Cyber security:

the current threat status and its development

Author
Dr Stefan Frei, Security Architect, Swisscom

August 2015

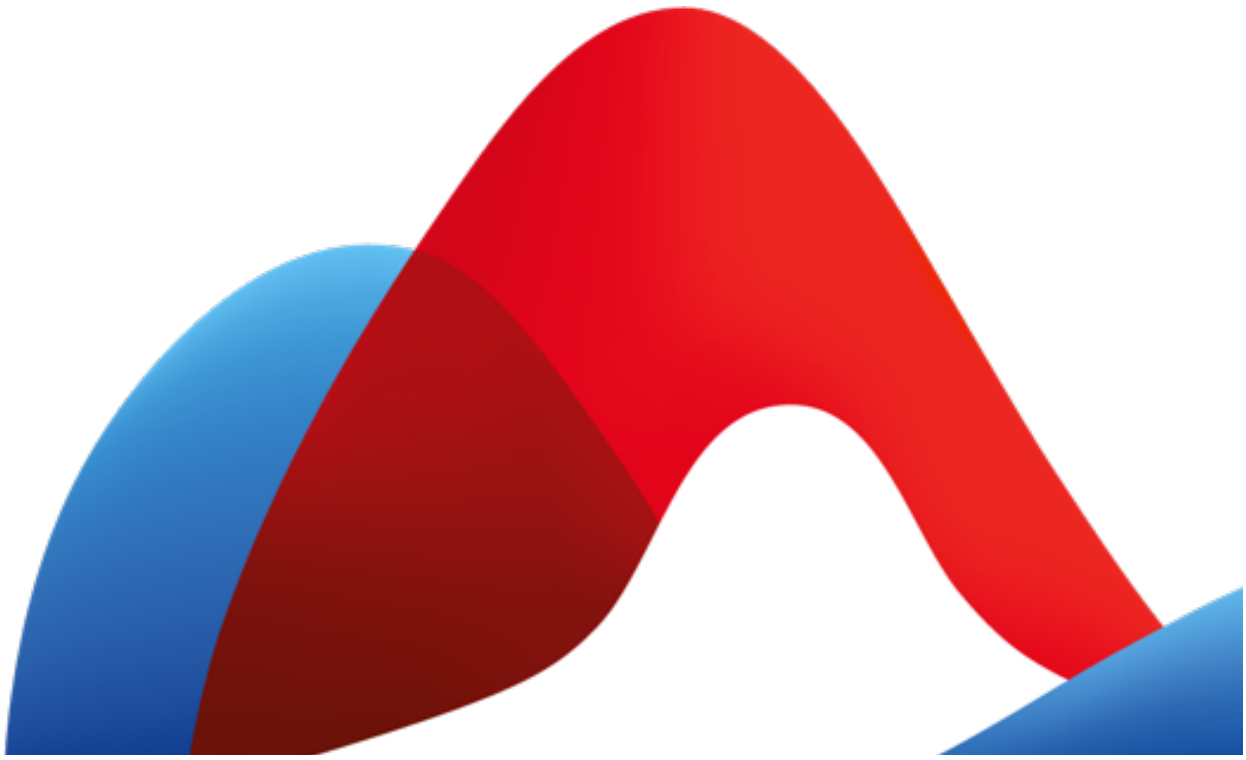

Table of contents

1 Introduction

Over the course of the past two decades, the development of new technologies and, in particular, the Internet has opened up unbelievable opportunities that have durably changed our lives both in the private and the professional sphere, and will continue to do so.
The changes that the Internet brought about can be considered disruptive. Their worldwide repercussions are comparable to the consequences of the industrial revolution and innovations such as oil exploration, the invention of the car or the introduction of antibiotics.
Today, more than three billion people have access to the Internet, equating to 42% of the global population in 2014.[1] The proportion of mobile usage is steadily increasing (94% of the world's population have a mobile phone), as well as the average time we spend connected to the Internet per day, we are "always on". Internet security has become a critical factor and will continue to grow in importance at the same rate as people and devices become increasingly interconnected.
As a society and as an economy, we are still in the early stages of adapting these possibilities. Naturally, these developments also give rise to new threats and dangers. The area of Internet security has developed and changed with immense speed at the interface between technology, economics and society.

This report sheds light on the current status of cyber threats from the perspective of Swisscom and of Switzerland as a whole. As a leading Swiss ICT provider, we bring to you an evaluation of the developments forecast for the coming 12 to 24 months.

2 The development of the cyber threat status

The Internet now connects people, machines, technology and businesses on a scale never seen before. Countless technical innovations and new applications and services based on these innovations have led to new possibilities, but also to new threats. The current threat status is complex and changes continuously. This report shall not limit its scope to extrapolating familiar, historical threats or individual branches of technology. It is our goal to evaluate current threats based on the dynamics and developments we have observed, and to present our expectations of the developments over the coming 12 to 24 months.

2.1 Status report – threat radar

Threats are borne of the constant development of new technologies and their application and distribution across society. Potential threats must be recognised at an early stage and systematically recorded. We have chosen to depict the current threat

[1] Internet World Statistics - http://www.internetworldstats.com/stats.htm

status and its evolution using a radar image, as illustrated in Figure 1. Topics and threats have been added to the radar in the form of dots. The dots you can see in Figure 1 depict the current situation. The traces of faded dots show each threat's development, in line with our expectations for the next 12 to 24 months.

