Information Security – trends 2015

A Swedish perspective

Publication MSB851 - May 2015
ISBN 978-91-7383-572-5

Preface

The development of information technology creates national and global challenges and new opportunities. It is a development that challenges many traditional ideas and has resulted in new forms of interaction between people. These changes also make society more vulnerable, entailing huge challenges for security.

The Swedish Defence Commission notes in its 2013 report, *Choices in a globalised world* (Ds 2013:33), that the vulnerabilities arising in today's global IT system are, and for the foreseeable future will continue to be, one of our most complex issues. The Swedish Defence Commission emphasises in its 2014 report *The Defence of Sweden* (Ds 2014:20) that there is a continuing need to evaluate possibilities for further strengthening the robustness of IT in society and to analyse the need for developing cyber capabilities. In the report submitted by the Swedish National Audit Office (RiR 2014:23) the picture of the challenges facing society becomes even clearer.

This increasingly unpredictable and complex development emphasises the need for an operational and comprehensive analysis of international developments. The Swedish Armed Forces, the National Defence Radio Establishment, the Swedish Civil Contingencies Agency and the Swedish National Bureau of Investigation have jointly produced this trend report as a foundation for supporting further information security work, much needed in all parts of society. We hope that it will offer a rewarding reading experience and useful support to everyone working with information and cyber-security in Sweden.

Stockholm, 10/01/2015

Mattias Hanson, *Head of Security Division, Military Intelligence and Security Service, Swedish Armed Forces*

Tuve Johansson, *Head of IT Crime Investigation Section, National Operations Department, Swedish Police Authority*

Charlotte Lindgren, *Director of Cyber Division at the Swedish National Defence Radio Establishment*

Richard Oehme, *Director of Office of Information Assurance and Cybersecurity, Swedish Civil Contingencies Agency*

Table of Contents

Summary

The report addresses seven trend areas. Within each of these, three main items have been identified and are delineated below. Taken together, the items give an overall picture of the situation in the information security field.

1. Strategic decisions on information security are always taken in a context where security is weighed against other values. The following bullet points are important for decision-makers to reflect on:
    - In the future, information security will increasingly be considered a matter of protecting society and its prosperity as a whole, rather than just a matter of technology.
    - It is becoming an increasingly important challenge to shape practices and laws so that good information security becomes an advantage rather than a disadvantage in the global competition.
    - The development of software and services places high demands on both procurement skills and security awareness with the procuring party in order to achieve a sufficient level of security.

2. IT services in modern enterprises are often complex and distributed, both physically and organisationally. This has consequences for security:
    - As data from organisations pass through many different jurisdictions and technical systems, risks become more difficult to assess and cross-dependencies become harder to see.
    - Compliance with, for instance, the requirements of the Personal Data Act will place increasingly high demands on the procurement skills of the public sector.
    - It is becoming increasingly common to use continuous monitoring and responsive measures rather than preventive protection.

3. More information about ourselves and our technical solutions become available to the public. Three key factors for understanding the consequences of this are the following:
    - Questions of privacy become all the more relevant when greater amounts and more types of data become available in modern society.
    - The increased sharing of information means increased uncertainty about who owns data.

- Rapid technological development makes statutes and regulations on the electronic exchange of information between government agencies obsolete, making both desirable systems integration and the protection of privacy more difficult.

4. In recent years, the geopolitical dimension of information security has grown. A few key observations are the following:
   - Information operations where internet-based propaganda is combined with diplomacy, lies, media gambits and traditional military activities have become commonplace in armed conflicts.
   - Cyber espionage and cyber sabotage are part of the "security policy toolbox" in an increasing number of countries.
   - Increased opportunities for free and uncontrollable communication via the internet has resulted in backlashes in many states, with attempts to isolate their national networks from the internet.

5. In modern society, virtually all crime has an IT connection. The following items summarise trends in this area:
   - Today's IT-related organised crime generally has financial incentives, and an internet-based criminal service sector, *crime-as-a-service*, has emerged in recent years.
   - The interaction between traditional and electronic crime is increasing and is becoming increasingly complex.
   - Today's crime places new demands on the judicial system, not least in terms of interaction with foreign police forces and private sector.

6. There is a constant race between attackers and defenders. A few trends well worth drawing attention to are the following:
   - Software that identifies vulnerabilities and simple and inexpensive technical tools for attacks have lowered the threshold and put tools in the hands of more attackers. At the same time, the most advanced attack tools are still hard currency, reserved for a select few.
   - Despite technical vulnerabilities, the weakest link is often the human in the system, who can be fooled into downloading malware or disclosing sensitive information.
   - Even though more and more organisations introduce regulations for information security, the step from regulations to real security is a long one.

7. As society becomes ever more dependent on technical systems, these must be robust. Important aspects of this are the following:

- In modern society, the consequences of information systems outages are becoming greater and more difficult to grasp.
- Risk management and continuity planning are becoming increasingly important in order to achieve robust information systems, as is proper understanding of the increasingly complex dependence of business operations on IT.
- The market for cyber insurance is in its infancy, but will grow in the future.

1. Introduction

This trend report has been drawn up to provide an easily accessible overall picture of the situation in the information and cyber security field, and to give an overall assessment of conditions that are particularly urgent for decision-makers in society. The assessment is mainly based on developments in 2013 and 2014.

Participating bodies in the production of the trend report were the Swedish Civil Contingencies Agency (MSB), The National Defence Radio Establishment (FRA), the Police and the Swedish Armed Forces, together with support from the Swedish Defence Research Agency (FOI). The contents of the trend report have been compiled based on the knowledge and the continuous analyses of each participant.

The report covers national and international trends. In this report, trends refer to stable, long-term changes in the information security field that are assessed to affect society in some way and which have been identified by the participating government agencies. In some cases trend extrapolations are presented, but since the area is relatively new there is often a shortage of statistical indicators with long time series, making it difficult to predict future developments.

The report has a broad approach and covers many kinds of threats and risks. Depending on the context, the attackers who are mentioned range from very competent state actors with large and specialised resources, through organised crime, where attack tools are bought and sold on black markets, to less qualified "hacktivists" or even dissatisfied teenagers who do not really understand the consequences of their actions. In addition, the report discusses threats and risks which are not the results of attacks, but rather result from mistakes and inadequate risk management in organisations.

The trends presented in the report have been identified in collaboration with representatives from the participating government agencies. The information has then been supplemented using other sources, such as media coverage, scientific literature, a selection of interviews and official publications. The text has been edited in several iterations and representatives from the participating agencies have been asked to submit comments and feedback.

The report contains a large number of references to allow further reading for those interested. Many of the sources are scientific publications which have undergone *peer review*. The methodology discussions in these are invaluable when assessing the results reported. These resources are also of interest since it is of great importance to systematically develop sources such as statistics on information security.

The report addresses seven trend areas. Their order does not reflect priorities: the report does not take a position on whether some of the challenges, threats or risks are larger than others. Each chapter begins with three main bullet points which summarise the most important messages.

2. Information security - a trade-off with other values

- In the future, information security will increasingly be considered a matter of protecting society and its prosperity as a whole, rather than just a matter of technology.
- It is becoming an increasingly important challenge to shape practices and laws so that good information security becomes an advantage rather than a disadvantage in the global competition.
- The development of software and services places high demands on both procurement skills and security awareness with the procuring party in order to achieve a sufficient level of security.

Information technology has changed modern society and has become an indispensable part of it. We now work, pay bills, amuse ourselves and socialise using computers and the internet in a way that was difficult to imagine ten or fifteen years ago. Organisations such as the EU and the OECD (Organization for Economic Co-operation and Development) agree that the new digital economy will play an increasingly important role for future growth and prosperity [1], [2]. Such a development certainly puts increased demands on security - but also makes the meaning of security more complex. Information security is no longer just a special interest for those interested in technology. Decision-makers will increasingly have to deal with conflicting goals, where information security is weighed against other values and where there are no easy solutions. A leitmotif in this chapter is that issues of governance are complex and require both involvement and strategic decisions at the highest level.

2.1 Information security to protect society and its prosperity

The OECD decided in December 2013 to revise its guidelines on information security, which had not been changed since 2002 [2]. In this decade-long perspective, long-term trends become clear: IT drives innovations, economic and social development, but it is also an infrastructure that is critical for the functioning of modern society. Threats also change constantly. This has caused a large number of countries, though not Sweden yet, to adopt national strategies for cyber security and related issues. The most important change in the revised OECD guidelines is the shift of security emphasis from the protection of the digital environment to the protection of economic and social activities which rely on it. Security issues are no longer considered to be only about keeping networks free from viruses or keeping secrets secret; they are vital for society to function, for the competitiveness of the economy and for the very basis of our prosperity.

The Cybersecurity Strategy for the European Union [1] was adopted in 2013. At the same time, work on the Network and Information Security (NIS) directive was initiated, as part of the effort to ensure a high common level of NIS across the union. . The proposed directive requires all Member States to ensure that they have a minimum level of national capability, as well as some capability for international cooperation. The directive will affect public administration and companies within specific critical sectors. As the directive passed the European Parliament, significant amendment proposals were made. The European Commission is now pushing to reach a decision on the Directive as soon as possible.

2.2 The legislator's challenges

The fact that security issues are increasingly about protecting prosperity makes for challenges. Legislation that aims to strengthen security also risks reducing competition and productivity in the economy. In particular, small and medium-sized companies can suffer disproportionately from security rules [3]. Large companies can even turn to legislators with proposals on tough security requirements in order to undermine smaller competitors with less resources. At the same time, smart regulations, such as the EU harmonisation of standards for electronics, simplify the situation for companies and increase trade [4]. Since neither the legislator nor the innovators can know how technology will be used in the future, poorly designed laws can be an obstacle to innovation and growth.

Research has shown that the large effects on growth rarely occur where they are expected – for example, the IBM PC was intended for spreadsheets only, when it was being developed [5]. It is becoming increasingly important to shape practices and laws so that good information security becomes an advantage rather than a disadvantage in the global competition [6].

