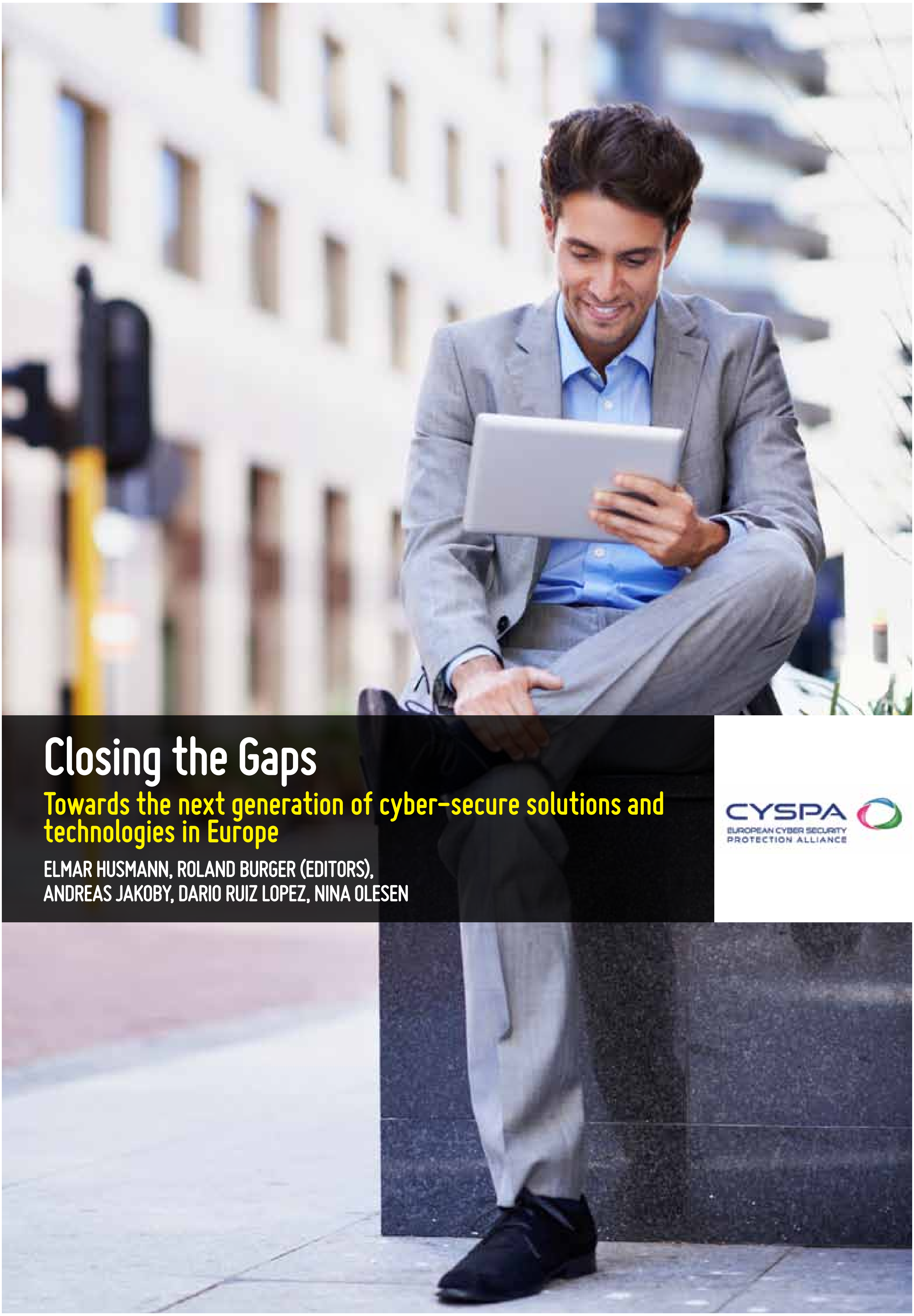


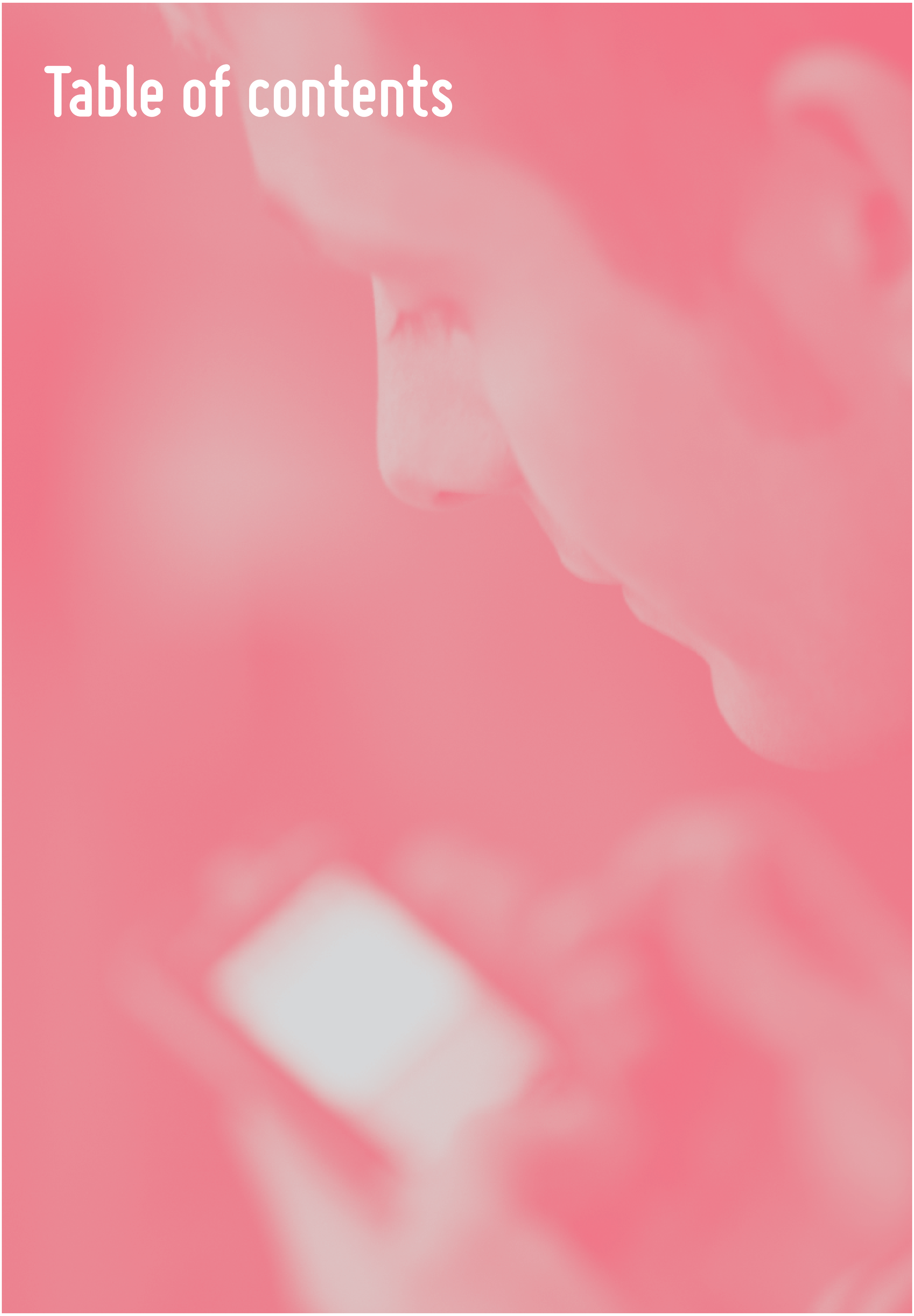
Closing the Gaps

Towards the next generation of cyber-secure solutions and technologies in Europe

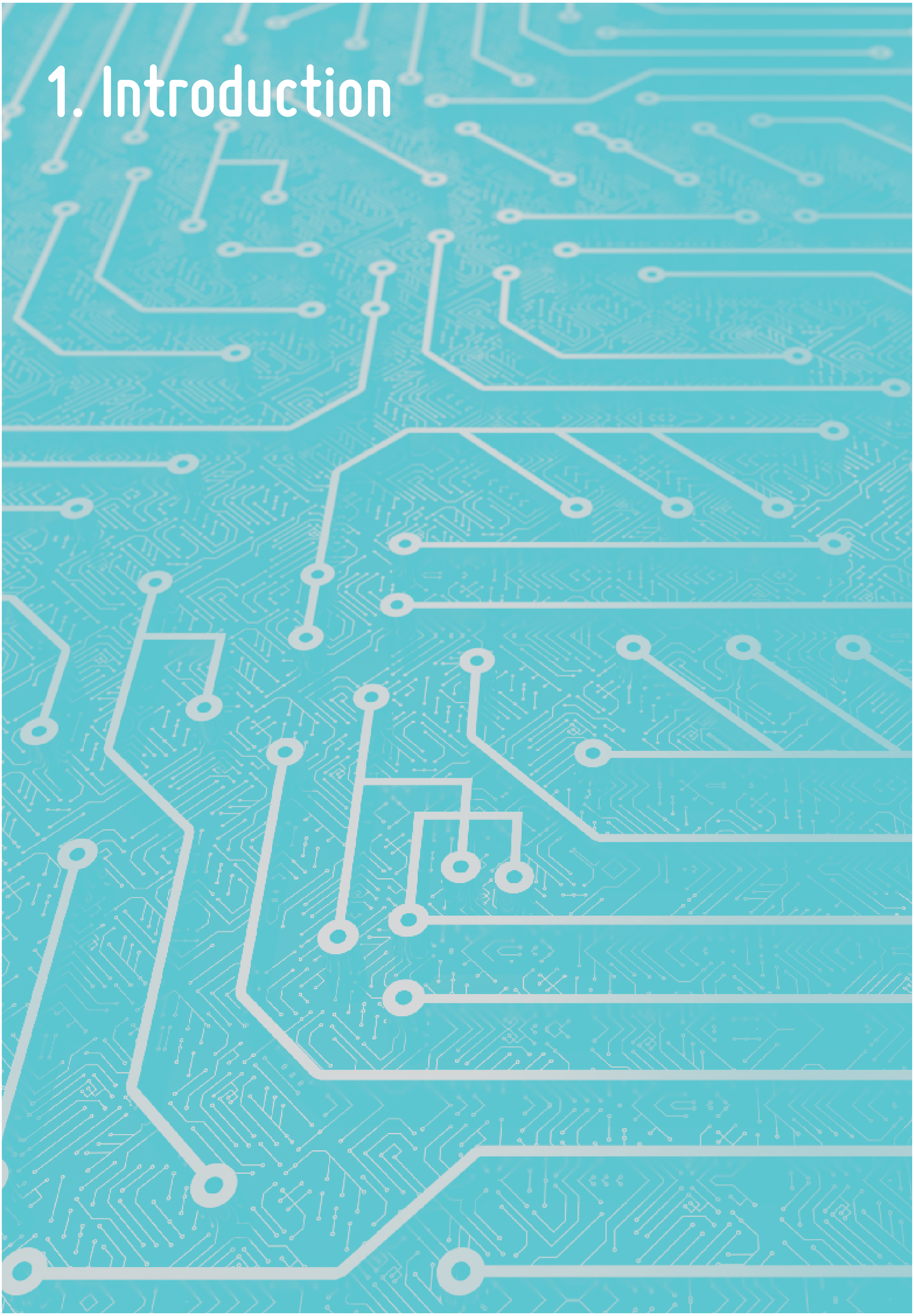
ELMAR HUSMANN, ROLAND BURGER (EDITORS),
ANDREAS JAKOBY, DARIO RUIZ LOPEZ, NINA OLESEN

CYSPA
EUROPEAN CYBER SECURITY
PROTECTION ALLIANCE

Table of contents



1. Introduction



1.1. Overview of technology and solutions Gaps

We need to ensure that our current and future digital technologies, our diverse electronic devices and Internet services are trustworthy and protected against cyber criminal activities. We have described a broad range of cyber threats and risks in detail in our CYSPA guide on „Understanding and Managing Cyber Risks". We have also described how trends such as the Internet of Things, Cloud Computing or Big Data are creating further cyber risks and allow for new forms of threats.

These cyber risks are real, multifold and potentially harmful. They may affect the individual user but also entire organizations in the same way as criminality is since longtime a facet of other areas of our everyday life. We have also wittnessed the rise of organized cyber criminality, more complex threats and sophisticated attacks.