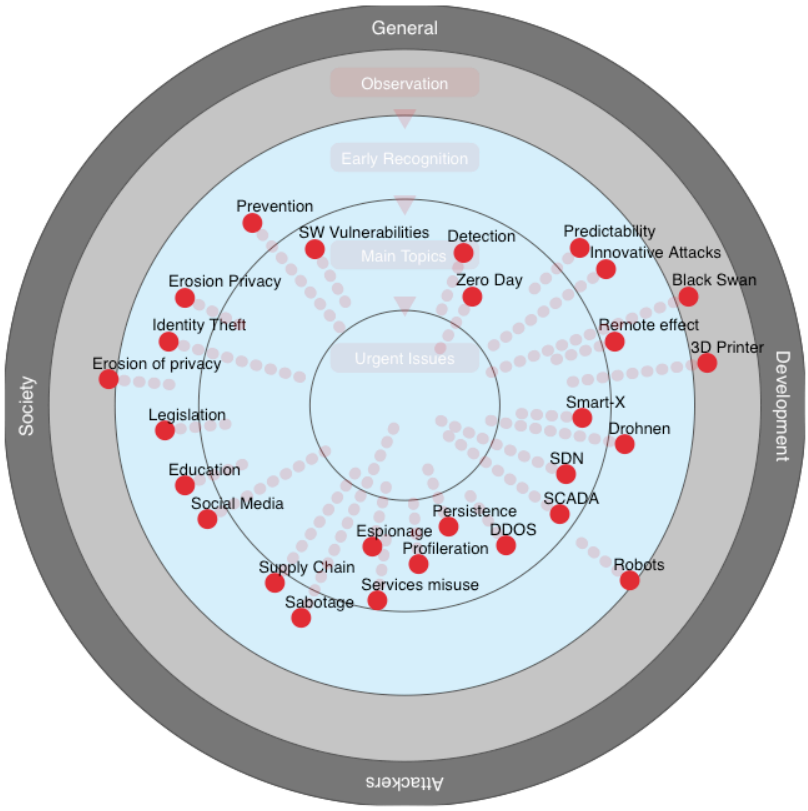

Figure 1 – Threat radar

In Figure 1, we differentiate between four types of topics and threats, dividing the radar into the segments *general* , *development*, *attackers* and *society*:

Development	Threats that are caused by technological development, without specific stimulation from a particular attacker or actor.
Attackers	Targeted threats from attackers.
Society	Threats resulting from our society being increasingly interconnected.
General	General threats that cannot be allocated to the above categories or apply to more than one category.

Topics cannot always be unambiguously allocated to just one of these four categories.

New threats, as well as their recognition, evaluation and corresponding counter-measures tend to follow the same evolution pattern, which is depicted by means of the concentric rings labelled *observation*, *early recognition*, *main topics* and *urgent issues*.

Topics and developments that could potentially develop into threats have been entered into the outer-most ring, *observation*. Topics entered into this ring are being systematically monitored, but have been allocated limited resources. Threats that could become relevant in the coming years have been entered into the *early recognition* ring. These threats are being actively and intensively researched in order to gain a better understanding of the risks, and to develop and prepare counter-measures. Current threats have been entered into the *main topics* ring. Here, counter-measures have already been introduced and are implemented in regular projects and processes.

If threats develop in line with these three phases *(observation, early recognition, main topics)* and we tailor our reactions accordingly, we can work proactively, from systematic recognition in the early stages to the implementation of counter-measures.

Unexpected, emergent threats and those that develop more swiftly than expected will be dealt with reactively. These threats have been entered into the inner-most *urgent issues* ring.

The radar serves to provide an overview and to systematically record the current situation, as well as forecast developments. In the following, we will address each of these developments and individual threats in more detail.

3 Evolutionary threats

Technological innovation, new applications, society's evolved approach to the Internet and changed parameters create new possibilities, but also new threats. Many of the topics and threats depicted on the radar can be deduced from over-arching processes or developments:

3.1 The increasing complexity of society and the Internet

Today's society and Internet use are far removed from the turn of the millennium when the dot.com bubble burst. The coming years are set to progress in a similarly dynamic way, providing numerous innovations. The interplay between the Internet and society is becoming rapidly and relentlessly more complex, with the number of new interaction and combination options between human, machine, services and manifold interlinked processes on the rise. Some of these interaction and combination options between human and device, emerging in great numbers on a daily basis, make way for entirely

new attack scenarios. We cannot foresee these scenarios purely by looking back. This means that we have to differentiate between threats that are predictable and can be modelled and those which cannot be foreseen in principal.

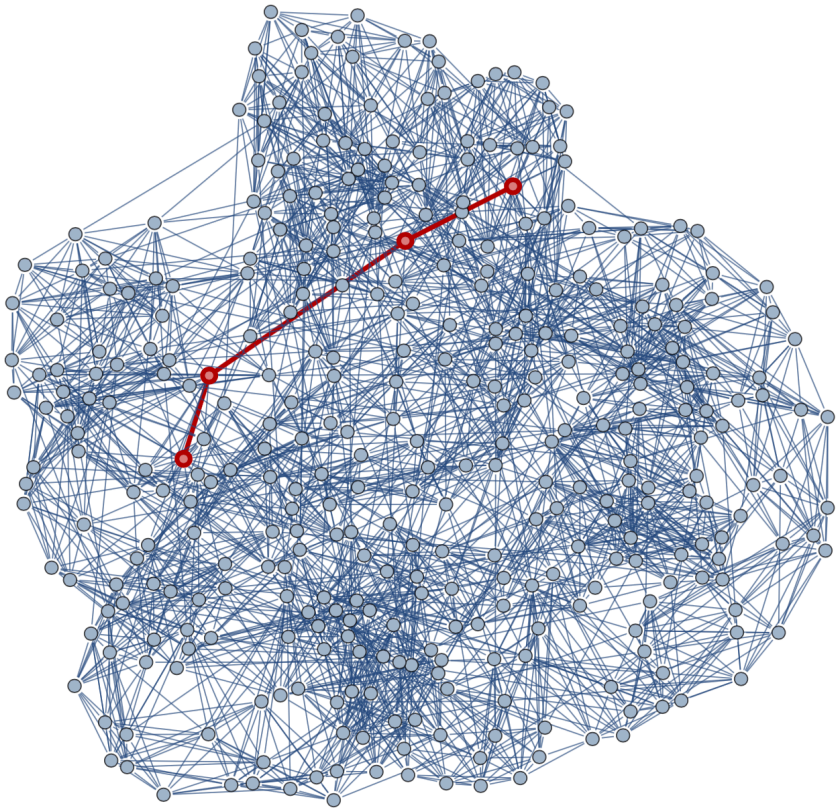

Figure 2 – Simplified overview of the complex Internet-society interaction system The nodes represent people, machines, applications and services that can interact with one another in diverse ways. Every new node disproportionately increases the number of possible new interaction paths (depicted as lines) between the nodes.