2.3 Requirements on procurement skills and security awareness

When developing software, security is rarely put first . The focus is on functionality: that the IT service does what it is supposed to do. Security is a *non-functional* quality, and these are often added afterwards, successfully or not.

"Agile methods" have become increasingly common in software development in recent years. These methods are intended to avoid just following a specification established in the beginning, and to work instead with shorter lead times , early deliveries and continuous adaptation of the software to the needs of the customer. This poses new challenges for security [7]:

- Dynamic process changes hinder process security audits
- New solutions and design changes make it difficult to ensure security over time.

- A one-sided focus on functional requirements result in neglected non-functional security requirements .
- A lack of traceability and missing security expert roles in project teams, etc.

While there are also plenty of suggestions on how security can be integrated into agile software development [8], [9], [10], there is still no major empirical study that can answer how security is affected by agile development.

How should security be ensured in future software development? To a large extent, the solution probably lies in increasing the knowledge and awareness of security issues on the purchaser side. Agile methods are often more effective at delivering the software that the customer wants. This means that the customer has a responsibility to demand security. This must now take place throughout the entire development process, regardless of whether it is agile or not. It is not enough to include security in the initial specifications. Close cooperation between system developers and information security experts will probably just become even more important to achieve a good level of security.

3. The complexity of modern IT services

- As data from organisations pass through many different jurisdictions and technical systems, risks become more difficult to assess and cross-dependencies become harder to see.
- Compliance with, for instance, the requirements of the Personal Data Act will place increasingly high demands on the procurement skills of the public sector.
- It is becoming increasingly common to use continuous monitoring and responsive measures rather than preventive protection.

IT continues to become more centralised. Whereas ten years ago, every business had its own system for salaries, warehousing and sales, today such functions are increasingly being outsourced to external suppliers. Sometimes it is just storage and computing capacity that is hired, but increasingly the software itself is also rented, as in software-as-a-service or cloud services. The driving force is the desire on the procuring side to reduce fixed costs - it is far cheaper if one hundred companies share a data centre than if each has its own solution. It is this economic potential which has caused the National Audit Office to criticise government agencies for not examining the question of cost savings and efficiencies through outsourcing, due to strong internal IT departments with low efficiency requirements [11]. Economies of scale make it likely that cloud services are here to stay. The market also becomes progressively more mature, with more and more players and competition between them, which drives the quality of service forward. Outsourcing, however, also puts large demands on the procurer to avoid unwanted risks.

In particular for small players, the transition to externally procured IT can mean that both intrusion protection and operational reliability increase, because the organisation thus gets access to expertise and better technology. This is often the case with private individuals, who put more and more data "in the cloud" and less on home computers without any backup. It is unlikely that a small business owner who sets up his own e-mail service will have better reliability than one of the major advertising-financed "free" services on the internet - although he does keep his own data and does not have his e-mail scanned for advertising purposes. What is best depends on the circumstances. However, you never get more than what you demand and pay for, whether from an outsourced system or one operated in-house.

3.1 Outsourcing can lead to less predictable risks

At the same time, the development towards increased outsourcing inevitably leads to more and more eggs being put in one basket, and the consequences of attacks as well as accidental downtime become more difficult to assess. A customer in a cloud, for example, may have access problems if another customer's activity suddenly grows very quickly. Another possibility is that a Denial-of-service attack (DoS) on one client affects all the others by crashing the entire platform. A related risk is that illegal activities of a single customer affect all other users if a police investigation suddenly forces the cloud provider to close down. A sophisticated attacker could even pose as a customer in a cloud for exactly this purpose, or use their purchasing power to negotiate terms that in some way are detrimental to other customers [12].

This whole range of simple and sophisticated threats and risks must be taken into account in a risk analysis before operations are outsourced to sub-contractors or data is stored in cloud services. In addition, the risk of service provider ownership changes must be factored in, particularly in the context of safeguarding the confidentiality of sensitive information.

The number of possible attack scenarios should not lead us to underestimating the risk of downtime, regardless of whether it is a consequence of an attack or not. The Tieto crash at the end of 2011 is an excellent example of how centralised operations under unfortunate circumstances suddenly can lead to unexpected and unpredictable problems for large and seemingly unrelated parts of society [13]. The complexity of the cloud environment, as well as the fact that nobody has an overview of the dependencies that have arisen, make risk analyses very challenging.

Cloud services illustrate the fact that responsibility is increasingly being spread over a number of organisations, despite the fact that good security requires clarity and cooperation. Security cannot be outsourced; even though the perceived security of a cloud solution may be high, it does not replace the procuring organisation's responsibility or the need for in-house security. A scientific study points out a number of important issues related to dispersed responsibility [14]: Among the most important problems is the difficulty to audit cloud services, coordinating parties and building a common and effective security culture across organisational boundaries. It may also be difficult to localize data, as well as carrying out preventive work and forensic investigations.

Standardized technology and contracts, as well as better follow-up of agreements, are part of the solution to these problems. However, research shows that it may be difficult to act rationally when signing a contract concerning, for instance, availability [15]. Security cannot be completely delegated. Consumers, companies and organisations will probably be central players in this work, and the standards thus developed will possibly become incorporated into legislation only later [16]. The ability to manage security

across organisational and operational boundaries is becoming increasingly important.

3.2 Procurement skills in the public sector

Even though cloud services are here to stay, growth in the use of such services by Swedish municipalities is expected to fall after a number of cases of dubious handling of personal data. The Swedish Data Protection Authority has repeatedly criticised the use of cloud services where agreements have not ensured compliance with the Personal Data Act.

In July 2014 the Administrative Court in Stockholm ruled in favour of the Data Protection Authority in a case where a municipality had appealed because the agreement had allowed the provider too much freedom to process personal data for their own purposes and the municipality was not sufficiently informed about which sub-contractors the provider had employed [17]. The public sector is torn between different requirements, where information systems are expected to be efficient and save money, offer citizens better service and at the same time be secure. At the same time, the coordinated public sector framework agreements drive the development towards consolidated IT services hosted by a small number of players, since the agreements prescribe that all public outsourcing must go to the players who have won the framework agreements.

In the Swedish Legal, Financial and Administrative Services Agency's framework agreement for IT services, aspects of information security are included. The agreement is really more of a template; in fact, the contracting parties can choose what to include in their final agreement. In 2014, the Swedish Civil Contingencies Agency investigated whether and how different parties used the Legal, Financial and Administrative Services Agency's framework agreement. The investigation showed that agreements signed often lacked relevant requirements on information security. On many occasions, the parties had chosen to ignore the possibilities to set requirements. The requirements that were included in agreements concerned singular aspects rather than systematic, risk analysis based, work [18].

Sometimes it is not the agreement which is the problem, but the lack of an agreement. Information systems cooperation between different actors in the public sector is becoming more common, but is often not regulated in agreements. This means that it is not possible to establish accountability through legal process if something should go wrong. The Swedish Civil Contingencies Agency has stated that we must investigate how public sector actors can be allowed to enter into agreements, similar in function to commercial ones, with each other [18]. In its 2009 review of collaboration between agencies in IT investments, the Swedish National Audit Office drew attention to deficiencies in legislation on registers governing agencies' information management, partly due to outdated regulations and incomplete definitions [19]. Given the quick developments in IT investments and

collaboration, there is a substantial risk that the conclusions of the Swedish National Audit Office are still equally relevant today.

3.3 From preventive protection to continuous monitoring

The sheer number of connected devices creates complexity in itself: Cisco predicts that in 2020 there will be 50 billion devices connected to the internet [20]. This is mainly a positive development that streamlines old activities and enables completely new ones: a doctor can monitor patients remotely, household appliances can save power and inexpensive sensors can monitor environmental changes. At the same time, it means that there will be new ways to carry out attacks. What applies to mobile phones and tablets increasingly also applies to washing machines, refrigerators, video conferencing systems, automation in buildings and medical technology.

All connected and poorly protected devices can come under attack by various methods [21]. These could be denial-of-service attacks, either on other connected devices or traditional IT infrastructure such as routers and internet servers. They could also be about accessing sensitive information. Another threat is damage with unpredictable consequences, such as an attack on the frequency stability of the power grid by switching hacked household appliances on and off.

Industrial information and control systems, so-called SCADA systems (Supervisory Control And Data Acquisition), are often constructed using standard components and it is increasingly common that PC platforms and communications solutions are built on standard protocols (TCP/IP). The result is that IT components are increasingly used in more functions, increasing the number of communication channels, and thus attack vectors, in industrial information and control systems [22].

It is also difficult to install anti-virus software: real-time-critical control systems in the SCADA world cannot risk a sudden loss of performance or a reboot when the anti-virus software does something, and a one dollar sensor in the "internet of things" cannot be equipped with for tens of dollars' worth of protection. Large companies in network and data communications have now reached the conclusion that the time when security could be managed in every device is now over [23]. This development puts increasing demands on continuous monitoring of networks and situation awareness in complex architectures [24].

4. Privacy, the information explosion and security

- Questions of privacy become all the more relevant when greater amounts and more types of data become available in modern society.
- The increased sharing of information means increased uncertainty about who owns data.
- Rapid technological development makes statutes and regulations on the electronic exchange of information between government agencies obsolete, making both desirable systems integration and the protection of privacy more difficult.

The amount of electronic data is growing exponentially in modern society. In 2013 it was reported that 90% of all data in the world had been created in the last two years [25] and the trend has accelerated. A major source of data is user-generated content in the form of pictures, videos, status updates and blogs posted on the internet. As the resolution of cameras improves and algorithms become better at identifying people and patterns, surveillance cameras will generate more and more information and human guards become increasingly rare. This information explosion has put privacy on the agenda and resulted in much discussion about who owns the data and how it is used.