The 10 Gaps that are described in this document summarize larger areas of CYSPA analysis on emerging technologies and solutions that have the potential to improve European cyber security in the next years. More corresponding detail for each of these areas can be found in the input documents that are mentioned in the methodology appendix.

A cross-cutting concern in all our analysis is that in the future an approach to cyber security protection is needed that is active - even pro-active - rather than re-active as it is still mostly today. This means that cyber security concerns are taken into account not as a technological- and ICT management afterthought but already at design time of new ICT products and services.

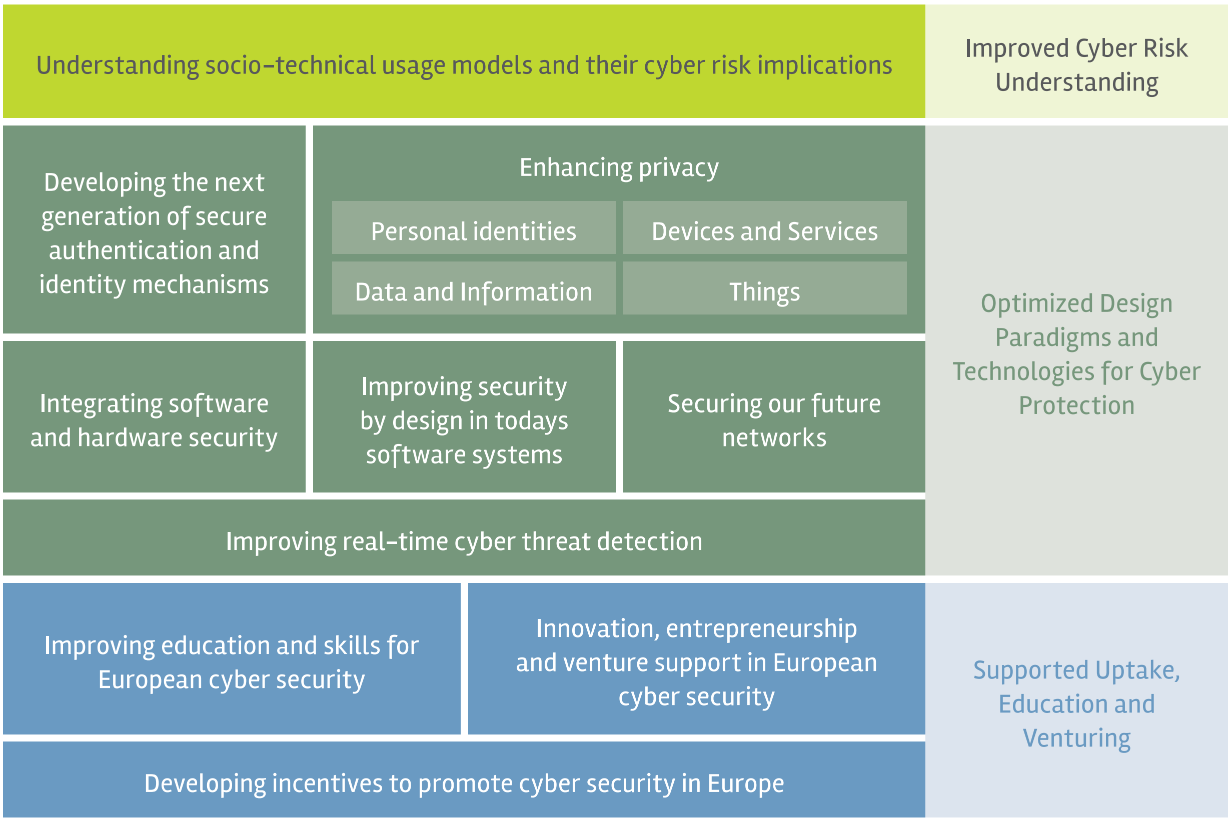
The same applies for critical infrastructures where risks need to be analyzed early-on and more systematically in order to implement multiple levels of protection. This will further benefit from a range of new technologies and design paradigms that already imply a higher concern for cyber protection.