The more interconnected we are, the more of these nodes are introduced into the Internet-society interaction system. It is from these numerous and sometimes surprising new interconnections arising every day that we can deduce observations on the current threat status:

New, innovative attacks	The number of new attacks in qualitative terms, based on new interaction paths, will increase. These entirely new attacks need not necessarily be particularly technically advanced. As the basic protection of newly introduced systems and their networks is often insufficient and the new interaction paths are not yet well understood, surprising new attack routes are created continuously.

Predictability	The predictability of attacks will decrease. Trends and developments such as the *Internet of Things*, *smart home*, *smart grid*, etc. are currently at the forefront of this development and the resulting threats.
Prevention	The wider the variety of opportunities for attack, the more difficult prevention becomes. In addition, attacks that are new in qualitative terms cannot generally be foreseen. Existing security systems and services can only provide protection against scenarios that they have already modelled.
Remote effects, cascades	In complex systems like the one depicted in Figure 2, components that are presumed to be unrelated are also connected and can at times influence one another in many ways. This means that attacks on remote system components (or components that were previously isolated) can suddenly have a direct impact on one's own components. Moreover, minor (or well-intentioned) interventions at one location within the system can lead to severe or unforeseen effects at an entirely different system location ("cascades"). For this reason, we expect to see more attacks on subsystems and suppliers aiming to compromise a primary target. Furthermore, we expect to see increasing incidences of small mistakes or attacks causing surprising damage by means of a cascade.

An example to illustrate these mechanisms:
Everybody knows what GPS devices are, and they are used in positioning for a variety of purposes. What is less well-known is that several critical services and devices depend on GPS signals to provide them with the accurate time and to synchronise processes. Should there be a GPS system outage, whether it be an accident (resulting from extreme sun activity, a configuration mistake, jamming) or an attack, it would compromise more than just navigation systems.

An example: In San Diego, US, GPS signals were interrupted by unintentional jamming in 2007. The interruption led to an outage among *emergency pagers*, *mobile phones*, *traffic management systems* and *ATMs* for two hours across the entire city.[2]

[2] http://www.newscientist.com/article/dn20202-gps-chaos-how-a-30-box-can-jam-your-life.html

Since this incident the dependence on GPS for timekeeping and synchronisation has grown even further. Uncountable services that do not seem to be in any way related to navigation or positioning can be affected:[3]

- Communications systems, telephones, mobile and data networks
- The power grid
- Financial transaction systems
- Global transaction synchronisation
- Distributed systems and sensors

The potential damage that could be caused by a GPS signal outage is almost impossible to forecast. Should there be an outage of this kind, there would be a cascade of repercussions. Prevention is very challenging, as GPS receivers built into comprehensive systems cannot simply be replaced.
After the event, it is easy to explain the described outages, because, in the case mentioned above, the interdependencies were correctly identified. It would be quite difficult, however, to list the current dependencies on GPS timekeeping in full.

3.2 Innovative dynamism

Continuous innovation and the sustained improvement of existing technologies, coupled with a fall in prices, make many types of attack more readily accessible. Presumed security

- based on the limited availability of the technology used in attacks,
- the technology being expensive
- or of a limited performance capacity

will be relativised over the course of the coming years. For example, new, surprising applications and attacks are to be expected in the imminent future due to the general accessibility of 3D printers, drones, robots, etc.

3D printers	Presumed security based on the complexity or singularity of mechanic elements will become obsolete. Mechanic keys and specific tools are increasingly easy to make and to copy. Replacing the security elements effected by this is often very complex and expensive, and cannot always be done with the speed required or simply by updating software.

[3] http://www.gps.gov/applications/timing/

Drones, robots	Both drones and miniature robots can be operated by remote control, which enables them to overcome access barriers with ease. The current presumptions on physical access protection must be rethought. We will see an increase in attacks prepared by spying on physically inaccessible areas. Access systems that do not grant access into secure areas, but allow people to leave the area unhindered (e.g. emergency exits, fire doors, garage doors) can be easily overcome by infiltrating robots.
Software defined radio (SDR)	As software defined radios (SDRs) become more widespread, there are more types of radio networks and control systems for attackers to target and doing so becomes easier. Using undocumented protocols will no longer provide the same presumed security. As a result, presumed security based on privileged access to radio equipment and frequency bands will become obsolete. There will be more numerous attacks on all types of radio remote controls and communication devices (affecting vehicles, buildings, traffic, access management, WiFi, GSM, GPS, etc.). Nowadays, GPS jammers can be bought for less than USD 100, for instance.

3.3 The Internet and machines

Spurred on by connectivity available anywhere at any time and the persistent miniaturising of components, more and more machines, devices and sensors of all kinds are connected to networks. This development is rapidly gaining ground in various fields. Alongside control systems that manage industrial processes and power flow, we are now seeing an increasing number of devices and sensors that influence our daily lives. The coveted energy turnaround via a smart grid, smart homes, smart traffic controlling and smart cars, wearable devices and robotics are all prominent examples of this trend. The more widely these technologies are used, the greater the potential for attack. Malfunctions and online attacks will increasingly cause non-virtual damage, with potentially fatal consequences for human beings, the environment, society and material objects. Devices are ever more interconnected, be this purposefully or unintentionally, and so we expect more attacks in this area in the coming years.

Industry control systems ICS/SCADA	Vulnerabilities in ICS/SCADA systems and the tools used to attack them are spreading more rapidly than the systems can be protected. Successful, targeted attacks on control systems of this kind will become more frequent. Built-in, inaccessible control systems without an integrated mechanism with which to securely update software cannot be protected, or at least not without incurring sizeable costs. Furthermore, such control systems are in use for far longer than typical end user systems, such as PCs, tablets or mobile phones. Many of the control systems currently fulfilling vital roles are outdated and were constructed at a time when the threat environment was comparably harmless. As a consequence, these systems are now exceptionally vulnerable and could, in part, be compromised by trivial attacks.
Smart home, smart grid, smart car, smart whatever	Strong competition, the fall in prices and miniaturisation are accelerating the spread of smart systems and devices of all kinds. Security often plays a subordinate role in their design. • There is a lack of awareness of complex, innovative attacks. • Time to market is more important than security. • The security of individual components and of the interplay between many components is still inadequately understood. • Too few resources have been allocated to effectively securing extremely miniaturised devices. These systems are still often used for innovative purposes not originally intended during the design phase. This leads to control systems of this kind or their communications being underprotected. We expect a rise in attacks and new extraordinary outages causing damages of a non-virtual nature.