4.1 Privacy on the agenda

In July 2012, the Government gave the Swedish Agency for Innovation the commission of developing oppnadata.se, a technical platform for the dissemination of open data. The central idea was simplifying the everyday lives of individuals and entrepreneurs and the efficiency of the public sector through e-services [26]. In February 2014, the government committee of inquiry on PSI (Public Sector Information) presented its final report on how the European PSI Directive, setting minimum rules for the re-use of documents owned by public agencies, would be implemented in Swedish law [27]. Among other things, it proposed measures that would make it easier to use government information to develop new services and products. The study noted, though, that the increased digitization and dissemination of information could entail a risk of undue invasion of privacy. In particular, it expressed concern over the possibility of requesting large amounts of public documents on paper and then scanning them into a machine readable format. All of this suggests that privacy issues will only become more pressing as more types of data become available.

The Swedish debate about the use and abuse of public documents took off in 2014 in connection with the events surrounding Lexbase, an internet service for queries about people who have been heard in Swedish courts. Not only did the

the misleading presentation of the Lexbase contents lead to intense criticism, but the service is also an example of how poorly planned IT solutions can cause unforeseen consequences. Since anyone who was a paying customer could request any information, shortly after its introduction the entire database - complete with personal information - was posted online, with dire consequences for people's privacy and for the company's business model.

4.2 Uncertainty about who owns data

In the wake of the data explosion, there is increased uncertainty about the ownership of data. This applies both to private individuals' ownership of their information and to uncertainties in contractual relationships between companies or government agencies. What constitutes legitimate use, legally and morally, of the vast amounts of data in today's society are topics increasingly being discussed.

In many countries, public information from the authorities is made available on internet, usually with interfaces that are intended to facilitate automatic reading and processing. There is also a market on which government agencies sell data about individuals. One example of this is the Swedish Tax Agency's database, SPAR. A new market has also emerged as companies buy information directly from individuals about what they do on their computers, tablets and smartphones for a monthly payment. Thus, individuals are able to make money from their own data. The market value is due to the high data quality of professionally and voluntarily collected data, but also because traditional banner ads now have less than a 0.01% chance of being clicked. The possibility of smarter marketing makes high quality information about consumer behaviour valuable throughout the marketing value chain [28].

4.3 Transparency and protection of information in public administration

It is a major challenge in the Swedish public administration for all actors to maintain transparency under the Principle of Public Access, as well as protection of privacy under the Personal Data Act. Unfortunately, compromise solutions risk leading to shortcomings in both areas. The long lifespans of both information and information systems do not make it any easier. Technical solutions must work for many years into an uncertain future. There are strong technical and organisational incentives for integrating systems between agencies, but management instruments and regulations for the public sector do not always keep up.

One example of the problem is that the Patient Data Act's provisions regarding confidentiality differ depending on whether the information is exchanged between different care providers or within the same care provider, which has been pointed out by the National Audit Office[29]. In a review of electronic data exchange between different agencies, it was also noted that the rules - usually a combination of the Public Access to Information and Secrecy Act, the Personal Data Act and legislation on the matters concerned - have a complex

structure. All this means that agencies find it difficult to know what information may be exchanged and how electronic exchange of information may take place [30].

In June 2014, the eGovernment Delegation suggested a number of changes in secrecy legislation, partly to facilitate cooperation between agencies and partly to provide better service and protection for those who use e-services. If an agency is going to outsource IT operations to another agency, the same secrecy must apply on both the providing and procuring sides. To avoid any gaps in secrecy, a regulation is proposed for the transfer of applicable secrecy [31].

From a security perspective, it is worth noting that it is very difficult to predict how information made available from different sources can be combined and what conclusions can be drawn. Research shows, for example, that US social security numbers can be predicted from publicly available data, even though the numbers are intended to be private [32]. New research also shows that it is surprisingly easy to single out individuals, even in databases where personal information has been removed or modified with the aim of anonymisation [33]. In the large data sets that are available today, one cannot ignore the risk that someone could find and exploit a specific organisation's important data, or at least find a way into them.

5. The geopolitical dimension of information security

- Information operations where internet-based propaganda is combined with diplomacy, lies, media gambits and traditional military activities have become commonplace in armed conflicts.
- Cyber espionage and cyber sabotage are part of the "security policy toolbox" in an increasing number of countries.
- Increased opportunities for free and uncontrollable communication via the internet has resulted in backlashes in many states, with attempts to isolate their national networks from the internet.

In 2013, Freedom House, a US non-governmental organisation that has measured and promoted democracy in the world since 1941, concluded that global internet freedom had declined for three consecutive years. According to the report, out of 60 countries surveyed, freedom had declined in 34 countries and increased in 16 [34]. Blocking and filtering of unwanted political and social content is on the rise, particularly in authoritarian countries like China, Iran and Saudi Arabia, but also in democracies like South Korea.

This negative trend is partly at odds with the positive image of the internet as a force for freedom that was established in connection with the Arab Spring of 2011. While it was popular then to talk about "Twitter revolutions", the picture is now more balanced. A review of the research literature shows that several parallel trends coexist [35]: the new digital forums may indeed enable people to exchange information and expose injustices, but they also offer new opportunities for censorship and disinformation.

5.1 Information operations in armed conflicts

It is clear that the use of information operations in conflicts is here to stay. A number of aspects of information warfare are described in a report from FOI, the Swedish Defence Research Agency, on Russia's annexation of the Crimea [36]. In February 2014 allegedly authentic e-mails were published suggesting that the new Ukrainian leaders were ruled from the West, leaked by someone calling themselves Anonymous Ukraine - a story that was amplified in Russian-controlled media [37]. Russian authorities then ordered the blocking of pro-Ukrainian groups on social networks in Russia [38]. In addition, prominent Russian opposition figures such as Alexei Navalny and Garry Kasparov saw their sites officially blocked by the Russian authorities [39]. Websites of Ukrainian authorities and both pro-Russian and pro-Ukrainian newsrooms were subjected to denial-of-service attacks of unknown origin [40]. The Ukrainian Security Service reported intrusions by malicious code in the cell phones of members of parliament [41] and the telecom operator *Ukrtelecom*

announced at the beginning of the Crimean operation that fibre cables had been cut and that uniformed personnel had taken over their hubs [42].

Most striking, however, was perhaps what may be perceived as coordination between different methods of conducting information warfare: the message from the Russian political leadership, its diplomatic missions and Russian state-controlled international media such as RT (formerly Russia Today) were probably supported through leaked telephone calls from American [43] and Estonian [44] diplomats. The intercepted diplomatic discussions suggest that advanced signals intelligence was used to obtain media impact that spread doubt and uncertainty in the West. This information was spread on social media and was subsequently picked up by traditional media.

Information operations complemented traditional military operations and were an important factor in the Russian success in the Crimea operation, says FOI [36]. A similar assessment is made by the Norwegian Defence Research Establishment: Russian cyber attacks on major Ukrainian communication channels aimed to control the communications of selected target groups, and as communications from Crimea were cut off from the outside world, there was a massive information campaign against the West to get across the message that Russia's actions were legitimate [45]. Similar examples can be found in other modern conflicts. The Islamic State (IS), which operates in Syria and Iraq, skilfully used the modern media landscape throughout their offensive in the summer of 2014 to spread propaganda and intimidate their opponents. Although in both cases it is naturally unclear which side is behind what acts and what is done by state actors as opposed to individual volunteers, it is equally clear that modern warfare takes place in both the physical environment and the information environment. Tanks and troop movements are still pieces of the puzzle, but so are malware and propaganda in the form of "Twitter bots".

Although there is a clear trend toward the use of IT in general and different types of cyber attacks in particular in modern conflicts, this does not mean that they are always effective. Researcher Emilio Iasiello has investigated some of the most high profile cases in recent years and is sceptical: In its cyber attacks against Estonia in 2007, Russia tried to influence the country and it certainly created a lot of attention. But the bronze statue was still moved, and Estonia brought up the cyber issues in NATO and remains solidly west-oriented. If the US or Israel tried to derail Iran's nuclear program through Stuxnet, they certainly managed to create some problems in the short term. But in the longer term, it is not at all certain that Iran's capability or desire to become a nuclear power was affected [46]. What is clear is that there are many resourceful players who try to exploit vulnerabilities in IT systems and procedures to gain advantages. There are also hidden statistics: the most skilled cyber attacks have probably never been revealed, and so their effects cannot be openly evaluated. It is important to be aware that there are advanced threats that affect many parts of society.

5.2 Cyber espionage and cyber sabotage

Issues of cyber espionage are also gaining ground in the diplomatic arena. The US decision to prosecute Chinese cyber spies in the spring of 2014 is an example of how a legal mechanism that will probably never lead to any sentence is used to send a diplomatic message. Larger consequences probably result from American import barriers on for example Huawei, and the resulting Chinese ban on Apple products issued by the authorities in August 2014. The rationale for such measures is a fear that trade secrets are being stolen, undermining national competitiveness. However, while it is easy to assess the effects of political negotiating positions or military plans being stolen - this damage is done as soon as they end up with someone else - the impact on competitiveness and economy are difficult to assess. Here you have to take into account both the information that was stolen and the thief's ability to put the stolen goods into commercially viable products.

Another threat that plays a role both for intergovernmental relations and for individual companies is the implantation of vulnerabilities in hardware or software from foreign suppliers. This creates the desire to buy domestically, at least for the top-level military and civilian leadership. If this becomes a common phenomenon, though, it may mean that all countries get inferior products, because competition from abroad makes the domestic industry more innovative and better at using technologies [47]. Technological lag and more expensive IT is thus the price to pay for increased security against implanted vulnerabilities – at least while domestic suppliers are not infiltrated. The same dilemma applies on the service side: IT and telecom services purchased from abroad may pose potential security risks, but research shows that free trade in services leads to better growth in the long run [48].

This development poses new challenges for government agencies, security and intelligence services and private companies.

5.3 The threat to the open internet

Freedom House, whose measurements are widely used in academic studies, notes in its analysis of freedom on the internet in 2013 a trend towards more cyber attacks on opposition movements: in 31 of the countries studied, the authorities have apparently attacked social networks, tapped communications and knocked out websites through the use of malware, among other methods. The trend is also towards increased surveillance: two-thirds of the countries studied increased the state's legal or technical ability to eavesdrop in 2013. Another legal trend is for more responsibility to be put on intermediaries, such as internet providers or platform owners, for content. The most extreme case is China, where censorship is largely outsourced to newspaper offices and ISPs who more or less manually sift through and delete tens of millions of messages every year [49].

