How can we efficiently and reliably analyse the large amount of IP traffic data from lawful interception (e.g. smart phones)?
- What techniques and tools can be used to do forensic analysis on big data?
- How to do incident response for an ICT infrastructure compromised by an Advance Persistent Threat (APT)?

Long term research questions

- How can we perform sound forensics on the huge amounts of data stored in different locations that may be hard to physically access (e.g. Clouds, remote servers, etc.)?
- How to establish reliable forensic evidence from public sources on the Internet (e.g. forums, social media, chats)?
- How to manage large scale cyber security incidents with societal impact (i.e. cross-organisation, cross-border)?

- What is the role of the human security operator in automated cyber security incident response and how to best facilitate the operator in this role?
- How can we watermark bulk data (databases, multimedia) in such a way that stolen or leaked data can be traced?
- How can we forensically discover when (corporate) data is leaked to unauthorized entities?

1.5 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.

Possible research topics	Disciplines
• Data access management techniques • Access control models & design methodology • Data policy definition and enforcement • Data policy languages and their semantics • Security policy translation and matching • Audit techniques • Multi-level security: MLS, MILS • . . .	• Computer science • Cryptography • ICT Law • Organisation & Management • Policy studies • Software engineering • System engineering • . . .

Existing long term research: Privacy Compliance and Enforcement (PriCE)

Data protection legislation in the EU empowers users to control the access and usage of their data and imposes stringent requirements on the collection, processing and disclosure of personal data.

Furthermore, nowadays IT systems operate in unpredictable environments, where different individuals access services and devices in different capacities. In contrast, the current security and data protection mechanisms are very rigid. The basic notion of enforcement relies on the idea that infringements (e.g. deviations from policies and procedures) are violations and as such should not be permitted. Moreover, current security mechanisms neglect the existence of business processes and do not take advantage of the opportunity to analyze the event logs and business processes to support the IT system in the security decision-making process.

This project aims to develop the foundations of a novel approach that empowers users to control their data and enables organizations to comply with user policies and with legal requirements. This will be achieved by defining: (1) a user-centric system in which users can specify security and privacy policies that regulate the access and usage of their data and in which they are fully aware of the consequences and risks of the specified policies in terms of security, privacy and accountability; (2) cryptographic protocols and mechanisms that can keep the data persistently encrypted, while still ensuring data availability; (3) a flexible infrastructure for infringement identification and management; (4) a policy learning mechanism for policy refinement.

Contact: Prof.dr.ir. W.M.P. van der Aalst
(Technische Universiteit Eindhoven)
Partners: AMC, Philips Electronics, UvA

Existing short term research: Secure Information Grid

This project targets the development of a Secure Information Grid. This is an information system that is not dependent on a central server, but scales with the number of users and is insensitive to failures of subsystems. Through the use of cryptography both the integrity of the system as well as the authenticity and authorization of users will be enforced. The result is a decentralized information system in which there is no central responsibility for the assurance of security. No one within the network needs to be trusted. Secure Information Grid improves security and reliability of the IT infrastructure.

Contact: Coblue Cybersecurity B.V.

1.5.1 Example Research Questions

Short term research questions

- How to securely setup a privacy-preserving but auditable distributed information system (e.g. for electronic patient records in an EPD)?
- What techniques and tools can be used to make access decision transparent to policy makers when access to data is regulated by different authorities?
- How can we assess and quantify the diversity in privacy policies?
- What are understandable and manageable access policies for end users?

Long term research questions

- How can we empower users to control access to and usage to their personal information?
- How can we protect information owned by different entities (e.g. genetic data) taking into account the policies authored by each owner?
- How to balance fast access to (say, medical) data and security to protect the integrity and privacy?
- How can we assess anonymization or pseudonymization techniques?

1.6 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.