3.4 Automatic security updates

In an increasingly high-risk environment, the ability to easily update a system with the most recent security attributes is of paramount importance. Operating system manufacturers and popular software products (Windows, web browsers, app stores, etc.) have recognised this and driven forward the user friendliness and automation of security updates.

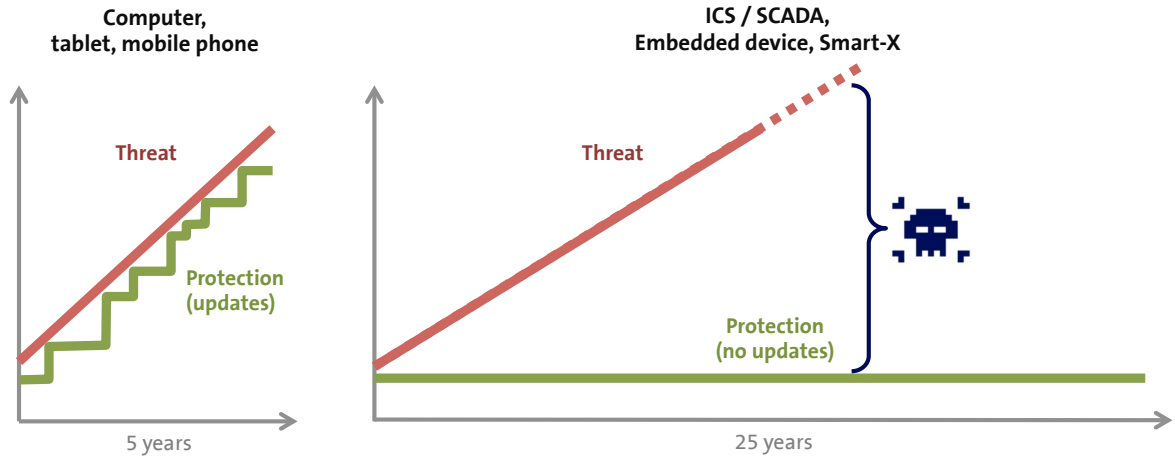

Figure 3 is a rough sketch of both threat development and the development of protection by means of security updates for average computers. Security updates allow protection to be regularly adapted to new threats.
Control systems of all kinds (ICS/SCADA, Smart-X, etc.) that do not have a mechanism to rapidly and easily carry out updates are becoming increasingly vulnerable. The threat increases, and the level of inherent protection decreases, as depicted in

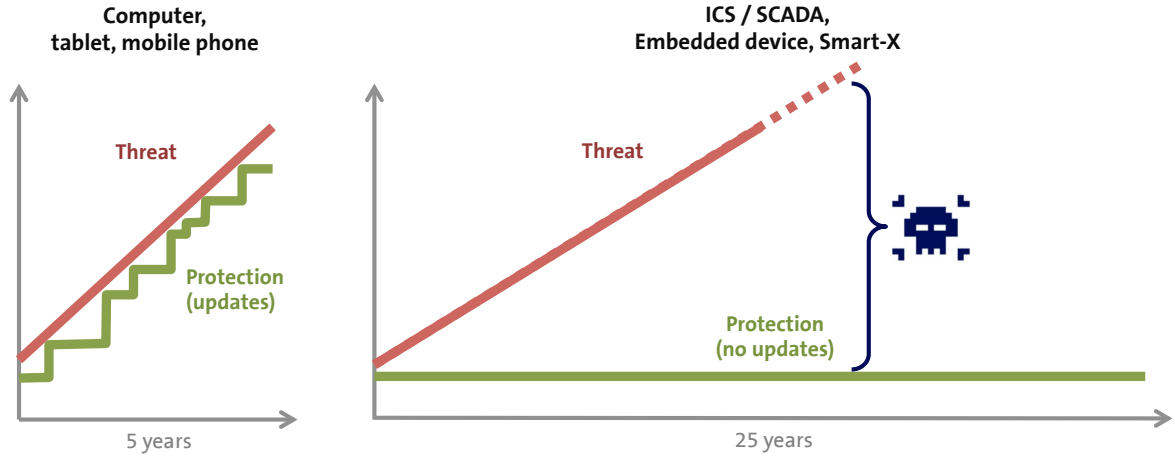

Figure 3. This is aggravated by the fact that systems of this kind are usually in use for far longer than PCs.

Effective update mechanisms for all networked systems are an essential prerequisite for secure operations over a long period of use.

Products and networked devices without security update mechanisms must be considered a certain indicator of future attacks or outages.

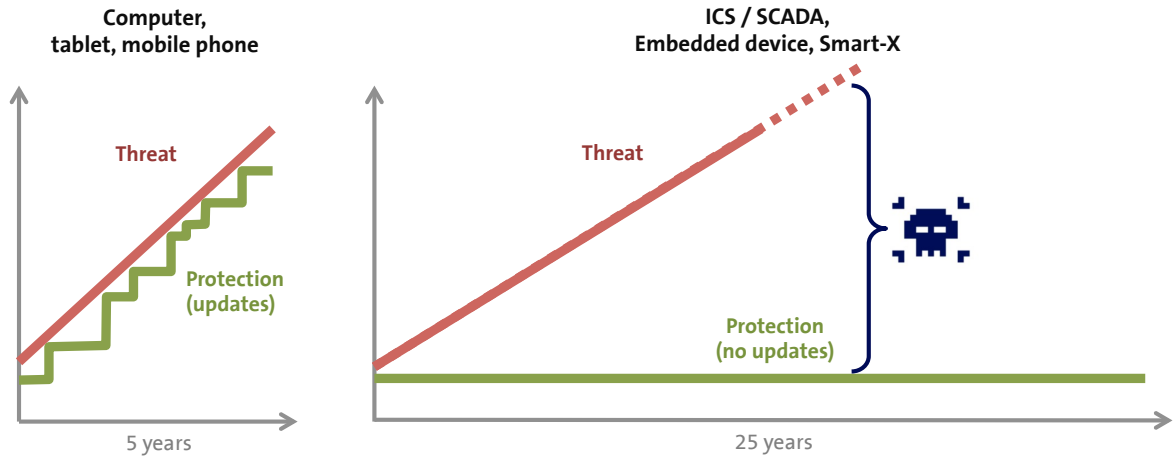

Figure 3 – ICS/SCADA systems are often in use for a long period of time without the option to carry out security updates, making them increasingly vulnerable.