The status of the internet has also become a hot diplomatic issue. At a meeting of the International Telecommunication Union, ITU, in Dubai in late 2012, the

lines of conflict became clear between the US and the EU on the one side and Russia and China on the other side. The latter wanted to see a future model for internet governance in which the UN agency ITU would have a larger role - which the former saw as a disguised way of allowing more censorship and government control. The conflict was no surprise: For many years Russia has tried to build international acceptance for its agenda on what is called "international information security" [50]. In September 2011, Russia, China, Tajikistan and Uzbekistan wrote a letter to UN Secretary General calling on member states to work together to stop the spread of information that undermines stability in other countries [51]. The Russian message is that all countries face common challenges such as cybercrime, cyber terrorism and cyber warfare and must therefore work together, preferably in the United Nations. Areas such as freedom of expression online, where there are obvious disagreements, are not mentioned.

However, at the large NETmundial Conference held in Brazil in April 2014, with private sector, civil society and government participants from 97 countries, human rights and freedom of expression were adopted as fundamental principles for the global internet policy. This was seen as a success for the line supported by, inter alios, Sweden. However, an increasing number of countries are trying to isolate their national networks from the rest of the internet, a phenomenon called *splinternet* [52]. If this trend continues, we will move towards a fragmented internet, where more and more people live in information bubbles. It may affect not only diplomacy, advocacy and public discourse, but also international companies and even cross-border online crime, *crime-as-a-service*.

6. Crime in the information society

- Today's IT-related organised crime generally has financial incentives, and an internet-based criminal service sector, *crime-as-a-service*, has emerged in recent years.
- The interaction between traditional and electronic crime is increasing and is becoming increasingly complex.
- Today's crime places new demands on the judicial system, not least in terms of interaction with foreign police forces and private sector.

Today, virtually all crime has an IT component. The most obvious cases are crimes which by their very nature require modern technology, such as computer fraud and hacking [53]. But modern society's communication paths are such that crimes like handling stolen goods, benefit fraud, credit card fraud and false invoices have large IT components today, almost by definition. Indeed, it is often the case of old crimes in a new guise.

6.1 A new internet-based criminal service sector

Specialisation and division of labour also occur among criminals. Technological developments have enabled the emergence of a criminal internet-based service sector, *crime-as-a-service*. This means that criminals do not need to do everything themselves, but can buy ready-made components and assemble them for their own purposes. One example is web hosting that gives criminals security, reliability and anonymity and rarely cooperates with police [54]. By setting up these services in countries with weak or non-existent IT legislation, it is extremely difficult to have the servers shut down or to track who is behind operations [55].

Another example of financially-driven crime is *malware-as-a-service*: complete solutions with malicious code that can be reused in different contexts. These operations are becoming better at providing services similar to commercial enterprises, such as customer support, continuous updates and product development. Malware makes possible much of the crime against information systems that we see today. The technical development of mobile devices has made them more lucrative to attack and this threat has increased dramatically in recent years. The banking sector is also very vulnerable: criminals stealing login credentials or obtaining codes for two-way authentication is becoming more common. There is also a trend where instead of targeting bank customers through mass infections, the focus is on service providers that store large amounts of customer information. By creating a backdoor or placing a trojan at just a single such actor, large amounts of personal data can be stolen and sold.

So-called *ransomware* is malware that is installed on the victim's computer, which then allows the criminal to encrypt the computer or parts of the material on the computer. The criminal then demands that the victim pays money to regain control of the computer, or the material that is encrypted. Cases of ransomware have increased dramatically in Europe over the past two years. The method is lucrative because it generates a lot of money with little risk of prosecution. Digital currencies and prepaid debit cards have made it easier for criminals to get away with the profits of their crimes. Ransomware attacks can easily be orchestrated by criminals who lack special technical skills, and the services are easy to buy online. The problem with this type of case is complicated by the fact that the players and infrastructures are often abroad. Sweden has not been hit as hard as many other parts of Europe, but there are known cases in Sweden too. Ransomware can be obtained for both PCs and mobile devices [56].

In 2014, anti-virus company McAfee estimated that the world annual cost of cybercrime is around USD 445 billion, which included both the value of the stolen information and the victims' costs for protection and recovery [57]. In 2013 a competitor, Symantec, estimated the cost at a more modest USD 113 billion, of which Swedish costs were reportedly USD 838 million [58]. As with any crime statistics, there are many unreported cases. Not all companies discover that they have been compromised, and those who do discover it do not want to talk about it. One reason to remain silent is reputation and stock market value: research shows that IT failures in companies affect the share price negatively [59]. At the same time, security companies have an interest in exaggerating the threat [60].

Unfortunately there are many easy targets for financially-driven cybercrime, such as computers that have not been patched with the latest security updates. A study of 1424 software vulnerabilities that hackers have written exploits for showed that over 30% of the exploits had been written *after* the security update had been released [61]. This clearly shows that relaxed patching routines result in lucrative targets, and underlines the need to update and maintain systems.

6.2 The interplay between traditional and electronic crime

One example of how traditional organised crime utilises modern technology comes from the port of Antwerp, Belgium. In June 2011, two enterprise networks in the port were infiltrated by Dutch hackers. Their clients were drug traffickers from South America who had hidden cocaine and heroin alongside legitimate goods in containers. By hacking the computers, they were able to control the containers' arrival, location and security so that they could fetch them before the rightful owners did. After two years, this was noticed by port workers who saw containers disappear without any explanation. How much drugs that passed the port in this way is not clear, but over two tonnes of cocaine and heroin and more than a million euros were seized when the operations was exposed. It is also worth noting that the first cyber attack, which

sought to gain access to the system by sending malicious e-mails, failed. The criminals then attacked the weakest link instead by physically breaking into the offices to install equipment for interception and system manipulation [62]. This interaction between traditional and electronic crime places new demands on the judicial system and its ability to investigate complex crimes.

A large part of the internet consists of pages and services that are not indexed or accessible by conventional search engines. In these closed networks there is a large marketplace for criminal goods and services, so-called *dark markets*. Trade has increased significantly, particularly in drugs but also ID documents, weapons, malware and documented child sexual abuse. Silk Road is an example of such a marketplace that was closed by American authorities in October 2013. Despite the fact that this closure was described as a breakthrough in the fight against online drug sales, there are estimates that indicate current sales being twice as large as in the heyday of Silk Road. In just two years Silk Road gained 200,000 registered users and achieved a turnover of one billion US dollars during the period [63]. Drug dealers on the internet have evolved and today you can order Bolivian fair trade cocaine or opium from non-violent producers.

In order to obstruct investigations and cover their tracks, much of the criminal economy has traditionally been cash based. As other payment methods have emerged for completely legal purposes, the criminal world has been quick to catch on. One example is prepaid debit cards, where a sum is deposited on a VISA card which can then be used for payments without it being possible to trace who made the purchase or where the money originally came from. Crypto-currencies, of which Bitcoin is the most well-known, have much the same function. Bitcoin is a currency and an electronic payment system in one and is popular among criminals for the same reason as cash - deals that are done cannot be undone and are difficult to link to specific individuals. For these reasons, bitcoin or other crypto-currencies are in principle the universal method of payment in *dark markets*. Unfortunately, this gives new technologies a bad reputation and hampers innovations: bitcoin also has great potential in completely legitimate areas such as crowd funding, donations and secure transactions [64]. Finding an effective method of regulating digital currencies that make criminal use difficult without undermining the positive effects is an important future challenge.

6.3 Modern crime poses new demands

Even though the law is the same in the physical and the electronic world, people's behaviour is affected by different conditions. Unfortunately, it seems that the threshold for threatening and insulting people anonymously on the internet is lower compared to saying the same thing eye to eye. On top of this, the technical circumstances of the investigation are more complicated when the perpetrators can hide using anonymising services and when the platforms and infrastructure used to spread the message are often abroad. Offences such as threats and slander now include clear components of information security.

Another crime that has grown into a major social problem in recent years is identity theft. Once an identity has been hijacked, the perpetrator can quickly take out a loan and buy products online. Both companies and individuals are affected. It is common for identities to be hijacked and used to start a company, which then commits crimes. One response to this is the proposal of a new penal provision for identity intrusion put forward by the government committee of inquiry on property protection (SOU 2013:85) in December 2013 [65]. It was proposed that the offence should be punishable by a fine or imprisonment of up to two years.

On 23 November 2001 Sweden signed the Council of Europe's Convention on Cybercrime along with a number of other states (ETS no. 185), also called the Budapest Convention. The purpose of the Convention, among other things, was to harmonise legislation among convention states and facilitate international cooperation. It recommended that the states should introduce the category of crime *serious hacking*, which Sweden did on 1 July 2014. The offence results in a minimum of six months and a maximum of six years imprisonment. In the new law, attempted hacking and preparation for serious hacking are also punishable. Sweden has not yet ratified the Convention, as there is an ongoing review of the constitutional amendments needed for Sweden to comply with its demands [66].

As IT-related crime is often international, there has been a need for harmonisation, coordination and police support. For these reasons the EC3 (European Cybercrime Centre) was founded in 1 January 2013 at the European Police Cooperation Agency, Europol. Against this background, a decision has been made to create a similar national cybercrime centre in Sweden in connection with the new police authority that was established on 1 January 2015. This is to manage cybercrime better and comply with the Cybercrime Convention.

7. The race to find the weakest link

- Software that identifies vulnerabilities and simple and inexpensive technical tools for attacks have lowered the threshold and put tools in the hands of more attackers. At the same time, the most advanced attack tools are still hard currency, reserved for a select few.
- Despite technical vulnerabilities, the weakest link is often the human in the system, who can be fooled into downloading malware or disclosing sensitive information.
- Even though more and more organisations introduce regulations for information security, the step from regulations to real security is a long one.