Possible research topics	Disciplines
• Understanding cybercrime techniques and modus operandi • Cybercriminal behaviour • Cybercrime economics • Criminal law & cybercrime • Geographical aspects of cybercrime • Legal, political, social and psychological aspects of cybercrime • Cross-jurisdictional collaboration • Law enforcement tactics • Methodologies to counter or frustrate cybercrime (preventive, judiciary, technical, counterintelligence) • …	• Computer science • Criminal, ICT, and International law • Criminology • Economics • Policy studies • Psychology • …

Existing long term research: Cybercrime Offender Profiling: The Human Factor Examined

Research on the human factor in cybercrime has not kept pace with research and innovation regarding its technological dimensions. Yet, while the latter may be able to defuse a threat, they do little to tackle its causes. Like any type of crime, understanding the causes of cybercrime requires insight into offender motivations, personality, social networks, and the development of criminal careers. To date, very little research has ventured into these aspects leading our knowledge of the field to be strewn with questions rather than answers. The proposed project addresses this gap by applying established insights from criminological research to shed new light on the human factor in cybercrime. In doing so, it identifies profiles of key individual-level correlates, with a view on developing more effective cybercrime policy and better targeted interventions. The project combines the analysis of data from multiple sources: police and public prosecutor's registration data, data on offender characteristics from the Dutch Probation Service, and primary survey and interview data that will specifically be collected for the project.

Contact: Mr.dr. J.L. van Gelder (Nederlands Studiecentrum Criminaliteit en Rechtshandhaving)
Partners: KLPD, Openbaar Ministerie, Dutch Probation Service

1.6.1 Example Research Questions

Short term research questions

- What is a reliable assessment of the damage due to cybercrime?
- Is there a strong link between organized cybercrime and "regular" organized crime, or are these two separate worlds?
- What are the trends in the underground economy? For instance, is Bitcoin becoming popular at the expense of Webmoney, are dropzones mostly located in specific countries, how are money mules recruited, etc?
- How do the criminal laws and law enforcement with respect to cybercrime differ per country? In particular, how do they differ to countries known as origin of cybercrime.

Long term research questions

- Is a strong emphasis on repression of the underground economy (a focus on punishment) effective as a means to reduce it?
- What (inter-)dependencies exist in financial infrastructures used by cybercrime and can they be taken out to disrupt the activities?
- What makes a person engage in cybercrime and what are effective policies to prevent this from happening?
- What are the technical and legal possibilities for pro-active police investigation of cybercrime?

1.7 Risk Management, Economics, and Regulation

The focus of this research theme is on improving risk management, better understanding the economics of cyber security, and what the role of government(s) both in national and international context should be in cyber security. Ultimately, good risk management should provide the basis for allocating resources to improve cyber security 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.

Possible research topics	Disciplines
• Risk assessment and analysis methods • Risk management in complex value chains • Security models and metrics • Security economics • Behavioural & psychological aspects security and privacy • Government policies on Cyber Security • Legal and regulatory frameworks (national, EU, and international) • Effective means to increase security and awareness • (International) law • . . .	• Actuarial science • Computer science • Economics • ICT and International law • Organisation & Management • Policy studies • Psychology • Risk management • . . .

Existing long term research: The personal information security assistant (PISA)

The growing dependence of society on ICT has increased information security risks. PISA attempts to improve this by focusing on end-users. First, they are the weakest link, as they lack resources and expertise that enterprises have. By strengthening them we remove a large vulnerability in society. Second, they are early adopters of technology and drive change bottom-up.

Our approach is to help end-users perform risk management. This is an iterative process of defining goals, examining the threats against them, deciding how to act on them, and actually implementing these actions. Risk management is commonplace in enterprises, with demonstrated effectiveness, but it is too complex for end-users. We will simplify it, creating a lightweight risk management process that is usable by end-users. For this we will (1) develop a simple but expressive risk ontology to represent risks. We will also (2) develop a repository of end-user risks, and (3) design a secure tool that can answer questions about the end-users' risks (for example of online social networks) and suggest actions to reduce these together with their cost. We will (4) perform experiments with prototypes on test subjects, to test prototypes, usability, persuasiveness and effectiveness in reducing risks. Finally we will (5) use the knowledge gained in these experiments to create one end-user risk management method that can be standardized.