3.5 Legacy systems

Many IT systems and the applications which run on them are used far beyond the shelf life indicated by the manufacturer. Systems in this position no longer receive support from the manufacturer and use outdated operating and development environments and communication protocols. In addition, they rarely have the protection mechanisms we would expect to be installed on PCs (i.e. anti-malware, exploit mitigation). These systems are typically complex and fulfil critical, specialised functions – which are both reasons that speak against replacing them.

Any yet legacy systems are under the same pressure to be networked, both directly and indirectly, internally and externally. These systems' capacity to avert attacks remains constant, while the risk to which they are exposed increases steadily, as depicted in

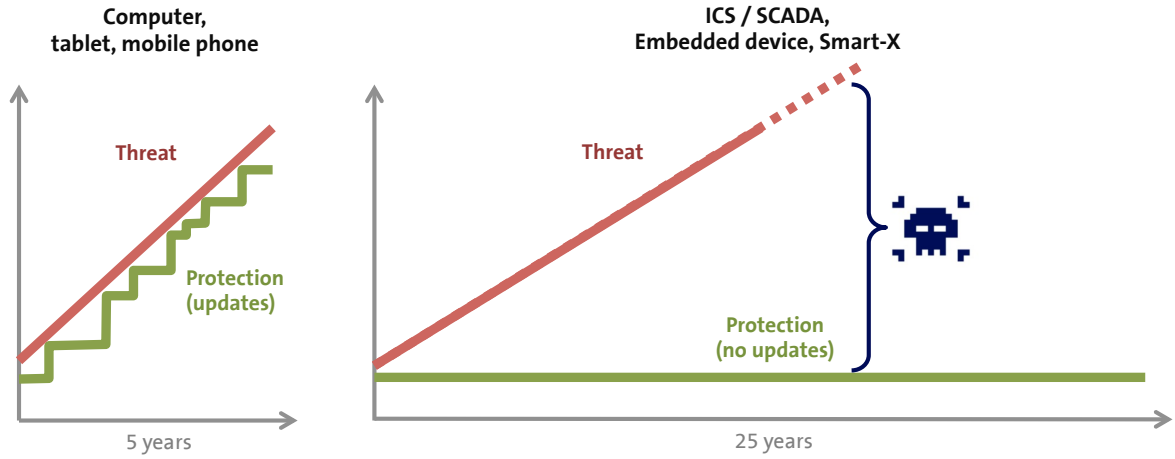

Figure 3.

Legacy systems and protocols	We anticipate more attacks on critical and outdated systems and protocols. As specialist knowledge of the systems becomes more widespread, risk increases.
Networking and API	Legacy systems that have no direct contact to the outside world are increasingly connected to modern API interfaces. This exposes the systems, their data and functions that were once shielded from the outside world. We expect to see APIs and machine-to-machine protocols and communication become even more common, outstripping current protections areas, resulting in new, innovative attack vectors. In addition, we anticipate an increase in data breaches that will expose data from formerly isolated operating systems.

3.6 Software complexity

Despite good progress and considerable investment into the development of secure software, the industry itself has not yet been able to develop and bring to the market truly secure software. Only four in ten major software manufacturers have been able to reduce the number of vulnerabilities in their products over the past 12 months in comparison with the average recorded over the past five years. Figure 4 shows us how software vulnerabilities have developed over the past 20 years.

Software vulnerabilities	We expect to find several further vulnerabilities, especially regarding products that occupy a large market share. Systems that are not immediately perceived as computers, such as control systems, Smart-X and sensors, will not be exempt.

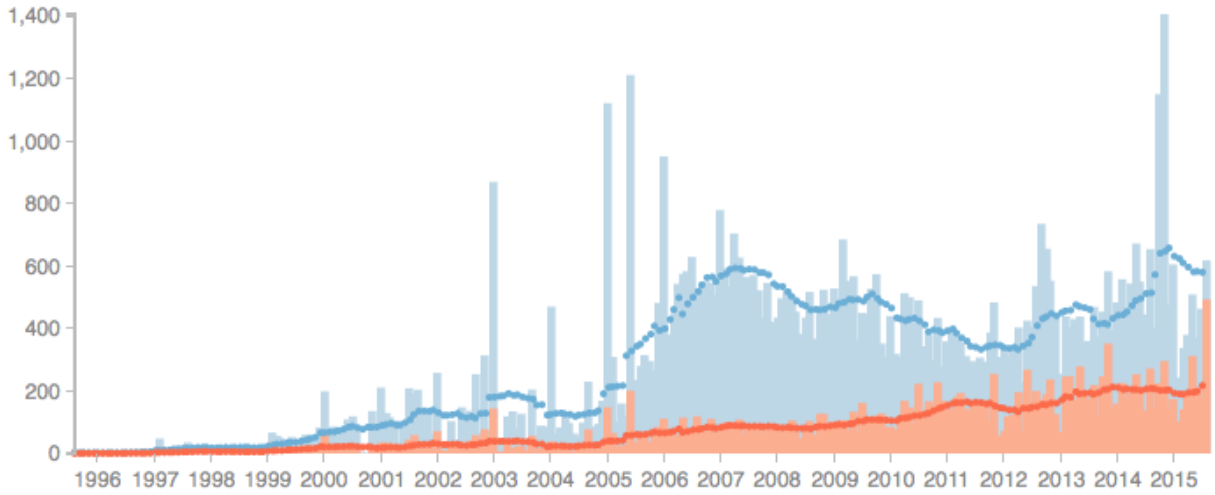

Figure 4 - Vulnerabilities published by month from 1995 to 2015. In red: vulnerabilities in products from the top 10 manufacturers. The lines illustrate the average over the previous 12 months.[4]

Effective software update mechanisms that are able to rapidly update a large number of affected systems will become more important. Products and networked devices without mechanisms of this kind must be considered a certain indicator of future attacks or outages.