Attackers are constantly searching for the weakest link. Technology, users, organisations and regulations may all have potential weaknesses that can be exploited. What gives the greatest effect varies over time and between different contexts. An example of a recent area is apps for mobile phones and tablets - devices that we always carry with us and that contain increasingly sensitive information. Although the largest study of app-security so far did not find any malware or vulnerabilities that could be used in the 1,100 most popular free Android apps [67], new examples of vulnerabilities are continuously being published. Examples include how camera functions can be abused [68] or how the review in the Apple App Store can be bypassed [69]. You can never relax - the race between attack and defence is constant.

7.1 Technology for attacks

Software for different kinds of attacks is becoming easier to obtain. Making an unsophisticated attack thus no longer requires any great skills and the threshold of attack is lowered. In Sweden, a number of denial-of-service attacks against schools [70] and municipalities [71], [72] attracted much attention in recent years, although the number of unreported cases makes the trend difficult to assess. The occurrence of such relatively simple attacks is probably due to the increased availability of tools. For the most advanced attack tools, the situation is different. Exclusive information about vulnerabilities in sensitive systems command a high value. Attacks carried out with the help of such information are kept well hidden and do not reach the headlines until long afterwards, if ever.

Amplified denial-of-service attacks appear to have become more common and several high-profile attacks have taken place in recent years [73]. Such attacks use the addressing in the internet's domain name system (DNS), or similar systems, in such a way that many third-party computers are tricked into sending so much traffic to the victim that the system cannot handle it. A

multiplier effect is thus achieved. In order to combat this threat, organisations must begin to look through all their internet-exposed services more systematically in search of vulnerabilities. Many services besides DNS have these characteristics and they can be used for amplification.

Information on vulnerable and internet-connected computer systems is becoming increasingly easy to find on the internet, lowering the threshold for attacks. In 2013, researchers managed to map the whole internet (more precisely, all the IPv4 address space) in less than an hour [74]. A scan like this can find millions of vulnerable devices at lightning speed, and allows a hacker to immediately take advantage of newly discovered vulnerabilities on a large scale. A research project at Cambridge was looking for internet-connected SCADA systems and found thousands, most without password protection and many with known vulnerabilities [75]. It goes without saying that such information is valuable to a hacker. Advanced hackers have long been able to gather such information on their own, of course, but the existence of compiled pages on the internet lowers the threshold for opportunists who are looking for easy targets. Other parties' saved scan results also make it possible to study targets without sending any traffic to them.

7.2 The user is often the weakest link

Technical vulnerabilities are often not the weakest link, however. That is the user - the human factor in the system. Behavioural research shows that we are very willing to share our personal data on the web [76]. Such information can be used for attacks in at least two ways. Firstly, many services still use personal questions to reset forgotten passwords. In a world of open data and plenty of personal information on the internet, a hacker can easily use such information to get past password protection. Secondly, the possibilities of manipulation (*social engineering)* are made easier.

A classic example of *social engineering* is phishing e-mail – tricking the victim into doing something harmful under false pretences. Even if it is an old method of attack, it is constantly developed and has become more popular since client security has generally improved. According to the security company Symantec, there was a clear change in phishers' modus operandi in 2013 compared with the previous year; while the number of recipients and the number of letters sent in each campaign was smaller, the time window during which each attempt was made was extended from a few days to a week [77]. This was probably a conscious strategy to reduce the risk of detection.

When phishing uses a false but trustworthy looking sender and is aimed specifically at the victim, it is called *spear phishing*. A Swedish experiment shows that targeted phishing works better at deceiving users than non-targeted phishing [78]. At the same time, the risk of detection increases; the non-targeted message was never reported to security staff, while the targeted message was quickly reported. The researchers concluded that under certain circumstances a hacker might avoid too targeted phishing, since it raises the

risk of detection. It not possible to say in general terms whether targeted or non-targeted phishing is more dangerous; it depends on the context.

Having a social life on the internet is normal for many people today. Many choose to disclose personal information and click on links despite an awareness of the risks, because the benefits are large. Risk behaviour varies between generations, making it difficult to isolate a single trend in this area. A Dutch study has shown that older generations are more likely to accept unknown persons that contact them on the internet, whereas younger people gave more information at the same time as they more frequently used built-in security settings [79]. Behavioural differences between users will probably need to be taken into account when developing future security training.

The limited ability of people to memorise many different passwords is another problem. Many websites require visitors to create their own personal accounts with information stored by the provider. In order to protect such systems against intrusion, there are often requirements for stronger passwords and double authentication (such as security codes via text messages and another e-mail address). But far from all services use such solutions, and the effect is that information about users is stolen and sometimes even published.

7.3 Technology for defence and the difficulties of creating security

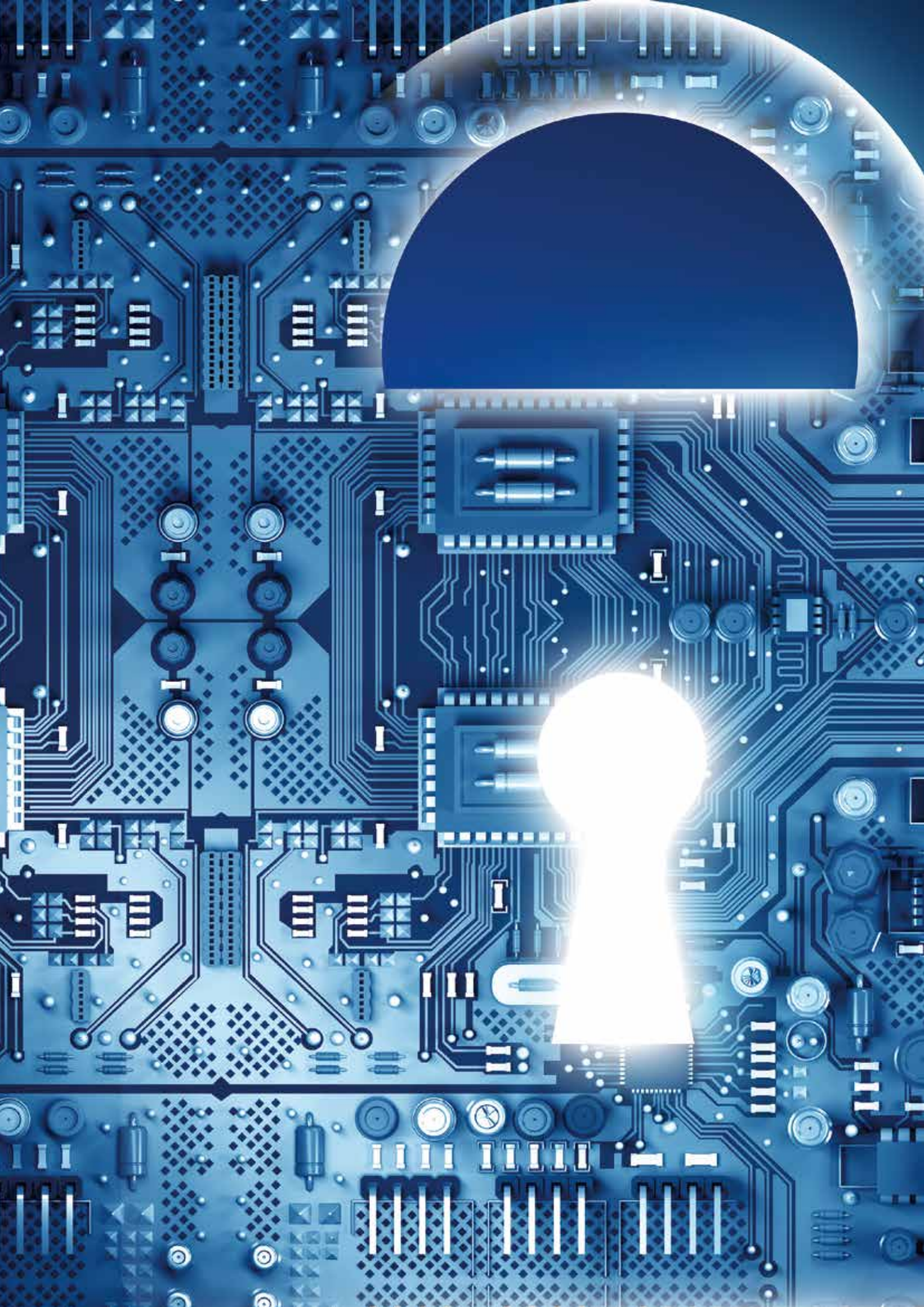
Even defence mechanisms are automated and turned into products. According to the consultancy company Gartner, the global market for firewall solutions amounted to USD 8.7 billion in 2013, showing a growth of 9% compared to 2012 [80]. That is considerably larger than the market for the protection of individual machines (*endpoint protection*) which in 2012 amounted to USD 2.8 billion - not significantly more than 2011 [81]. According to Microsoft, approximately 75% of all of the world's computers had some form of real-time monitoring security software that was constantly switched on in 2013 [82].

While protection tools are useful, it is also important to realise their limitations. A quantitative study of vulnerability scanners (which are used to find known vulnerabilities in operating systems and other software) showed that scanners provided with the relevant credentials for the system found about 30-50% of the known vulnerabilities that were actually there [83].

Intrusion Detection Systems (IDSs) are used by many companies and organisations, but they give a lot of false alarms if they are not properly configured, so they require extensive manual work to be useful [84]. At the same time, IDSs can be surprisingly good. It is easy to believe that a system based on known attack signatures would not be able to detect new, unknown attacks (*zero days*). However, new research shows that there are intrusion detectors which can even detect some attacks that do not yet have a signature, even though their effectiveness is clearly poorer than for known attacks [85]. The race between technology for attacks and technology for protection continues.