Contact: Prof.dr. R.J. Wieringa (Universiteit Twente)
Partners: KPN, XS4All, CSC IT consultancy, Hyves.nl, ITUnited

Existing long term research: Reputation Metrics Design to Improve Intermediary Incentives for Security

The past decade has highlighted that cyber security failures are not only the result of technological vulnerabilities but also of misaligned economic incentives. Improving the incentives for security, the forces that shape the security decisions of market players, is therefore a key challenge. It is especially urgent for Internet intermediaries, which are increasingly recognized as critical nodes for cyber security. These include ISPs, hosting providers, registrars, certification authorities and cloud service providers.

While these Internet intermediaries are critical to cyber security, it is difficult for businesses, consumers, regulators and even the intermediaries themselves to reliably assess how well they perform. Who knows, for example, which Dutch ISP is most effective in mitigating botnets? Such information asymmetries severely impede the functioning of markets and weaken the intermediaries' incentives to invest in security.

This project aims to reduce this information asymmetry by developing empirical reputation metrics for the security of Internet intermediaries. It builds on recent innovations which extracted such metrics for ISPs from data being collected by third parties for incident response and situational awareness.

This research project had a pre-cursor in short-term contract research for the Ministry of Economic Affairs where researchers at Faculty of Technology, Policy and Management of the TU Delft carried out a fact-finding study on the problem of botnet infections in the Netherlands and the role of ISPs in mitigating this problem, to provide hard data as a solid basis for recommendations for government policies and ISP practices [4].

Contact: Prof.dr. M.J.G. van Eeten (Technische Universiteit Delft)
Partners: NCSC, SIDN

1.7.1 Example Research Questions

Short term research questions

- How to balance the economic costs, security costs and privacy costs?
- Which national interests can affected by a cyber security incidents and to what extend? Which developments are expected?
- What events or what activities can damage (national) ICT interests, who are the actors, what tools do they use and what developments are expected?
- How to do risk management for systems-of-systems with complex multi-stakeholder situations?

Long term research questions

- How to collect incident data in a systematic approach and identify relevant indicators for the cyber security status at different levels (company, sector, country)?
- What is the role and the most effective way for government to improve cyber security? Should it aim to impose standards, reduce information asymmetries, or combat security externalities, and which ones?

1.8 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.

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.

Possible research topics	Disciplines
• Security engineering principles and methods • Security by Design & Privacy by Design • Secure coding techniques • Security protocol analysis • Security testing and verification tools • Security assurance and certification methodologies • Economics of secure software engineering • Usable security • Impact of outsourcing • Liability • Design and engineering of secure systems of systems • Security lifecycle management • Continuity and integrity of services in the Internet value chain • . . .	• Computer science • Cryptography • Economics • ICT Law • Microelectronics • Software engineering • System engineering • Software & hardware certification • . . .

Existing long term research: Opening backdoors on embedded devices (OpenSesame)

Networked embedded devices such as routers, switches, firewalls, sensors and actuators are part of our critical infrastructure. These devices are often assembled and programmed overseas – beyond our control – and placed within our trusted networks or even used for military applications. But can we really trust them? There have been several incidents where backdoors have been found in the firmware (also on silicon) of these devices. Such a backdoor allows an adversary to gain (remote) access to the device.

OpenSesame addresses this problem by developing novel automated techniques to test the software and firmware of embedded devices for the presence of such backdoors. Standard protocol fuzzing techniques, such as feeding programs invalid or random data to test for unexpected behaviour, are not very effective as the chances of hitting the right input are tiny. Our approach consists of first recovering the (read-protected) firmware from the device. Having access to the firmware enables us to apply smarter techniques, such as symbolic execution, to detect the presence of backdoors in any possible execution path. This technique does not scale very well when addressing large computer programs. However, embedded devices with their smaller code bases are exactly the right target for symbolic execution.