The transition towards a pro-active approach on cyber protection is supported by different means: education and skill programmes - at the level of users as well as that of experts and developers. At the same time, specific innovation transfer, entrepreneurial and venture support mechanisms need to support a strong role of European industry and the link to research institutions in this growing market.

Finally, Europe should consider specific incentives for industry to promote, support and value cyber security. This also includes incentives for information sharing. Cyber security protection and the related concern of cyber privacy protection are not only in the interest of the individual organization but they represent wider challenges for society. Only concerted efforts of all actors can address these. The federal government of Germany has e.g. recently published a comprehensive Digital Agenda Strategy that includes a legal duty1 for organizations that run critical infrastructure to report on cyber incidents.

More corresponding detail for each of these areas can be found in the input documents that are mentioned in the following methodology section.

Figure 1:
Overview of technology and solutions Gaps



Understanding socio-technical usage models and their cyber risk implications

Improved Cyber Risk Understanding

Developing the next generation of secure authentication and identity mechanisms

Enhancing privacy

Personal identities

Devices and Services

Data and Information

Things

Integrating software and hardware security

Improving security by design in todays software systems

Securing our future networks

Improving real-time cyber threat detection

Optimized Design Paradigms and Technologies for Cyber Protection

Improving education and skills for European cyber security

Innovation, entrepreneurship and venture support in European cyber security

Developing incentives to promote cyber security in Europe

Supported Uptake, Education and Venturing

The 10 Gaps can be categorized on three levels:

1) On the level of risk understanding. This includes the modelling and analysis of different factors and dependencies that contribute to cyber risks. Such as taking social factors – e.g. user or group behaviour – into account as well as technological and other context factors.

2) On the level of the technical architectures, interlinked solutions and design paradigms for cyber protection.

3) On the level of supporting elements for the uptake of cyber security awareness and design paradigms – including e.g. education and skill building, innovation transfer or entrepreneurial support.

1.2. Methodology

The consolidated Gap analysis presented in this document is derived from several CYSPA analysis tasks and corresponding deliverables of the CYSPA project from two workpackages (WP3 and WP2). The different inputs that have led to this Gap analysis are:

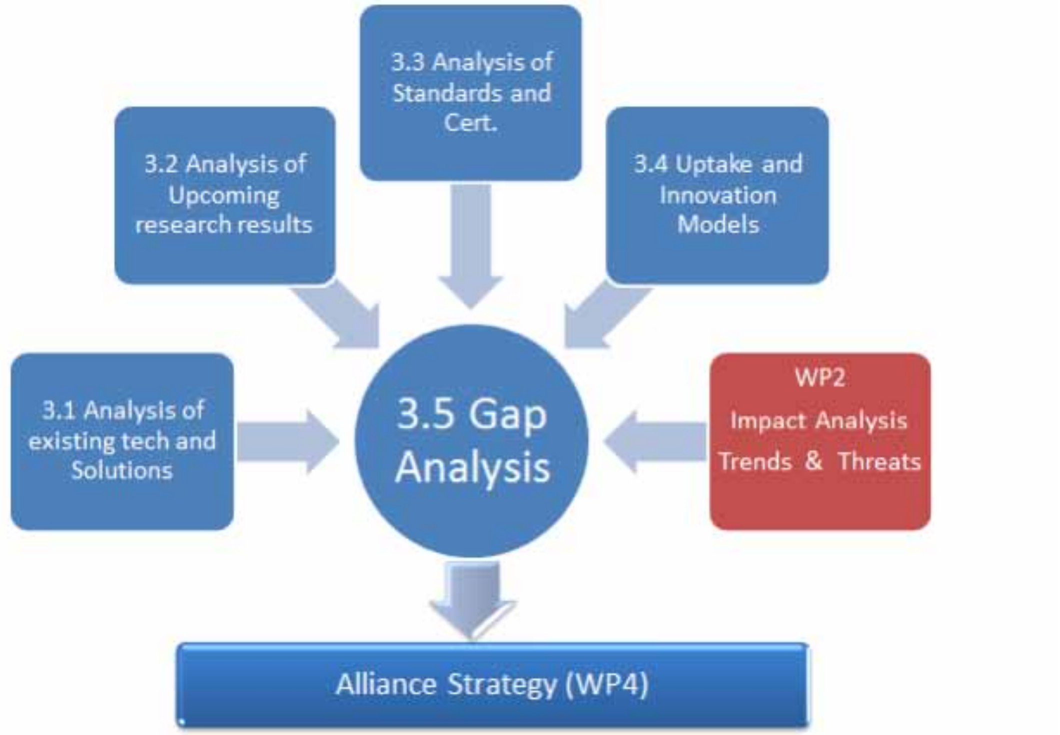
- The CYSPA publication "Understanding and Managing Cyber Risks – A guide to risks, threats and impact in European cyber space" that was derived based on the WP2 deliverable D2.3 (Trends and threats – impact contribution).

- The CYSPA analysis of the "Existing technology and solutions portfolio" D3.1. This analysis provides an extensive overview on existing security technologies, services and solutions in the market. It also provides an overview on European cyber security research projects and their results as well as on education, training and certification programmes. The later part is further supported by the Analysis of "Standards and Certification" in D3.3.

- The CYSPA analysis of "Upcoming research results" D3.2 which describes cyber security research strands as supported by the large-scale research funding programmes in the EU, the US DARPA programme and in Japan.

- The CYSPA Analysis of "Uptake and Innovation Models" D3.4 which investigates mechanisms for the transfer of cyber security innovations from research into the market as well as corresponding European organizations and channels.

Figure 2: Relationship of WP3 deliverables


3.3 Analysis of Standards and Cert.
3.2 Analysis of Upcoming research results
3.4 Uptake and Innovation Models
3.1 Analysis of existing tech and Solutions
3.5 Gap Analysis
WP2
Impact Analysis
Trends & Threats
Alliance Strategy (WP4)

This Gap analysis and the corresponding CYSPA documents that have contributed to it also feed into the overall CYSPA Technology and Solutions Observatory (D3.6) – an online tool that provides dynamic access to the different CYSPA results.

The way how this document is intended to be used is therefore as a possible entry point into CYSPA analysis. Whereas further detail (e.g. extensive overviews on existing technologies by area and vendor) can be obtained via the Technology and Solutions Observatory.