In Sweden the National Defence Radio Establishment develops a technical detection and warning system (TDW) which is designed to detect advanced IT attacks against critical systems in society. The system is supplied with signatures obtained through signals intelligence, and is therefore subject to secrecy in order to protect national security. The signatures give the system the ability to detect IT attacks that cannot be detected using commercially provided systems for the detection of malware. The information and experience generated by a TDW can be used for effective protective measures.

Many organisations try to increase their security by introducing information security regulations for users to follow. However, for the regulations to have a positive impact on information security, they must be complied with. It is not enough to have the documents. Scientific studies show that compliance with security rules is a complex issue and that there is no simple way of ensuring the impact of regulations [86]. Just as with other behaviour, the individual's attitude, social norms and the inconvenience of regulations all play a large role. In contrast, severe penalties for breaking the rules make very little difference. One objective for information security to strive towards would be the flight safety culture in the air force. Without shame or embarrassment, pilots regularly report mistakes they have made and in doing so, they strengthen future safety [87].



8. Robust information systems and business continuity

- In modern society, the consequences of information systems outages are becoming greater and more difficult to grasp.
- Risk management and continuity planning are becoming increasingly important in order to achieve robust information systems, as is proper understanding of the increasingly complex dependence of business operations on IT.
- The market for cyber insurance is in its infancy, but will grow in the future.

Technology has made possible many obvious benefits: automation of manual work, economies of scale in information management and the reduction of transaction costs for companies and consumers. At the same time, our increased dependence on functioning technology means that the impact - both monetary and non-monetary - of outages is increasingly large and difficult to grasp.

8.1 Downtime with unexpected consequences

It is easy to underestimate non-antagonistic threats - those that do not come from an outside attacker but from our own shortcomings, short-sightedness or negligence. The Encyclopaedia of Information Assurance [88] aptly notes that “Business resumption and disaster recovery planning is probably the part of information security that is easiest to overlook and postpone”. This attitude can quickly backfire. When an actor with many customers experiences outages, the consequences can be severe and unexpected in many different places at the same time. One such example was when the IT company Evry had problems on New Year's Eve 2013, resulting in data availability problems in several completely different sectors of society.

Even though antagonistic threats are more exciting, everyday quality assurance work must not be underestimated. Bugs in software and hardware, quality defects in software development and missing or careless procedures in software updates can create major problems, as the Swedish Social Insurance Agency found out after a firmware bug in a switch caused a crash in September 2014 [89].

One problem with paying too little attention to ordinary downtime is that this in itself may open for antagonistic attacks. A smart hacker who wants to affect an enterprise IT system may very well disguise attacks as intermittent downtime. If the victim does not have procedures for checking the cause of each downtime incident and just re-starts the system, the attack may go undetected. The hacker can then introduce problems and disruptions

repeatedly over a long period of time, without having to find a new attack vector. A study based on data from the security company Symantec shows that it can take years before malware is detected [90]. In August 2014, a study by KPMG gained a great deal of attention when it was found that of the 14 Swedish companies and government agencies investigated, 13 were infiltrated by malware that was in contact with a hacker's control server somewhere else in the world. Information was sent out from 11 of the organisations - secrets of one sort or another - to the hacker [91]. The relatively small group selected makes the results difficult to assess, but a similar study carried out by KPMG in Finland gave comparable results.

8.2 Risk management and business continuity planning are becoming increasingly important

Not enough organisations realise how their strategies and agreements affect recovery time after unplanned downtime. The first step towards more mature risk and incident response is to understand the operations and their need for continuity and availability. A company whose income depends on the availability of a credit card payment system would rather have many short outages than a single long one. After a brief interruption, a customer can insert the card again and no damage is done - but if a long outage occurs just before Christmas it could wipe out a large part of the profit for that year. An industrial process such as a steel or paper mill would rather have a single long interruption than many short ones. Each interruption means a stop in a large physical process, including the logistics supply chain, with considerable costs for recovery and restart [92].

Unfortunately, maturity in incident response is still low in many enterprises. A study by the Swedish Civil Contingencies Agency confirms the picture: in a survey of 334 Swedish government agencies, it turned out that 65% had no continuity plan [93]. Of the 35% that actually had a plan, only 36% had exercised putting the plan into effect [93]. The use of standards such as the Information Technology Infrastructure Library, ITIL, or the International Organization for Standardization, ISO's standard for business continuity management contributes to increasing maturity, but standards do not take effect until they are implemented - which can take time, given the long life-cycles of many ERP systems.

Perhaps management groups have a greater appetite for risk than those responsible for continuity. Who is right? This puts the spotlight on a very crucial aspect: it is difficult to manage risks rationally without having an overview of your organisation's IT dependence. A development has taken place in recent years, moving from a situation with vertical solutions (separate payroll system, separate sales system) to an increasingly integrated IT landscape, where ERP systems are linked with each other, both within and outside the company. Controlling and optimising logistics chains across multiple suppliers with the help of integrated IT is standard in many industries

today [94]. Even if this increases efficiency and enables completely new business concepts, it has also led to many large companies not knowing how many IT systems they have, how they are interconnected or exactly how they support operations. The trend towards outsourcing operations or services to third-party providers in the cloud that are only controlled via contracts (*service level agreements*, SLAs) makes it even more difficult to manage risks effectively and correctly. Since it may be difficult to act rationally when signing contracts [15], this requires good procurement skills.

Risk management is increasingly being recognised as a way of strengthening information security in organisations. Nevertheless, far too many organisations still make no risk assessments of their dependence on information for operations in advance, and can only improvise when something unexpected happens. In a survey answered by 334 Swedish government agencies it turned out that 59% did not use risk analysis to support continuity planning [93]. Around 40% of the agencies had no rules for what to include in risk analyses or who should initiate them [93]. Reversing this trend will take time and requires work on several fronts. The Confederation of Swedish Enterprise guide "Security in the acquisition and development of systems," which argues that information security is determined early in the life-cycle, in procurement and development, is one example [95]. It is important to specify in the contract who is responsible for what throughout the whole life-cycle. Similar advice is found in the Swedish Civil Contingencies Agency's "Guide to information security in procurement" [96].

8.3 Costs for IT-related incidents and the importance of financial incentives

There is no reliable compilation of the total costs of unavailable IT systems in Sweden. A study carried out by the Swedish Social Insurance Inspectorate estimates that the cost of non-productive time due to faults and downtime was SEK 19 million for the Swedish Social Insurance Agency and SEK 1.7 million for the Swedish Pensions Agency in 2012 [97]. In commercial activities costs may be much larger. In conjunction with the Stockholm Stock Exchange outage in June 2008, Dagens Industri newspaper reported that "billion-kronor deals were lost" [98] and according to Computer Sweden, Axfoods' costs during a four-hour long cable break that stopped credit card payments amounted to SEK 4.25 million per hour [99]. Often, though, no cost estimates are made even for events receiving widespread media attention such as the Tieto incident in November 2011. The difficulty of making estimates is also a symptom of a deeper problem: most companies and businesses do not know how vulnerable they are, they do not know what downtime may cost when they do their risk management and they even find it difficult to calculate the cost of the downtime after it occurred.

Economic incentives are an important factor in risk management. For example, companies acting on competitive markets appear to be more proactive than municipalities. One particular difficulty is that many public sector actors interact with each other without formal contracts and would need to be able

enter into agreements corresponding to commercial contracts [18]. Without proper responsibilities established, they find it difficult to reach mature incident management. In this area, commercial enterprises have an edge over the public sector. Being at risk should also play a role: players who manage valuable data and companies with sensitive industrial processes should be more mature than others when it comes to risk management. All in all, these factors will hopefully lead to a greater awareness over time, but there is a risk that it will only happen after a number of serious incidents with large consequences. In addition, general maturity in risk assessment, for example with regard to financial risks, does not always lead to maturity in risk assessments of information security.

One way to deal with the lack of risk assessments is by making a stronger link between IT risk and financial risk, for example through more mature cyber insurance policies. The cyber insurance market is expanding. At the end of 2011 it was estimated to be worth USD 750 million [100], while an estimate from 2014 indicates that it has grown to USD 2 billion [101]. The Swedish market is still in its infancy, however. In the research literature it has been proposed that major players, such as governments, could kick-start the cyber insurance market by taking the first step and buying insurance themselves [102]. Insurance companies have a long history of producing risk profiles based on data and setting premiums based on risk behaviour, which under certain conditions can provide an incentive for policyholders to work on their own security and in doing so increasing security for everyone else [103]. On a cyber insurance market, insurance companies would be able to demand higher premiums from actors without basic security in place. In this respect, insurance policies can provide economic incentives for more organisations to learn from others' mistakes rather than their own.

At the same time, it is important to remember that an insurance policy does not replace the need for in-house security, just as fire insurance does not replace the need for fire drills, smoke detectors and fire extinguishers. Cyber insurance is an agreement, where the value of the information to be protected must be matched to the content of the policy and the conditions for which compensation is to be paid out.

9. Concluding remarks

It is very difficult to describe the complex ongoing development in the area of information security. The field is extremely wide, as this report recognises. It is even more difficult to predict the future. Technological development is only one of several factors. Human behaviour, global developments, new services and individual events that receive attention and affect our behaviour are all additional elements. The area is a complex jigsaw puzzle where the picture is changing all the time. This report will hopefully help to increase awareness about information security and the factors that may be important to take into account in the future, in particular for decision-makers faced with information security issues.

References

[1] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. European Commission, High representative of the European Union for Foreign affairs and Security policy, 2013. Joint communication to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions, available at http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf, read 13/10/2014.

[2] OECD. Review of the 2002 Security Guidelines. http://www.oecd.org/sti/ieconomy/2002-security-guidelines-review.htm, December 2013. Read 30/06/2014.

[3] Anindya Ghose and Uday Rajan. The economic impact of regulatory information disclosure on information security investments, competition, and social welfare. In: *Fifth Workshop on the Economics of Information Security*, 2006.

[4] Alberto Portugal-Perez, José-Daniel Reyes and John S Wilson. Beyond the information technology agreement: Harmonisation of standards and trade in electronics. *The World Economy*, 33(12):1870–1897, 2010.