Contact: Prof.dr. B.P.F. Jacobs (Radboud Universiteit Nijmegen)
Partners: VU, NFI, AIVD

Existing long term research: Profiling for Optical Fault Induction using Locationdependent leakage

We increasingly rely on embedded security systems in our lives, such as smart cards and RFID tags for public transport, banking, passports and ID cards, access control, and pay-TV systems. Ensuring the security and privacy requirements of these systems is a challenging problem, as witnessed by the breaking of the cryptosystems used in mobile phones, car keys, and RIFD card such as the 'OV-chipkaart'.

This project focuses on physical attacks, the main threat to the security of embedded security devices. In such attacks information about some physical (so-called side-channel) leakages, e.g. power consumption data is collected and analyzed by an adversary to retrieve secret keys of the device. More in particular, the project investigates fault injections, which are an extremely powerful tool for an attacker to extract data from devices, and the use EMA and optical emissions to guide fault injection attacks. Techniques for these attacks and proposed counter-measures will be verified in practice in collaboration with security evaluation lab Riscure.

Internationally, this project collaborates with partners across the EU in COST action IC1204, 'Trustworthy Manufacturing and Utilization of Secure Devices' funded by the ESF (European Science Foundation).

Contact: Dr. L. Batina (Radboud Universiteit Nijmegen)
Partner: Riscure

Existing short term research: Cyber Security: by design or by accident?

The project addressed the need to integrate cyber security into the design and development lifecycle of software systems. It aims to develop a prototype toolkit for the technical inspection of architecture and source code of large software systems, and develop a model that provide controls and procedures in the development life cycle, and an associated model for risk management based of a categorisation of risks.

Contact: Software Improvement Group B.V.
Partner: Radboud Universiteit Nijmegen

1.8.1 Example Research Questions

Short term research questions

- How to set up a cost effective secure software development process for SMEs?
- How can we assess the security of the software that we use today? Or a particular types of software, say web-applications?
- What is technically possible in the short term to improve the security of mobile devices that employees use professionally in the practice of Bring-Your-Own-Device (BYOD)?

Long term research questions

- How to secure automatic & cooperative driving solutions (incl. vehicle-to-vehicle and vehicle-to-infrastructure)?
- How can we establish a life-cycle wide security assurance for hardware and software products?

- What methodologies could be used to certify the security of software or hardware, at various levels of rigour (and cost)?
- Can we develop more secure computing platforms, using Trusted Execution Environments and micro-kernel/hypervisor solutions?

1.9 Offensive Cyber-Capacities

Operational cyber capabilities are becoming essential for defence organisations, 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.

Possible research topics	Disciplines
• Reliable and stealthy attack techniques • Offensive countermeasures • Cyber intelligence gathering methods and techniques • Legal and ethical aspects of offensive cyber capacities and striking back • Procedures and command structures for of cyber force • Training capabilities for offensive cyber missions/serious gaming • Damage assessment (including collateral damage) • Integrated cyber and traditional offensive measures • Command & control and governance of offensive cyber • Ethical and legal considerations • . . .	• Computer science • Criminal, ICT, and International law • Law enforcement • Military law • Military strategy • Organisation & Management • . . .

1.9.1 Example Research Questions

Short term research questions

- What are the current laws and regulations that govern the use of military cyberforce against a foreign target?
- How do we assess (collateral) damage due to a cyber-attack?
- How can law enforcement agencies and/or the military obtain (develop/purchase) offensive technology?
- To what extent do the offensive capabilities comply with national law and international agreements and conventions (including EU directives, and the European Convention on Human Rights)?

Long term research questions

- What are the wider-ranging consequences as governments enter the market for offensive technologies?
- What should be the proper governance and command structure for deploying military cyber force?
- What criminal activities could be reduced by offensive measures and will the effects be short-term or long-term?

2 Other research programs, roadmaps and agenda's

This section briefly describes the link between the NCSRA II and other programs, roadmaps and agenda's.

2.1 National Level

In its Top Sector policy, the Dutch government focuses on innovation through close cooperation between knowledge institutions and public and private organizations in Public Private Partnerships in nine economic top sectors for growth that have been identified. At least two top sectors, High Tech Systems and Materials (HTSM) and Energy, directly deal with cyber security, as does the Roadmap ICT for the top sectors (2012) that cuts across all Dutch top sectors.