1.3. How the Gaps were derived

The Gaps were derived through a process that involved several steps. In a first step, all input documents from the CYSPA analysis of WP3 and WP2 were screened in detail. During this screening, tags were assigned to recurring themes and security topics. In this context, we focused on topics where the CYSPA analysis highlighted important security vulnerabilities or areas of improvement. We also focused on areas where continuous and long term development of new solutions will be needed.

Subsequently, these tags were clustered into 10 Gaps and for each Gap a few sub-categories were derived. This structure of Gaps was then agreed in the CYSPA consortium and builds the baseline for this document.

As discussed in detail in the CYSPA report on "Understanding and Managing Cyber Risks", several important trends shape the development of our future cyber ecosystems – like the Internet of things, cloud computing, or big data. In the CYSPA Gaps, we have identified cross-cutting cyber security concerns to these trends. Therefore, none of the Gaps is specific to only one trend. However, in many Gap areas these trends are leading to new and extended demands. Where this was the case, it has been highlighted in the Gap description on the basis of examples.

1.4. Input to the CYSPA alliance strategy

The technology and solutions Gap analysis will further be an important input to the CYSPA alliance strategy. The CYSPA alliance strategy will at the same time take other elements into account like the analysis of the European legislative and policy environment for cyber protection as well as the CYSPA analysis of cyber security stakeholders. This is needed to determine an optimal strategic position of CYSPA in the existing environment and stakeholder landscape.

Our socio-technical ecosystems of people, devices, smart things, networks or services are in constant development. New trends – as they were discussed in D2.3 or D3.1 – are shaping it: cloud computing, the Internet of Things, Industry 4.0, or Big Data.

In CYSPA we advocate that cyber protection is not only a separate field, or a separate trend. At the same time, it is a cross-cutting concern in all these developments. The integration of cyber protection concerns from the outset in designing new ICT services will contribute not only to a higher resilience against cyber threats it will also address user concerns e.g. with regard to the protection of personal data and overall security of these new services.

In the following sections each of the 10 Gaps that we have determined will be described in more detail.

2. Gap 1: Understanding socio-technical usage models and their cyber risk implications

The CYSPA report on "Understanding and Managing Cyber Risks" provides an overview of several elements that compose today's complex cyber systems: people and identities, data and information, services, processes and applications, networks, servers, endpoint devices and other physical infrastructure. The report also investigates the cyber threat potentials to the different parts and actors of the ecosystem.

An important aspect in this context are new usage and business models – e.g. the different XaaS (X-as-as-Service) models of cloud computing or new usage models in the Internet of Things – such as the community oriented models of personal health or fitness trackers in the consumer market.

According to EY's Global Information Security Survey 2013 of nearly 2000 industry decision makers, 45% reported an increase in cyber vulnerability due to mobile use, 32% an increase due to social media use and 25% due to cloud use. Hence, new usage models and new cyber risks are two sides of the same coin.

New usage models may create new cyber risks on the side of industry and service providers. Also the acceptance of these models by customer and users critically depends on cyber protection. According to a recent survey by the German ICT industry association BITKOM[2] and the German Federal Criminal Police Office (BKA), cyber risks significantly affect the acceptance of Internet-based services. Already 21% of German Internet users avoid social networks, 24% avoid online banking, 47% would not send confidential documents via the Internet.

The figures are even significantly higher when it comes to more recent and emerging usage models, such as the Internet of Things, Industry 4.0, or cloud computing. Most industry organizations are acting in a similar conservative way as individual users. In a 2013 report by IBM[3] and the EU project TClouds, the surveyed organizations report very high concerns with regard to the use of public and multi-tenant clouds (e.g. concerns about attacks by externals, service interruption and data loss).

Overall, this leads to a situation where cyber security has become a critical success factor and ingredient in the adoption of new IT products and services. But these risks are too little analyzed at early stages when a new IT trend hits the market or even better in the development. The corresponding cyber risks are also too little quantified and transparent to impact business decisions at the board level.

2.1. New usage models – new risks

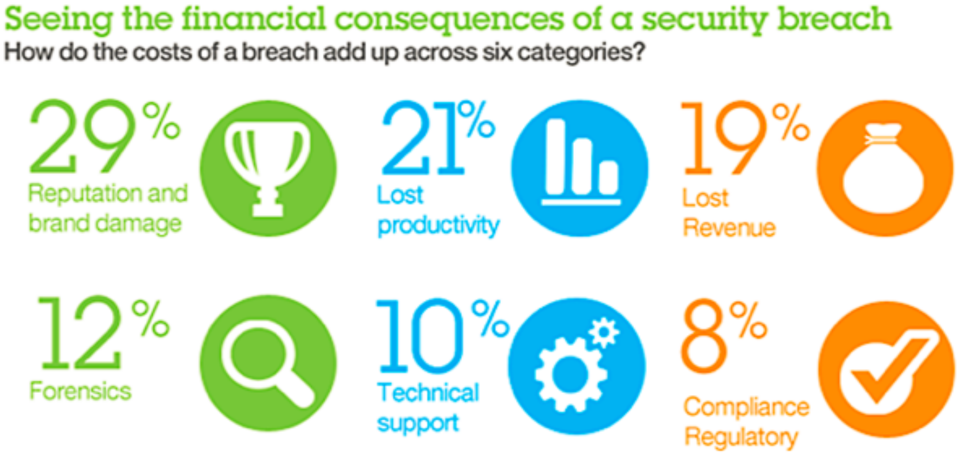
The IBM Cyber Security Intelligence Report 2014[4], has investigated the financial consequences of security breaches for organizations. Over 2/3 of the financial consequences arise in total indirectly from socio-economic effects – in particular (1) damages to reputation and brand image, (2) lost productivity and (3) lost revenues.

On the other side, direct financial consequences such as efforts for forensics and technical support to re-establish services, retrieve data, patch security holes etc. only make up around 22% of the total financial consequences.

This demonstrates that the larger part of the impact of cyber disruptions arises indirectly from the way how the overall service ecosystem is affected. This can imply social effects – like damaging trust relationships to customers or spreading bad reputation – to effects on the business side e.g. on lost revenues due to service downtime or customer business processes that are disrupted.

The CYSPA report on "Existing technologies and solutions" already describes a number of modelling and simulation approaches but mostly these address the technical side of cyber vulnerabilities. In the same way, it will be important to understand and model the impact potentials and the socio-economic risks.

Figure 3:
Multi-facetted consequences of a security breach by percentage of overall financial impact.
Source: IBM Cyber Security Intelligence Report 2014



2.2. From qualitative to quantifiable risks

Where technical risks are more easy to quantify, socio-economic risks are often assessed in qualitative terms. However, the quantification of risks is an important pre-requisite for business cases as well as for sizing risk insurance.

We will have to develop novel approaches to quantify socio-economic risks that arise from potential cyber threats. This needs to be done in close alignment with the understanding of new usage models and their implications. In other words: we need to translate cyber risks from an overly technical view into a business and socio-economic view.