[5] Ross Anderson and Tyler Moore. Information security economics – and beyond. In :*Advances in Cryptology-CRYPTO 2007*, pp 68–91. Springer, 2007.

[6] Beñat Bilbao-Osorio, Soumitra Dutta and Bruno Lanvin (ed.). Global information technology report 2014, 2014. World Economic Forum.

[7] Steffen Bartsch. Practitioners' perspectives on security in agile development. In: *Availability, Reliability and Security (ARES), 2011 Sixth International Conference on*, pp 479–484. IEEE, 2011.

[8] Konstantin Beznosov and Philippe Kruchten. Towards agile security assurance. In: *Proceedings of the 2004 workshop on New security paradigms*, pp 47–54. ACM, 2004.

[9] Mikko Siponen, Richard Baskerville and Tapio Kuivalainen. Integrating security into agile development methods. In: *System Sciences, 2005. HICSS'05. Proceedings of the 38th Annual Hawaii International Conference on*, pp 185a–185a. IEEE, 2005.

[10] Dejan Baca and Bengt Carlsson. Agile development with security engineering activities. In: *Proceedings of the 2011 International Conference on Software and Systems Process*, pp 149–158. ACM, 2011.

[11] Swedish National Audit Office (Riksrevisionen). IT inom statsförvaltningen – har myndigheterna på ett rimligt sätt prövat frågan om outsourcing bidrar till ökad effektivitet? RiR 2011:4, January 2011.

[12] Henrik Karlzén. Molnet – möjligheter och begränsningar. Swedish Defence Research Agency, 2012. FOI-R--3381--SE.

[13] Reflektioner kring samhällets skydd och beredskap vid allvarliga it-incidenter. En studie av konsekvenserna i samhället efter driftstörningen hos Tieto i november 2011. Swedish Civil Contingencies Agency, 2012. Publication number MSB 367-12.

[14] Stefan Thalmann, Daniel Bachlechner, Lukas Demetz and Ronald Maier. Challenges in cross-organizational security management. In: *System Science (HICSS), 2012 45th Hawaii International Conference on*, pp 5480–5489. IEEE, 2012.

[15] Ulrik Franke, Markus Buschle and Magnus Österlind. An Experiment in SLA Decision-Making. In: *Economics of Grids, Clouds, Systems, and Services*, pp 256–267. Springer International Publishing, 2013.

[16] Nir Kshetri. Privacy and security issues in cloud computing: The role of institutions and institutional evolution. *Telecommunications Policy*, 37(4):372–386, 2013.

[17] Municipality must renegotiate contract with Google - unlawful processing of personal data. Dagens Juridik, http://www.dagensjuridik.se/2014/07/kommun-maste-omforhandla-avtal-med-google-innebar-olaglig-behandling-av-personuppgifter, 22 juli 2014. Read 01/08/2014.

[18] Outsourcing of IT services in municipalities. Swedish Civil Contingencies Agency, 2014 Publication number MSB728.

[19] Swedish National Audit Office (Riksrevisionen). IT-investeringar över gränserna. RiR 2009:18, November 2009.

[20] Cisco. The Internet of Things. http://share.cisco.com/internet-of-things.html, 2011. Read 2014-08-01.

[21] Rodrigo Roman, Jianying Zhou and Javier Lopez. On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, 57(10):2266–2279, 2013.

[22] Guide to increased security in industrial information and control systems. Swedish Civil Contingencies Agency, 2014 Publication number MSB718.

[23] Cisco 2014 Annual Security Report. Technical report, Cisco Systems, 2014.

[24] Ulrik Franke and Joel Brynielsson. Cyber situational awareness – a systematic review of the literature. *Computers & Security*, 46:18–31, 2014.

[25] Åse Dragland, SINTEF. Big Data – for better or worse. http://-www.sintef.no/home/Press-Room/Research-News/Big-Data–for-better-or-worse/. Read 16/10/2014.

[26] Ministry of Industry, Government. Commission to develop and refine the technology platform öppnadata.se - a portal for innovation. N2012/3599/ITP, July 2012.

[27] One step further - new rules and measures to promote the re-use of documents. SOU 2014:10, February 2014.

[28] Winston Ross. How Much Is Your Privacy Worth? MIT Technology Review, 2014. Read 17/09/2014.

[29] Swedish National Audit Office (Riksrevisionen). Rätt information vid rätt tillfälle inom vård och omsorg – samverkan utan verkan? RiR 2011:19, May 2011.

[30] Swedish National Audit Office (Riksrevisionen). Informationsutbyte mellan myndigheter med ansvar för trygghetssystem – Har möjligheter till effektivisering utnyttjats? RiR 2010:18, October 2010.

[31] Så enkelt som möjligt för så många som möjligt – Bättre juridiska förutsättningar för samverkan och service. SOU 2014:39, June 2014.

[32] Alessandro Acquisti and Ralph Gross. Predicting social security numbers from public data. *Proceedings of the National academy of sciences*, 106(27):10975–10980, 2009.

[33] Magnus Jändel. Decision support for releasing anonymised data. *Computers & Security*, 46:48-61, 2014.

[34] Sanja Kelly, Mai Truong, Madeline Earp, Laura Reed, Adrian Shahbaz and Ashley Greco-Stoner (ed.). *Freedom on the net 2013: a global assessment of internet and digital media*. Freedom House, 2013.

[35] Mikael Eriksson, Ulrik Franke, Magdalena Granåsen and David Lindahl. Social media and ICT during the Arab Spring. Swedish Defence Research Agency, 2013. FOI-R--3702--SE.

[36] Johan Norberg, Ulrik Franke and Fredrik Westerlund. The Crimea Operation: Implications for Future Russian Military Interventions. In: Niklas Granholm, Johannes Malminen and Gudrun Persson, editors, *A Rude Awakening. Ramifications of Russian Aggression Towards Ukraine*. Swedish Defence Research Agency, 2014. FOI-R--3892--SE.

[37] The Voice of Russia. Anonymous Ukraine releases Klitschko e-mails showing treason. http://voiceofrussia.com/news/2014_02_23/-Anonymous-Ukraine-releases-Klitschko-e-mails-showing-treason-3581/. Read 14/10/2014.

[38] The Moscow Times. Russia Blocks Web Pages Linked to Ukraine Protests. http://www.themoscowtimes.com/article/495488.html. Read 14/10/2014.

[39] Roskomnadzor. Ogranitjen dostup k rjadu internet-resursov, rassprostranjavsjich prizyvy k nesanktsionirovannym massovym meroprijatijam [Begränsad tillgång till en rad internet-resurser som har uppmanat till olagliga massaktioner]. http://rkn.gov.ru/news/rsoc/-news24447.htm. Read 14/10/2014.

[40] Nicole Perlroth. Cyberattacks Rise as Ukraine Crisis Spills to Internet. New York Times, Bits Blog, http://bits.blogs.nytimes.com/2014/03/04/-cyberattacks-rise-as-ukraine-crisis-spills-on-the-internet/-?_php=true&_type=blogs&_php=true&_type=blogs&hpw&rref=technology&_r=1. Read 14/10/2014.

[41] RBK Ukraina. SBU podtverdila fakty telefonnych atak na mobilnye nardepov [SBU bekräftar fakta om telefonattacker mot parlamentsledamöter]. http://www.rbc.ua/rus/news/accidents/sbu-podtverdilo-fakty-telefonnyh-atak-na-mobilnye-nardepov-04032014120700. Read 14/10/2014.

[42] Ukrtelekom. V AR Krim nevidomimi u vijs'kovij formi povtorno zablokovano dekil'ka vuzliv zv'jazku [I den autonoma republiken Krim har okända uniformerade män upprepade gånger blockerat flera kommunikationsknutpunkter]. http://www.ukrtelecom.ua/presscenter/-news/official?id=120389. Read 14/10/2014.

[43] BBC. Ukraine crisis: Transcript of leaked Nuland-Pyatt call. http://-www.bbc.com/news/world-europe-26079957. Read 14/10/2014.

[44] Reuters. Estonia denies leaked call implicates Ukraine protesters in killings. http://www.reuters.com/article/2014/03/05/us-estonia-eu-ukraine-idUSBREA2423O20140305. Read 14/10/2014.

[45] Henning André Søgard and Janne Merete Hagen. *FFI-fokus: Kampen om sannheten*. Norwegian Defence Research Institute

[46] Emilio Iasiello. Cyber attack: A dull tool to shape foreign policy. In: *Cyber Conflict (CyCon), 2013 5th International Conference on*, ss 451–468. IEEE, 2013.

[47] Roberto Alvarez and Raymond Robertson. Exposure to foreign markets and plant-level innovation: evidence from Chile and Mexico. *The Journal of International Trade & Economic Development*, 13(1):57–87, 2004.

[48] Aaditya Mattoo, Randeep Rathindran and Arvind Subramanian. Measuring services trade liberalization and its impact on economic growth: An illustration. *Journal of Economic Integration*, 21(1):64–98, 2006.

[49] Gary King, Jennifer Pan and Molly Roberts. How censorship in China allows government criticism but silences collective expression. In: *APSA 2012 Annual Meeting Paper*, 2012. Tillgängligt på SSRN: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2104894.

[50] Ryska utrikesministeriet. Convention on International Information Security (Concept). http://www.mid.ru/bdomp/ns-osndoc.nsf/-1e5f0de28fe77fdcc32575d900298676/-7b17ead7244e2064c3257925003bcbcc!OpenDocument. Read 25/09/2014.

[51] Li Baodong, Vitaly Churkin, Sirodjidin Aslov and Murad Askarov. Letter dated 12 September 2011 from the permanent representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations, addressed to the Secretary-General. General Assembly reference number A/66/359.

[52] Anil Ananthaswamy. Age of the splinternet. *New Scientist*, 211(2821):42–45, 2011.

[53] Brottsförebyggande rådet. Anmälda brott. Slutlig statistik för 2013. www.bra.se/statistik, March 2014.

[54] European Cybercrime Centre (EC3) vid Europol. Internet Organised Crime Threat Assessment (IOCTA), september 2014.