- **Roadmap HTSM Security**
  The *Roadmap HTSM Security*[3] defines the following areas of application and technological challenges: System of Systems, Cyber Security, and Sensors. For the area of Cyber Security the HTSM Security Roadmap explicitly refers to the NCSRA. The challenges outlined in the area Cyber Security include protection of our vital ICT infrastructure and combatting cybercrime. With respect to System of Systems, the roadmap highlights security-by-design, data-protection-by-design and privacy-by-design as are important issues.

- **Roadmap ICT for the Top Sectors**
  The *Roadmap ICT for the Top Sectors*[4] makes it clear that ICT is the key driver of innovation in many sectors of our economy and is important for all top sectors. Cyber security is particularly relevant to the theme *ICT one can rely on*, one of the four ICT themes described in the ICT Roadmap. This theme focuses on making ICT secure, vital, and private, and defines action lines *secure and vital ICT* and *privacy and e-identity*. The Roadmap ICT recognizes the need for multidisciplinary research in a range of topics: identity, privacy and trust management, malware, forensics, data management, cybercrime, risk management, and secure design. Like the Roadmap HTSM Security, the ICT roadmap refers to the NCSRA as the agenda for cyber security research.

3 http://www.htsm.nl/Innovatie/Roadmaps/Security

4 http://www.htsm.nl/Innovatie/Roadmaps/ICT

2.2 International Level

Cyber security is not a national issue. For Dutch knowledge institutes, collaborating internationally is already a matter of course: in addition to the regular EU FP7 projects in the field of cyber security, Dutch universities are participating in EU networking initiatives such as ICT-FORWARD[5] , SYSSEC[6] (European Network of Excellence in the field of Systems Security), E- CRYPT[7] (European Network of Excellence in Cryptology), and NeSSoS[8] (European Network of Excellence on Engineering Secure Future Internet Software Services and Systems).

Major research initiatives and agendas in Europe and the US, and their relation to the NCSRA II, are discusssed below.

- **Cybersecurity Strategy of the European Union**
  The 2013 *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* [1] articulates five strategic priorities:

  1. Achieving cyber resilience,
  2. Drastically reducing cybercrime,
  3. Developing cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP),
  4. Develop the industrial and technological resources for cybersecurity, and
  5. Establish a coherent international cyberspace policy for the European Union and promote core EU values.

  For each priority the strategy proposes specific actions. Particularly for developing industrial and technological resources for cybersecurity, the strategy defines action to foster R&D investments and innovation.

  The NCSRA clearly contributes to the first four of the priorities above; the last priority is somewhat out of scope for a national research agenda. Moreover, the Cybersecurity Strategy of the EU several times stresses the need to foster closer collaboration between the research and academic communities and the private and public sectors, and the NWO Cybersecurity research programme has been set-up to stimulate this.

5 http://www.ict-forward.eu
6 http://www.syssec-project.eu
7 http://www.ecrypt.eu.org
8 http://www.nessos-project.eu

- **Horizon 2020**
  At the time of writing the work programmes for Horizon 2020 (H2020) have not been published. However, the proposal for the decision by the Council of the European Union [3] for establishing the Specific Programme implementing Horizon 2020 has been published and contains specific objectives with respect to cyber security. In particular, as part of the pillar *Societal Challenges*, the objective *Improve Cyber Security* has been defined for the challenge *Protecting Freedom And Security Of Europe And Its Citizens*. Within this objective H2020 will support research and innovation to help prevent, detect and manage in real-time cyber-attacks across multiple domains and jurisdictions, and to protect critical ICT infrastructures. It is emphasized that digital society is in full development and that this requires new type of research to quickly react on new contemporary developments. Also the need to the protection of children is emphasized, as they are highly vulnerable to the emerging forms of cybercrime and abuse.

  In addition to the objective *Improve Cyber Security*, other objectives relevant in the context of cyber security are the objectives *Fight crime, illegal trafficking and terrorism, including understanding and tackling terrorist ideas and beliefs and Ensure privacy and freedom, including in the Internet and enhancing the societal legal and ethical understanding of all areas of security, risk and management*. The latter for instance refers to privacy-by-design.