2.3. Understand emergent properties

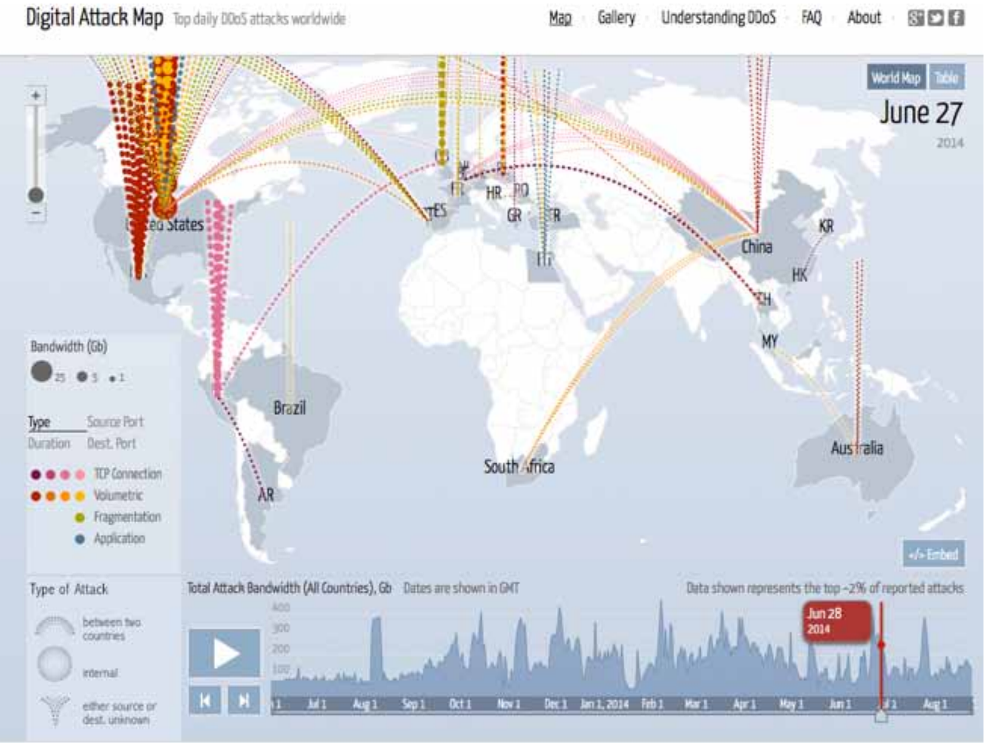
In addition to direct and indirect effects of a cyber incident for a single organization, we have to develop a better understanding of emergent properties at the level of the entire cyber ecosystem. Such emergent properties are e.g. the propagation of attacks across devices or sites as well as other chain-effects that are only possible because of the connection of partners in the ecosystem. Distributed Denial of Service Attacks e.g. use such “snowball” effects to amplify an attack. However emergent properties do not only hold risks or may lead to an amplification of threat impacts.

At the same time, the ecosystem could also respond differently in collaboration of different actors and elements and improve resilience beyond the capacity of a single organization. An example for this is the mitigation of distributed denial of service attacks (DDoS)[5]. Whereas the compute capacity of a single provider is in general insufficient to handle a massive DDoS attack, a concerted effort of multiple providers and the support of large bandwidth providers can effectively mitigate the impact.

On the other hand, this also means that individual cyber risks – e.g. that of a single organization or service – need to take into account how well the organization is embedded into overall mechanisms of cyber protection. This will be an important factor to determine if either a fast resilient response can be triggered in the ecosystem or if in the worst case a threat is simply amplified and carried forward to other actors.

The CTO of the U.S. Department of Homeland Security Peter Fonash has compared[6] the potential for growing the resilience of the overall cyber ecosystem with the functioning of the immune system of the human body. In this context he points out the importance of collective – ecosystem level – response mechanisms to cyber threats that are based on a close (near real time) interaction of actors – including also partially automated technical response mechanisms.

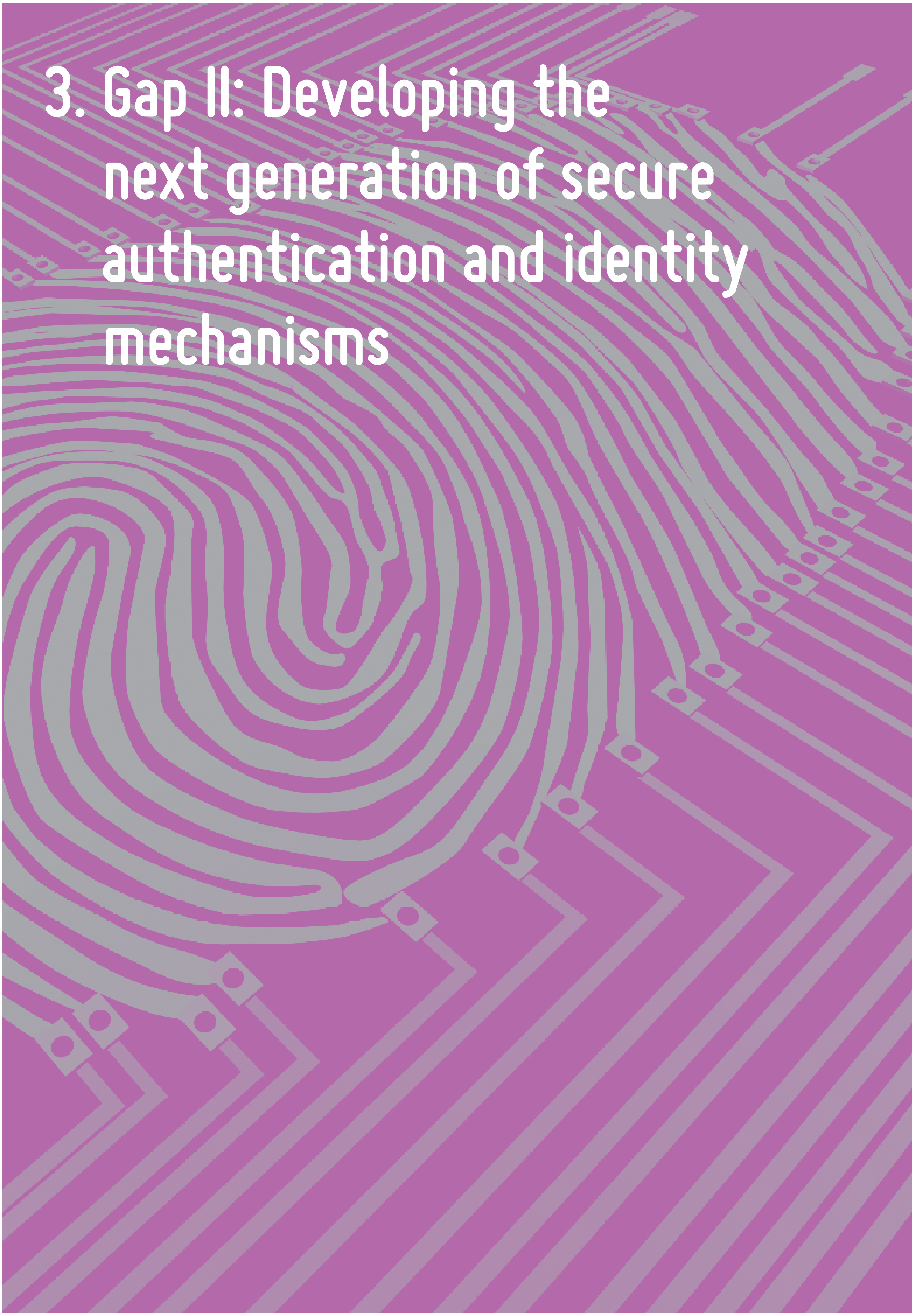
Figure 4:
Visualization of parallel DDoS attacks in the global Internet on a given day.
Source: DigitalAttackMap – a project of the GoogleIdeas Initiative



With regard to new usage models and trends like e.g. the Internet of Things, these response mechanisms are yet to be developed and many risks and ecosystem properties can not easily be determined upfront. This demands specific modelling, simulation and scenario analysis efforts in order to optimize the resilient actions of the ecosystem against different kinds of threats.