4 Threats from attackers

The threats presented thus far result from the development of the Internet, of technology and society, without any particular actor having planned, controlled or initiated a threat.

In part 4, in contrast, we will be looking at threats caused by specific actors.

In doing so, we differentiate between five groups of actors with different goals, resources and approaches. These groups are listed in Figure 5.

[4] http://techzoom.net/BugBounty/SecureSoftware

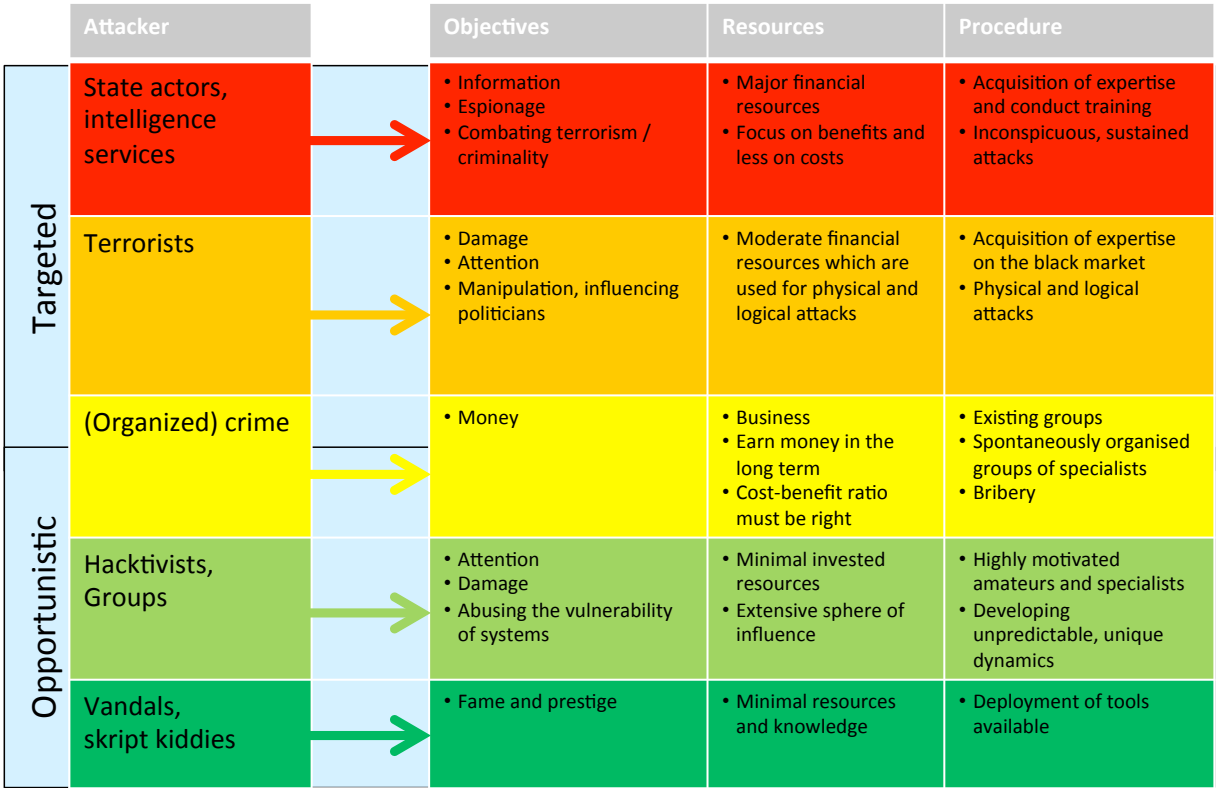

Figure 5 – Classification of attackers

Furthermore, we differentiate between *opportunistic* and *targeted* attacks, although the distinction between the two is hazy.

Opportunistic	Actors take opportunities online, either by chance or because the target is not adequately protected.
Targeted	Actors have clearly defined objectives that they pursue consistently and usually with the backing of considerable resources (finances, expertise, human resources, materials). Attackers of this kind are often relentless. They pursue their goals over a longer period of time and via multiple parallel channels.

4.1 State actors and secret services

States and secret services have conducted espionage and sabotage for as long as we can remember. Cyber espionage and sabotage is increasingly incorporated into military defence and attack strategies. Numerous states are currently pursuing a vast expansion of their offensive and defensive cyber skills.
As opposed to cyber criminals and other attackers, states have direct access to critical Internet infrastructure components (i.e. the Internet backbone), and service providers

and manufacturers are obliged by law to cooperate or monitor events. State activities range from systematic, comprehensive Internet traffic monitoring to secretly infiltrating other countries' (or competitors') target systems' hardware and software with malware. One objective is to gather information, another is to use hidden implants (i.e. back doors and kill switches) to prepare for a sabotage scenario should it become necessary. In the name of anti-terrorism and to keep opposition in check, Internet data is systematically and extensively filtered.
State attackers have vast resources at their disposal and the stamina to pursue a target persistently and via multiple channels of attack over long periods of time.

Supply Chain	We must work on the assumption that parts of our country's critical infrastructure are already compromised. In future, the integrity of delivered goods will have to be challenged and questioned to a greater extent.
Industrial espionage	Much of the value creation in our country results from the valorisation of intellectual property rights and copyrights. We expect to see an increase in attacks for industrial espionage purposes.
Sabotage/preparation	Secret services will employ more kill switches and other preparation measures to prepare sabotage should it be required. Both hardware and software products are affected by this. A functionality of this kind can manifest itself in the form of "software vulnerabilities" or permanent access accounts for "maintenance purposes". It has become difficult to unambiguously identify a defect as an intentional measure implemented by an adversary. Hardware can also be delivered with circuit breakers and predetermined breaking points, so that the function can be turned on or off from afar using a software impulse.
Mobile communications, WiFi	Mobile and WiFi networks will be more readily attacked, whether actively or passively (sniffing, jamming, spoofing, SS7, etc.).
APTs/zero-day exploits	Sophisticated technical attacks will increase, while simultaneously becoming more difficult to detect.