[55] Aditya K Sood and Richard J Enbody. Crimeware-as-a-service – a survey of commoditized crimeware in the underground market. *International Journal of Critical Infrastructure Protection*, 6(1):28–38, 2013.

[56] European Cybercrime Centre (EC3) vid Europol. Police Ransomware Threat Assessment, February 2014.

[57] Net Losses: Estimating the Global Cost of Cybercrime. Technical report, McAfee & Center for Strategic and International Studies, June 2014.

[58] 2013 Norton Report. Technical report, Symantec Corporation, October 2013.

[59] Anandhi Bharadwaj, Mark Keil and Magnus Mähring. Effects of information technology failures on the market value of firms. *The Journal of Strategic Information Systems*, 18(2):66–79, 2009.

[60] Paul Hyman. Cybercrime: it's serious, but exactly how serious? *Communications of the ACM*, 56(3):18–20, 2013.

[61] Muhammad Shahzad, Muhammad Zubair Shafiq and Alex X Liu. A large scale exploratory analysis of software vulnerability life cycles. In: *Proceedings of the 2012 International Conference on Software Engineering*, ss 771–781. IEEE Press, 2012.

[62] Hackers deployed to facilitate drugs smuggling, 2013. Intelligence Notification 004-2013, European Cybercrime Centre (EC3) vid Europol.

[63] The Crypto Crimson. UNODC: Online Drug Trade On The Rise Since Silk Road Demise. http://cryptocrimson.com/2014/07/unodc-online-drug-trade-thriving-since-silk-road-demise/.

[64] Wired World in 2014, 2013. Wired Magazine.

[65] Stärkt straffrättsligt skydd för egendom. SOU 2013:85, February 2013.

[66] Council of Europe Convention on Cybercrime. SOU 2013:39, June 2013.

[67] William Enck, Damien Octeau, Patrick McDaniel and Swarat Chaudhuri. A study of Android application security. In: *Proceedings of the 20th USENIX Security Symposium*, 2011.

[68] Longfei Wu, Xiaojiang Du and Xinwen Fu. Security threats to mobile multimedia applications: Camera-based attacks on mobile phones. *Communications Magazine, IEEE*, 52(3):80–87, 2014.

[69] Tielei Wang, Kangjie Lu, Long Lu, Simon Chung and Wenke Lee. Jekyll on iOS: When Benign Apps Become Evil. In: *Proceedings of the 22nd USENIX Security Symposium*, ss 559–572, 2013.

[70] TT. 18 year old charged with data hacking. VLT, 23 August 2014. p. 25.

[71] Annsofie Wieland. Hackers disrupt Bjuv's data traffic. Landskronaposten, 16 January 2014. p. A27.

[72] Ola Thelberg. Internet attack in Härnösand. Tidningen Ångermanland, 26 February 2013. p. 4.

[73] FuiFui Wong and Cheng Xiang Tan. A Survey of Trends in Massive DDOS Attacks and Cloud-Based Mitigations. *International Journal of Network Security & Its Applications (IJNSA)*, 6(3):57–71, 2014.

[74] Zakir Durumeric, Eric Wustrow and J Alex Halderman. Zmap: Fast internet-wide scanning and its security applications. In: *Proceedings of the 22nd USENIX Security Symposium*, ss 605-620, 2013.

[75] Éireann P Leverett. Quantitatively assessing and visualising industrial system attack surfaces, 2011. M.Phil. thesis, University of Cambridge, Darwin College.

[76] Jayant Venkatanathan, Vassilis Kostakos, Evangelos Karapanos and Jorge Gonçalves. Online Disclosure of Personally Identifiable Information with Strangers: Effects of Public and Private Sharing. *Interacting with Computers*, 2013. 10.1093/iwc/iwt058. In future issue.

[77] 2014 Internet Security Threat Report, Volume 19. Technical report, Symantec Corporation, April 2014.

[78] Hannes Holm, Waldo Rocha Flores and Göran Ericsson. Cyber security for a Smart Grid – What about phishing? In: *Innovative Smart Grid Technologies Europe (ISGT Europe), 2013 4th IEEE/PES*, ss 1–5. IEEE, 2013.

[79] Wouter Martinus Petrus Steijn. A developmental perspective regarding the behaviour of adolescents, young adults, and adults on social network sites. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 8(2), 2014.

[80] Greg Young, Adam Hils and Jeremy D'Hoinne. Magic Quadrant for Enterprise Network Firewalls. Technical report, Gartner, Inc., April 2014.

[81] Peter Firstbrook, John Girard and Neil MacDonald. Magic Quadrant for Endpoint Protection Platforms. Technical report, Gartner, Inc., January 2014.

[82] Security Intelligence Report volume 16. Technical report, Microsoft Corporation, 2014.

[83] Hannes Holm, Teodor Sommestad, Jonas Almroth and Mats Persson. A quantitative evaluation of vulnerability scanning. *Information Management & Computer Security*, 19(4):231–247, 2011.

[84] John R Goodall, Wayne G Lutters and Anita Komlodi. Developing expertise for network intrusion detection. *Information Technology & People*, 22(2):92–108, 2009.

[85] Hannes Holm. Signature Based Intrusion Detection for Zero-Day Attacks: (Not) A Closed Chapter? In: *System Sciences (HICSS), 2014 47th Hawaii International Conference on*, pp 4895–4904. IEEE, 2014.

[86] Teodor Sommestad, Johan Bengtsson and Jonas Hallberg. Varför följer inte användarna bestämmelser? – En metaanalys avseende informationssäkerhetsbestämmelser. Swedish Defence Research Agency, 2012. FOI-R--3524--SE.

[87] Säkerheten i första hand. *Försvarets Forum*, (4):21–22, 2014.

[88] Kevin Henry. Business continuity planning: Case study. In: *Encyclopedia of Information Assurance*, Chapter 42, pp 344–350. Taylor & Francis.

[89] Computer Sweden. Försäkringskassans cio om buggen bakom it-kraschen. http://computersweden.idg.se/2.2683/1.588563/-forsakringskassans-cio-om-buggen-bakom-it-kraschen. Read 14/10/2014.

[90] Leyla Bilge and Tudor Dumitras. Before we knew it: an empirical study of zero-day attacks in the real world. In: *Proceedings of the 2012 ACM conference on Computer and communications security*, pp 833–844. ACM, 2012.

[91] Unknown threats in Sweden. KPMG, 2014. Read 17/09/2014.

[92] Ulrik Franke. Optimal IT Service Availability: Shorter Outages, or Fewer? *IEEE Transactions on Network and Service Management*, 9(1):22–33, March 2012.

[93] En bild av myndigheternas informationssäkerhetsarbete 2014 – tillämpning av MSB:s föreskrifter. Swedish Civil Contingencies Agency, 2014. Publication number MSB740.

[94] Taco van der Vaart and Dirk Pieter van Donk. A critical review of survey-based research in supply chain integration. *International Journal of Production Economics*, 111(1):42–55, 2008.

[95] Tommy Svensson. Säkerhet vid anskaffning och utveckling av system. vägledning för informationssäkerhetsdeklarationen. Svenskt Näringsliv/Näringslivets Säkerhetsdelegation, October 2011.

[96] Vägledning – informationssäkerhet i upphandling. Swedish Civil Contingencies Agency, 2013. Publication number MSB555.

[97] Inger Sohlberg and Susanne Jansson. Dolda it-kostnader i verksamheten. Försäkringskassan och Pensionsmyndigheten. Inspektionen för socialförsäkringen, mars 2012. Report 2012:5.
[98] Jenny Askåker and Mikael Kulle. Miljardaffärer gick förlorade. Dagens Industri, pp 6–7, 4 June 2008.
[99] Jörgen Lindqvist. It-säkerhet är alltid för dyrt – tills något händer. Computer Sweden, 4 May 2012.
[100] John A. Wheeler and Paul E. Proctor. Understanding When and How to Use Cyberinsurance Effectively. Technical report, Gartner, Inc., April 2012.
[101] Defending the digital frontier. Special report: Cyber security. The Economist, 12 July 2014. p. 9.
[102] Eli Dourado and Andrea Castillo. Why the Cybersecurity Framework Will Make Us Less Secure. Technical report, Mercatus Center at George Mason University, April 2014.
[103] Marc Lelarge and Jean Bolot. Economic incentives to increase security in the internet: The case for insurance. In: *INFOCOM 2009, IEEE*, pp 1494–1502. IEEE, 2009.

About the agencies

The Swedish Armed Forces are responsible for the military defence of Sweden. The Swedish Armed Forces have a long experience in developing and monitoring nationwide secure and robust command and control information systems. These operations require relevant and up-to-date skills regarding both technology and security culture on the part of the Military Intelligence and Security Service (MUST), the IT operations and security organisations. The Armed Forces also provide support to other agencies and to the civil defence

The National Defence Radio Establishment (FRA) is a civilian intelligence agency whose activities contribute to protecting Sweden and Swedish interests. One of the agency's missions is to contribute to strengthening information security in areas important to Swedish society. FRA contributes to strengthening this protection by testing the vulnerability of IT systems or by giving concrete advice on how to improve security in the relevant operations.

The Swedish Civil Contingencies Agency, MSB, is a government agency with the task of developing society's capacity to prevent and manage accidents and crises. The Office of Information Assurance and Cybersecurity are responsible for supporting and coordinating work with information security in society, as well as analysis and assessments of developments in this area. The office provides advice and support in preventive work, and is responsible for regulations in the field of information security mainly towards the public sector. The office is also responsible for Sweden's national operational cybersecurity and IT incident response section.

The mission of the Police is to reduce crime and increase the security of society. The National Operations Department (NOA) has national responsibility for core activities of the Police, which include combating complex IT crime.

A collaboration between:

Swedish Civil Contingencies Agency
SE 651 81 Karlstad, Sweden Phone +46-771-240 240 www.msb.se
Publ.no. MSB851 – May 2015 ISBN 978-91-7383-572-5