This also implies to collect and analyse data from previous cyber security incidents on a large scale – not only from a technical and forensic perspective but also from a socio-economic impact perspective. An example is the Digital Attack Map project that was launched as part of the Google Ideas initiative on using Big Data and Data Visualization for societal challenges and that is based on secondary sources such as newsfeeds, articles and other websites that contain information on recent cyber attacks[7].

3. Gap II: Developing the next generation of secure authentication and identity mechanisms



An important element in proactively addressing cyber risks is to maintain continuous international development efforts on the core technologies that ensure security in our cyber ecosystems – today and in view of future usage models. As we describe in more detail in the CYSPA report on "Understanding and Managing Cyber Risks", many attacks are derived from weak points in the current Internet Protocol (IP) Stack as well as in related implementations. With regard to authentication and secure communication, several security vulnerabilities[8] [9] relate to the TLS/SSL protocol of the IP stack.

Two basic elements in any cyber ecosystem are the trustworthy identification of partners in a communication and the securing of the communication between these partners against eavesdropping and manipulation. Exploiting stolen identities, re-routing communications to criminal sites, spying into communications, altering transactions – all this is routed into attacking the basic transaction and communication security of the Internet.

3.1. The weaknesses of the current TLS/SSL standard

The TLS/SSL standard is the basis for secured transactions in many industries and applications areas – e.g. in secure Web transactions such as online banking or cloud storage as well as for digital communication such as voice over IP (VoIP). It is one of the key security standards in the Internet. Hence, it demands particular attention.

TLS/SSL secured transactions are authenticated using digital certificates (X.509) and use public-key cryptography. This type of communication has two breakpoints, the authentication and the communication itself. The secured communication using public-key cryptography has long been considered unbreakable. However, the growing maturity of quantum computing is challenging the breakability of current public key cryptography and approaches have already been demonstrated – based on quantum computing – to crack the underlying mathematical problems of current cryptographic methods in limited timeframes. At the same time, have quantum computers left the research labs and first commercial vendors have developed such as D-Wave Systems[10] as well as software tool vendors like 1QBit[11]. While this market is still in its infancy, the commercialization of quantum computers may put these technologies soon into the hand of criminal organizations or state-sponsored-teams with the necessary financial and intellectual resources to use them for advanced-persistent attacks.

Breaking the cryptography is not the only possible to attack the TLS/SSL communication. As a complex protocol it involves multiple steps and phases to establish a communication connection. This offers possibilities to exploit protocol weaknesses.

3.2. The broken trust chain of digital certificates

The other breakpoint is the digital certificate. Certificates prove the valid ownership of a public key and the electronic identity of the owner. They ensure that we can identify the opposite partner in a transaction in a trustworthy way. This e.g. prevents us from being re-connected with a criminal "man in the middle" without taking notice. Criminal sites may imitate a trusted service (such as an online bank, a company website or a mail provider) in a way that is almost impossible to detect. Hence, we need electronic trusted ways to identify a site or provider on the Internet.

This is currently ensured by a system of electronic certification based on a chain of trust and clear rules on which organizations are allowed to issue certificates. In the chain of trust, valid certificates can also be traced back to a trusted Root Certificate Authority like e.g. Verisign, DigiCert or Entrust.

In the European Union, certification providers are subject to strict quality criteria and regulations as described in the EU Directive 1999/93/EC on "a Community framework for electronic signatures". However, recent cases have demonstrated that digital certificates are not free from being attackable. e.g. the hack of the Dutch certificate authority DigiNotar[12] had resulted in issuing of more than 500 fraudulent certificates.

Another hack affected the U.S. based certificate provider Comodo[13] that was later traced back to an attack from Iran. Fraudulent certificates were used e.g. to re-route traffic from services such as Google, Yahoo and Skype to malicious sites in order to steal log-in credentials.

While browser firms and others have quickly adopted screening for dubious certificates – such as Diginotar, Comodo or Türktrust – and banning of certificates from such providers, these examples show that the trust chain of digital certificates is far from being unbreakable. New technological as well as organizational and regulatory actions are needed to re-install trust into digital identification and lift it on a higher level of security.

3.3. Quantum and post-quantum cryptography

One important research and development strand of the past decade has therefore been to develop new cryptographic primitives that are not breakable in reasonable timeframes by quantum computers. Also known as post-quantum. While further ground work on such primitives – e.g. Lattice-based cryptography – is needed, particular problems lie in the performance and adaptation to practical use contexts.

Already, there is a significant Gap between security relevant methods and protocols at research and development – which are very advanced – and those implemented into actual products and services. With the exception of a narrow range of products in high security areas. The same applies for the often poor quality of implementing security relevant protocols in widely used open programming libraries.

This will be further discussed in the Gap on "security by design" and the necessary education of software engineers on cyber security matters. However, combined with this is also significant investment in improving critical Internet standards.

At the same time, are quantum computing and cryptographic methods based on quantum computing such as quantum key distribution significantly increasing the protection in high-security domains such as for military or specific government applications. The technology is based on fibre optic networks and uses a stream of randomly polarized photons to transmit data. One of the vendors in this growing market is IDQ[14] from Geneva. IDQ has simplified this technology by combining a photons-based quantum key generation with more traditional crypto based on the Advanced Encryption Standards (AES).

IDQ has already reported commercial applications of networks based on quantum encryption for several Swiss Banks and the U.S. based commercial research organization Battelle[15]. This underlines that quantum based technologies are gaining commercial relevance for securing the communication and public key management in high security networks.

Figure 5:
IDQ quantum key generator and network encryptor[16]

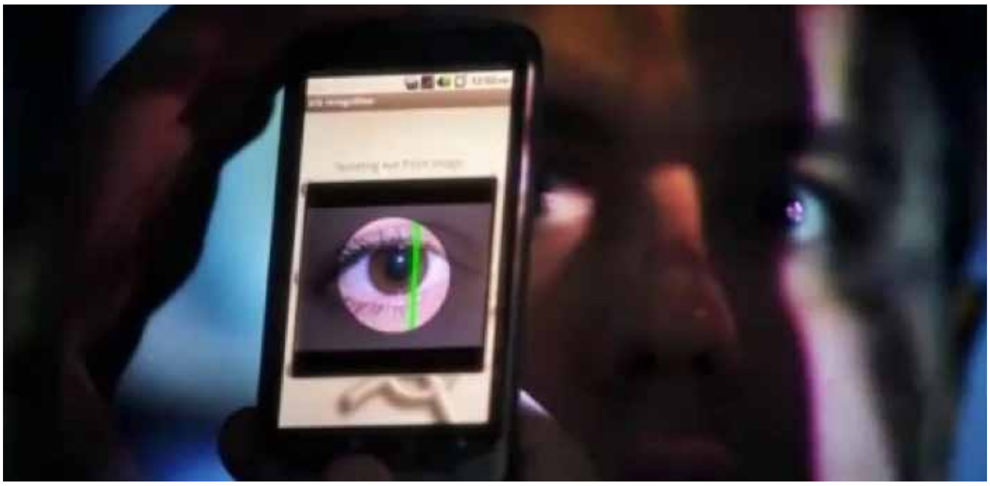
3.4. Next generation multi-factor authentication

A commercially relevant trend on a wider scale is to combine multiple factors into the authentication of communication and transaction partners in the Internet. The idea behind multifactor authentication is that taking multiple authentication factors at the same time into account increases the security of the authentication and makes it more difficult for hackers to break all factors at once (as an analogy: several locks on the same door with different keys).

Well known examples of this are e.g. smartcards or other tokens that many firms use to further authenticate the access e.g. to a firms virtual private network. This is then combined with digital certification on both sides and finally a password authentication.