4.2 Terrorism

Just like criminals, terrorists take advantage of the opportunities the Internet provides. Their goal is not financial in nature, but to draw public attention to their cause and to

influence and manipulate politics and society. This means that they may realistically strive to cause the greatest possible damage to attract the most attention perceivable in an attempt to instil fear.

Misuse of services	An increase of well established services being misused for propaganda and recruitment (e.g. hosting, social media, communications).
DDOS	Distributed denial of service attacks aiming to demonstrate power or inflict the greatest possible damage will increase.
Events	Major events or conferences on delicate topics will increasingly be targeted by cyber attacks. The suppliers and service providers involved in such events will increasingly be attacked.
Electronic media	We expect to see more targeted attacks on all kinds of media that are widely consulted (TV, radio, the web, social media). These targets are well suited to distributing propaganda, instilling fear and demonstrating power.
Critical user accounts	We expect to see more targeted attacks on individual user accounts that are widely consulted (Facebook, Twitter, blogs, etc.).

Major events or services that serve a broad audience (e.g. television stations, major broadcast events such the football world cup) are well-suited platforms for terrorist attacks. Alongside the overarching services, individual accounts (e.g. on Twitter, Facebook, etc.) that reach a wide audience will be in greater danger. We expect to see the number of targeted attacks on services and accounts of this kind to increase.

4.3 Organised crime

Crime and organised crime are among the oldest societal phenomena. History teaches us that criminals acquire and utilise new technologies very rapidly.
Criminals act professionally to achieve their financial goals, both in a target-oriented and opportunistic manner.
Various criminal gangs are specialised in specific areas, such as identifying vulnerabilities, producing malware, selling or renting out tools, managing botnets, recruiting money mules, drafting phishing mails, etc. The boundary between traditional and cyber crime has become hazy with the two complementing one another.
This division of the tasks enables criminals to provide high-quality services and tools, which can, in principle, be sold or rented to any interested parties.

The distribution of tools and services (proliferation)	Tools used in attacks and services that manage compromised systems are becoming more sophisticated and widespread.
Complex attacks	Complex, multi-level attacks (e.g. using DDOS as a distraction) will increase. Phishing attacks are becoming more psychologically sophisticated and better tailored to the victim in terms of formatting, content and timing (spear phishing).
Camouflage, detection prevention,	Malware and attack tools are becoming more adept at avoiding detection by security products.
Persistence	Vulnerabilities are sought out and exploited more systematically. Attacks of this kind are being commercialised and offered to potential buyers.

4.4 Hacktivists

Hacktivists are on a mission, typically within the context of an emotional topic. In order to coordinate an activity, large groups of like-minded individuals can be formed or congregate on social media, often spontaneously and over a very short time span. Targets for these attacks are either determined by the topic at hand (those who harm the environment, the government, dominant companies, etc.) or decided upon spontaneously. The actors are highly motivated and now have professional experts among their ranks. It is easy for uncontrollable group dynamics to develop.

Social media	We expect to more spontaneous campaigns and attacks coordinated via social media directed at targets that are directly or indirectly linked to the trigger topic.

4.5 Vandals, script kiddies

Vandals and script kiddies are non-professional attackers who conduct attacks and experiments out of boredom or a compulsion to prove themselves using readily available tools. They have no specific target in mind. Instead, the attackers seek to boost their reputations with minimal invested means and knowledge. In line with this, the targets chosen and the timing of the attacks are to be considered coincidental.
These attacks are perceived as omnipresent Internet background noise and should be dealt with as such. All networked systems should have basic protection that automatically averts attacks of this kind. As information is more readily available and the tools required are easier to use, these attacks will continue – basic protection must be consistently monitored and adapted.

5 Threats resulting from our networked society

5.1 Loss of orientation

Technical innovations and new Internet applications are being introduced at high speed. Niche players can become dominant providers within a few years, threatening current business models and presumed security. This is a tall order for people and the economy, with entire sectors being called into question over night (e.g. taxi services v. Uber, hotels v. AirBnB). It goes without saying that fighting off, capping or reversing this development has no hope of success in the long term.

„Because there is no army that can hold back an economic principle whose time has come"
John Donovan, AT&T

Our economy, our society, our legal framework and the emerging dynamics still run the risk of not being able to fend off the risk that the Internet has brought upon us, which could have fatal consequences for generations to come.

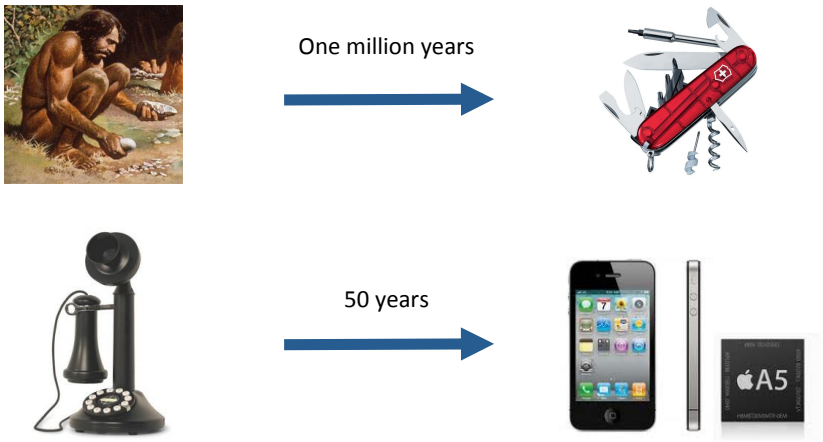

Figure 6 – New technologies are being introduced at ever greater speeds, posing a considerable challenge to people and to society.

We have to learn to deal adequately with this immense dynamism and agility in the Internet era on all levels. Developments such as cloud computing, the shared economy, distance learning, etc. demand a new mindset in order to adequately evaluate the advantages and risks. So as not to rush unaware into new, unwanted dependabilities, these risks and possibilities must be identified at an early stage, and we must have mechanisms in place to make the best of the potential.
The new replaces the familiar, the existing is in a constant state of change. It is becoming increasingly difficult to find one's way among this diversity, faced with this information flow.