  Furthermore, within the *Industrial Leadership* pillar H2020 will support privacy and security research related to emerging ICT technologies (e.g. Internet of Things, Future Internet, and next generation computing).

  In the Horizon 2020 consultation process the IIP Veilig Verbonden, which includes the editors of this document, has provided input based on the NCSRA.

- **US initiatives by the Department of Homeland Security**
  The Cyber Security Division of the US Department of Homeland Security has published a detailed research and development agenda [2]. This agenda lists 11 hard problem areas in cybersecurity:

  1. Scalable trustworthy systems (including system architectures and requisite development methodology),

2. Enterprise-level metrics (including measures of overall system trustworthiness),
3. System evaluation life cycle (including approaches for sufficient assurance),
4. Combatting insider threats,
5. Combatting malware and botnets,
6. Global-scale identity management,
7. Survivability of time-critical systems,
8. Situational understanding and attack attribution,
9. Provenance (relating to information, systems, and hardware),
10. Privacy-aware security,
11. Usable security.

Although the classification and sub-division is different, this list of problem areas by DHS and the research themes in the NCSRA II cover the same ground, except that legal issues, which are explicitly considered in the NCSRA II, do not feature in the list of DHS problem areas. Additional documents from DHS, including roadmaps for more specific sectors, are available from http://www.cyber.st.dhs.gov/resources.

- **UK initiatives**
  Reflecting the aims of the National Cyber Security programme in the UK, there has been a concerted effort in the UK to increase the academic capability in all fields of cyber security, led by GCHQ[9] . Here cyber security research has been classified into the following areas:

1. Cryptography, key management and related protocols,
2. Information risk management,
3. Systems engineering and security analysis,
4. Information assurance methodologies,
5. Operational assurance techniques,
6. Security of strategic technologies and products,
7. Science of cyber security and human factors, and
8. Building trusted and trustworthy systems.

This classification covers similar themes as the NCSRA II, except that it does not explicitly mention research into cybercrime, the underground economy, or indeed legal issues.

9 http://www.gchq.gov.uk/press/pages/cyber-security-research-centres-of-excellence.aspx

References

1 Council of the European Union. Proposal for a Council decision establishing the Specific Programme implementing Horizon 2020 - The Framework Programme for Research and Innovation (2014-2020), December 2012. Available from http://register.consilium.europa.eu/pdf/en/12/st17/st17029.en12.pdf.

2 European Commission. Cybersecurity strategy of the European Union: An open, safe and secure cyberspace, February 2013. Available from ec.europa.eu/information_society/ newsroom/cf/dae/document.cfm?doc_id=16%67.

3 US Department of Homeland Security. A roadmap for cybersecurity research. Available from http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf, 2009.

4 M.J.G. van Eeten, H. Asghari, J. M. Bauer, and S. Tabatabaie. Internet service providers and botnet mitigation: A fact-finding study on the Dutch market, 2011. Report prepared for the Netherlands Ministry of Economic Affairs, Agriculture and Innovation. Available at http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/01/13/internet-service-providers-and-botnet-mitigation.html.

Figure 6: Field consultations resulted in this wordle. Suggestions have led to various text improvements and additional possible research topics. Thanks to all individuals and organizations who shared their thoughts with the editors like, the Embedded Systems Institute (ESI), the Netherlands Forensic Institute (NFI), the Information Sharing and Analysis Centers (ISACs), the Openbaar Ministerie, De Nederlandsche Bank, the National Police, and more.

Colophon

Editors
prof.dr.ir. Herbert Bos
prof.dr. Sandro Etalle
ir. Frank Fransen
dr.ir. Erik Poll

Coordination
Field consultation

dr. Dick Brandt
drs. Jan Piet Barthel

Production
drs. Juul Brouwers

Design
Smidswater

Print
Albani Den Haag

Financers NCSRA II

NWO
Netherlands Organisation for Scientific Research

Government of the Netherlands