A common element is here to use as many factors as possible that are specific to the user. While certainly this raises the security level, attacks – e.g. via spyware – may get access to further authentication credentials like locally stored certificates or passwords. In the same way, are tokens or smartcards often left in the machine including times when the user is away. Also, once connected they can be used by any unauthorized hacker that has electronic access to the machine.

Figure 6:
Biometric mobile applications.
Example BioWallet by the
Spanish Start Up Mobbeel[17]



More advanced examples of additional factors therefore include e.g. biometrics where fingerprints or iris scans are used. An other development direction is the use of NFC combined into mobile devices (see Gap VI) to authenticate in a touch-less way but demanding a close proximity. As the NFC device is kept close to the user and is always carried by the user (e.g. as a phone, a smart wrist band or smart ring) it can also be used to automatically log-in and out e.g. from a laptop or PC when the user leaves the machine unattended for a time.

A further promising direction is provided by combining data analytics with authentication – e.g. to determine unusual patterns of activities such as changes on the site of access devices, geographies or service use patterns (e.g. detecting use by machines).

An even stronger security is provided by using integrity verification of the devices – e.g. by trusted computing as this prevents from undetected installation of malware.

In general, multi-factor authentication is an important direction to further improve the security and trustworthiness of online communication and transactions. We can assume that in the future almost all Internet based services will take a complex combination of factors into account when authenticating a user. In the same way, also the user can monitor multiple factors when connecting to a service or communication partner.

It is thereby important, that while these techniques will allow more secure authentication and management of trusted digital identities in the future, it can preserve seamless usability, ease-of-use, and mobility. In other words: to shield away the underlying cyber security complexity from the user. A pre-requisite will be continued efforts on industry standardization and improving the stack of IP protocols.

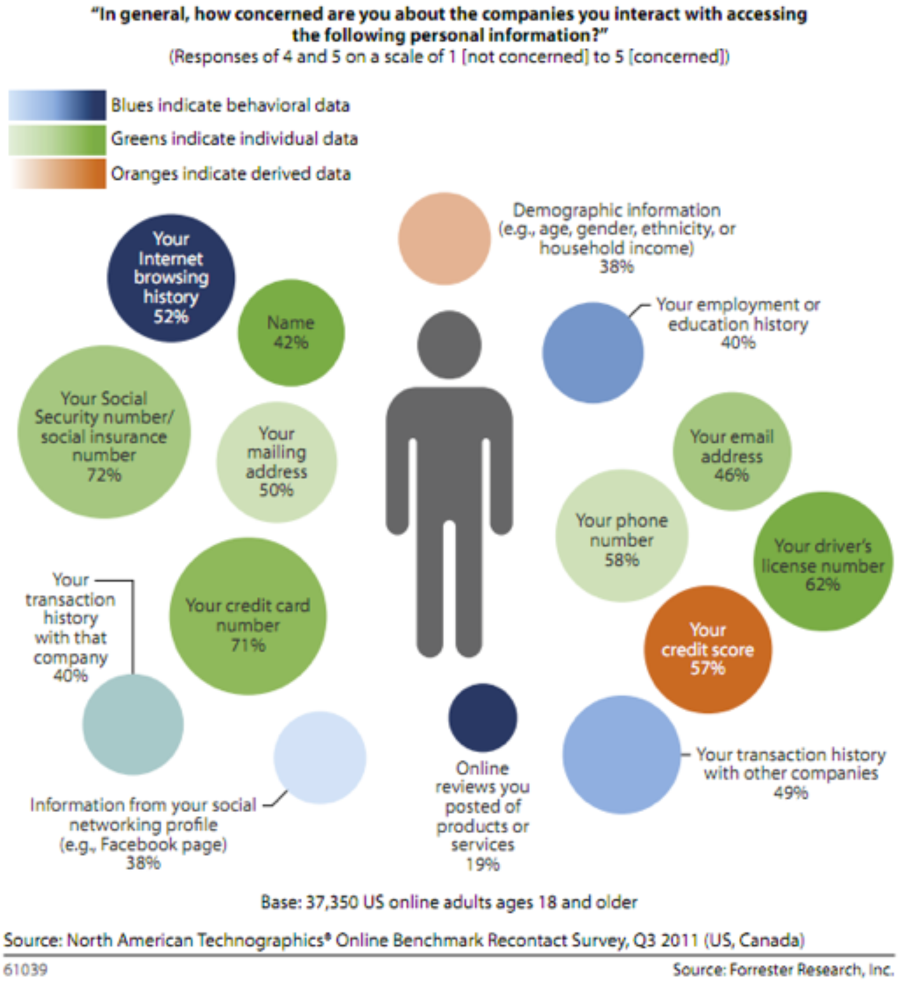
4. Gap III: Enhancing privacy

Enhancing privacy has become a central concern for users of Internet-based services. This has several dimensions. Not only users are seeing risks of losing private data or leakage as consequence of cyber criminal activity, but they are also increasingly suspicious to behavioural tracking and collection of data by commercial providers themselves.

In 2012, Forrester Research[18] has conducted an analysis of a large dataset of nearly 40.000 adults in the U.S. on their preferences as digital consumers. The study provides a differentiated picture by age groups and different types of personal data. The study also demonstrated that while consumers are concerned about exposing private data, they are well able to distinguish between different uses of such data – some of them regarded as legitimate and other regarded as non-legitimate.

From the viewpoint of cyber security, the user's need for differentiated privacy leads to several requirements. An example is that applications accessing data on a device (like a mobile phone) need to be strictly controlled in a way that only allows them to access those data, information or services that it is entitled to.

Figure 7:
Digital consumer concerns about exposing private data.
Source: Forrester Research, 2012



"In general, how concerned are you about the companies you interact with accessing the following personal information?"
(Responses of 4 and 5 on a scale of 1 [not concerned] to 5 [concerned])

Base: 37,350 US online adults ages 18 and older

Source: North American Technographics® Online Benchmark Recontact Survey, Q3 2011 (US, Canada)

61039 Source: Forrester Research, Inc.

4.1. Fine-grained access to personal devices and services

A pre-requisite for secured privacy is to enforce fine-grained access to personal devices and services. This means that access rights – e.g. to sensitive information such as the device location – have not simply to be managed. They also have to be protected against possible attacks e.g. through malware that is aiming to escalate its privileges in order to gain access to further data on the device.

The principle of fine-grained access can be applied to cyber ecosystems on any level of complexity. As already discussed in the CYSPA report on “Understanding and Managing Cyber Risks”, we have to distinguish in this context three different trust models in cyber ecosystems: (1) the origin-based trust model of the Web, (2) the role-based trust model of enterprise IT, (3) the permission based trust model – increasingly used in modern operating systems – e.g. in mobile device OS.

In the previously mentioned report, we have discussed vulnerabilities of each of these. A typical example for attacks to the role-based model are root compromise attacks, where hackers progress from limited access rights on a server (e.g. ftp access) to root-level access (admin role). Security expert Daniel Cid demonstrates in his blog[19] multiple popular hacking techniques for gaining root level access – mostly as a consequence of overly simplistic server configurations with regard to role-based access rights.

For web applications, access permissions is granted based on the origin of the request following the principle that requests from the same origin (as identified by URI) have equal access rights. This allows e.g. dynamic web applications to access a session cookie that it has placed on a user machine, while other web applications may not access it. However, multiple attacks have demonstrated that breaking the origin-based access protection is possible e.g. using cross-site scripting techniques. Again, these vulnerabilities are often the consequence of too little attention by web application developers to cyber risks. Cross-site scripting e.g. is based on injecting malicious scripts into input fields of web applications. If the application is not actively scanning input for executable code and detecting this, it might send the script right back to an unsuspicious user and the code is executed within the web browser of that user. He has little chance to detect this as now the code originates from a trusted origin. This may e.g. be used to steal a valid session cookie and re-open the session on behalf of the hacker from another machine.