Training	Our education system is still oriented towards primarily teaching skills that are needed during the fifth phase of industrialisation.[5] The danger of being overwhelmed by developments as a society and as an economy is intensifying.
Politics and law	Our legal framework can hardly keep up with the speed of the developments in the Internet era. The legal field rarely has access to knowledge in the area of cyber crime, which puts it at risk of introducing inadequate laws, and also of new laws being hopelessly outdated even as they first enter into effect. The current debate on intrusion software within the framework of the *Wassenaar Arrangement* aptly illustrates this challenge.[6]
People	People are increasingly challenged and overwhelmed by the rapidly increasing complexity and diversity of services, and of interaction and combination possibilities. This applies both to administrators of ICT systems as well as to end users. It provides attackers with a whole new range of opportunities. Complexity is security's greatest enemy, from a technical, human and social perspective.

5.2 The erosion of the private sphere

Every person has a limited range of personal attributes that can be given as identification to service providers and authorities. The number of Internet services that we use now use on a daily basis is constantly on the rise. Each and every data leak - from service providers or the authorities - reveals a few more personal attributes used to identify a person. Attributes such as e-mail addresses, passwords and security questions can be changed after a data leak fairly simply. Static attributes, such as social security number, date of birth, place of birth, gender or place of residence cannot be changed - or only to a very limited extent. This development, alongside the extent of personal data that is visible on social media (OSINT), means that it will not be possible to maintain the confidentiality of personal attributes in the long term.[7]

[5] https://www.youtube.com/watch?v=Optk-gYgFo8
[6] https://www.eff.org/deeplinks/2015/05/we-must-fight-proposed-us-wassenaar-implementation
[7] http://techzoom.net/Publications/Papers/databreach

Protecting private data that has been made available to third parties is becoming increasingly difficult. Attacks that use personal and private data to simulate trustworthiness to manipulate the targeted person into doing something will become more frequent and more sophisticated.

Identity theft	As the private sphere is increasingly eroded, attacks like identity theft will multiply. Attacks are becoming more and more sophisticated (personal) and detection is becoming more and more difficult, if not impossible.
Data misuse	The great and ever expanding volume of personal and meta data stored by the state, third parties and service providers increases the danger of misuse and monitoring.
One-way street	Personal data that are issued *only once* (voluntarily or involuntarily), cannot be revoked. A data leak or faux pas is enough to compromise someone's private sphere *forever*. Consequently, we must work on the assumption that a large part of our personal data (i.e. contacts) cannot be kept private in the long term. For example, many applications ask the user for access to contact data upon start-up. Even if the request is mistakenly approved only once, the contact data flow can no longer be reversed.

5.3 Loss of trust

The constant flow of information and the increasing misuse of private and personal information will cause us to lose trust in services and information in general.

Loss of trust	Recognising attacks that use sophisticated methods and personal and private data to simulate trustworthiness will become more difficult. Attacks of this kind will become more commonplace and more successful.

6 Summary

New technologies always lead to insecurity when they are first introduced. Adapting technologies and learning to deal with this situation correctly is a process that will take time. We must recognise which risks we can avoid as individuals (as users or organisations) and which threats are systemic, and so are created and can only be sustainably tackled at the society level or with international collaboration.

What we learn from these reflections:

- Internet security is primarily a complexity-management problem. Observing technology alone will not be enough to give us an understanding of the threats.
- 100 percent prevention is an illusion. Both companies and authorities must assume that their infrastructure will be compromised (or that it has already been compromised).
- Organisations need to ensure that any compromise is detected and mitigated as swiftly as possible.
- Any compromise detected must be dealt with following a predefined, well versed process and not an exception process.
- Products and networked devices without effective software update mechanisms must be considered a certain indicator of future attacks or outages.
- We are working on the assumption that targeted attacks will become more frequent and that predicting the nature and timing of these attacks will become more challenging.

7 Glossary

0-day/zero-day exploit	A software exploit recognised the first time a security gap is published - or even beforehand. This means that the exploit is made available before the software manufacturer has a security patch at the ready.
API	The Application Programming Interface enables programmes to directly exchange data (machine to machine) using a common language.
Back door	Software back doors are used to gain access to a computer by circumnavigating its access protection.
Botnet	A network of a large number of compromised computers that are controlled centrally by a botmaster.
Defacement	Uploading unwanted content to a hacked website.
DoS, DDoS	*Denial of Service (DoS)* A large number of requests causes the system to crash. *Distributed Denial of Service (DDoS)* A DoS attack is launched simultaneously by several distributed systems (e.g. a botnet). It is no longer possible to simply block the attacker.
Exploit	Programme, code or a series of commands used to take advantage of vulnerabilities in software.
Exploit mitigation	A general term for techniques that make it harder or impossible to abuse system vulnerabilities.
GPS	Global Positioning System A global satellite navigation system used in positioning and precision timekeeping.
ICS	Industry Control System For more specific information, see SCADA.
ICT	Information and Communication Technology
Jamming	The deliberate disruption of radio communications.
Kill switch	Hidden software that can disrupt or shut down the functioning of a system when given the command from afar.
Malware	Software that executes damaging, unwanted functions.
Money mule	Criminals convince people to take money from "clients" and, after having taken their cut, pass it on to a money transfer service. Money mules believe they are working for a legitimate organisation.
OSINT	Open Source Intelligence gathers information exclusively from sources that are accessible to the public.

Patch security update	Programming code that replaces defective software to eliminate security gaps.
Phishing	Users are tricked into disclosing sensitive data (using e-mails, giving fake instructions).
SCADA	*Supervisory Control And Data Acquisition System* Used to monitor and manage technical processes (e.g. industrial processes).
Vulnerability	A vulnerability or weak spot in hardware or software that attackers can use to gain access to a system.
SDR	*Software Defined Radio* Universal high-frequency emitter and receiver, which uses software to process signals, which the user can adapt to different protocols and applications.
Smart grid	Intelligent power grid The smart grid interconnects and manages electricity generation and storage, electrical appliances and energy transfer and distribution networks.
Smart home	The overarching term for networked, partially automated energy management, entertainment and security in homes.
Social media	Websites that enable users to interact via personal profiles (e.g. Facebook, Twitter, LinkedIn, Xing).
Spear phishing	Targeted, personalised phishing attacks.
Spoofing	Deceitful behaviour in networks intended to conceal the actor's identity.