Even the largest commercial services are not immune to these types of attacks. This has recently been demonstrated at the example[20] of ebay Germany by experts from the security firm Greenbone. This is only one vulnerability in a series of cross-site-scripting vulnerabilities that have been detected for ebay.

Also the permission and sandbox based access model of mobile OS like Android has been under attack. Researchers from Microsoft and India University have e.g. demonstrated[21] a new kind of Android malware that was able to gain increasing privileges – by exploiting a weakness in the regular Android update process.

The secure management of fine-grained access to devices and services is a cross-cutting concern for developers of device OS, browser firms, security tool providers, web services, IT administrators, and alike. There is certainly not a simple solution, rather the secure management of fine grained access – with its sub principles like isolation, narrow privileges etc. – needs to become a serious consideration at design time. This can be further promoted with specific skill building and educational initiatives.

Also further development effort needs to be put into security-hardening of device OS as well as into emerging software platforms – with securing fine-grained access being one of the key concerns.

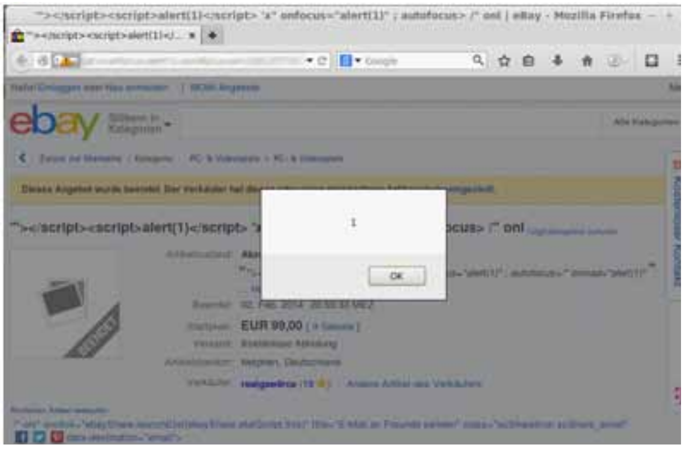

"></script><script>alert(1)</script> "a" onfocus="alert(1)" ; autofocus> /" onl | eBay - Mozilla Firefox
ebay
1
OK
EUR 99,00

Figure 8:
Demonstration of cross-site-scripting vulnerability of ebay Germany.
Source: ZDNet, 2014

4.2. Protecting data

In a similar way as protecting access to devices and services and ensuring that such access is only granted within clearly defined privileges and limits – further attention needs to be put on the secure handling and access of data.

However, current ways of storing data rarely contain enough meta data to assess how sensitive the stored data is from a security and privacy perspective.

In general, the access control and handling of data takes place via applications. And access control (e.g. to a specific personal data record) is granted based on the role-based access scheme in the application. However, hackers will mostly gain access to sensitive data directly via the lower level – e.g. via direct access to database tables, to files etc.. The same applies to legitimate admin level users who also have far reaching rights in accessing the data on that level – which implies risks for insider attacks.

To avoid these risks, sensitive data needs to be protected when stored. It should only be made transparent when actually needed in a transaction. This is e.g. ensured by encrypting sensitive data in storage.

More intelligent, secure and privacy aware data storage techniques will be needed.

4.3. Protecting identities and anonymization

A related concern is to protect personal identity elements of sensitive data sets – like name, birthday or addresses in medical records – while still allowing that the data can be used in relevant contexts.
This is known as data anonymization and de-anonymization. Different ways are possible to achieve this e.g. via encryption of sensitive parts.

In the sense of the fine-grained access to data and services – anonymization can be linked to access rights of a particular application or service. This can be combined with techniques that prove the validity of the data while not revealing the private elements.

But not only data can be anonymized. Another aspect is to anonymize the identity of a digital transaction partner while still allowing a valid transaction to take place. This may effectively reduce the amount of privacy relevant information that has to be transferred and put the user further into control about what he is willing to transfer. IBM has developed this as a new field – under the name of Identity Governance[22] with further European partners in two EU projects: Prime and Primelife.

4.4. Privacy and the Internet of Things

The Internet of Things with its billion of devices and data sources is a particular challenge to privacy and security. More important are the principles and Gaps as stated above: to develop possibilities of user privacy control combined with techniques to ensure that access to personal devices, to data, services, and to personal information is only granted within the limits set by the user and the clear privileges that were originally intended and accepted for a particular application or service.

With regard to cyber security risk, the challenge is further to secure the access to a wide emerging range of new devices, to protect the data on these devices and the communication between them.

A particular problem springs also from the fact that smart things expose a number of data services but the purpose of using the data will in many cases arise dynamically and can not be fully defined upfront. This is not necessarily a contraction to the fine grained access principle but it means that access needs to be granted on a different set of criteria. These criteria would allow a matching to a range of purposes while strictly excluding other ones. The EU research project RERUM[23] is e.g. addressing this challenge.

As also expressed in the CYSPA report on "Understanding and Managing Cyber Risks" a large degree of "smart things" – e.g. consumer devices like smart TVs, fridges etc. – is using relatively low levels of security and hence protection from cyber threats. At the same time is the connectivity of the Internet of Things opening remote and potentially criminal access to these devices on a much larger scale than ever before.

These devices are often based on embedded systems – using operating systems like e.g. embedded Linux – and those suffer from a number of deficits with regard to security. One example of such weaknesses is a much less developed security patching and updating process. At the same time have many of these devices already sufficient compute and memory capacity – e.g. to make them attractive enough as hosts for botnets and other malware. While being useful for general criminal activity like sending spam, this can further allow criminals to actively broadcast sensitive data from the device as well as spy-out and record details about use profiles.

A further aspect of the Internet of Things is that many devices can not only be used to retrieve sensitive data but also contain actuators to control sensitive parameters such as the heating at home up to controlling remotely machines in an industry 4.0 scenario.

Hence, it is important to develop secure mechanism to authenticate in a trustworthy way with the device, ensure its integrity, securely control the access to its data, actuators and other services as well as secure the communication with the device.

5. Gap IV: Improving security by design in today's software systems

As cyber security and privacy protection are becoming increasingly important, they need more rigorous consideration at design time in today's software based systems. In the traditional thinking of enterprise security, trusted zones (e.g. an Intranet) were distinguished from un-trusted zones. Security measures concentrated on protecting the perimeter of trusted zones similar to the walls around a castle. This is still reflected in concepts like firewalls or secure gateways.

As stated before, with emerging trends like the Internet of Things and an increasingly growing number of devices and flexible connections, the concept of protectable perimeters is seriously challenged. Even simple hacking methods – like spreading malware into enterprise IT from infected memory sticks – have shown how easy it may be in fact to circumvent traditional methods of perimeter security. Further to this there are growing concerns about insider attacks or attacks that use intermediate trusted sources, employees devices or are injected into popular trusted websites.

Cyber security risks are the downside of the openness, integration and flexibility of today's cyber ecosystems. A first important element is raising awareness and educating developers (see Gap IX) on cyber risks, different hacking techniques and cyber attack approaches. It is important to start seeing cyber ecosystems, devices or apps with "the eyes of the hacker" – that means from the viewpoint of potential security weaknesses, entry- or break-points that allow to misuse or exploit the system and move beyond the originally intended purpose and functioning.

5.1. Testing and scanning

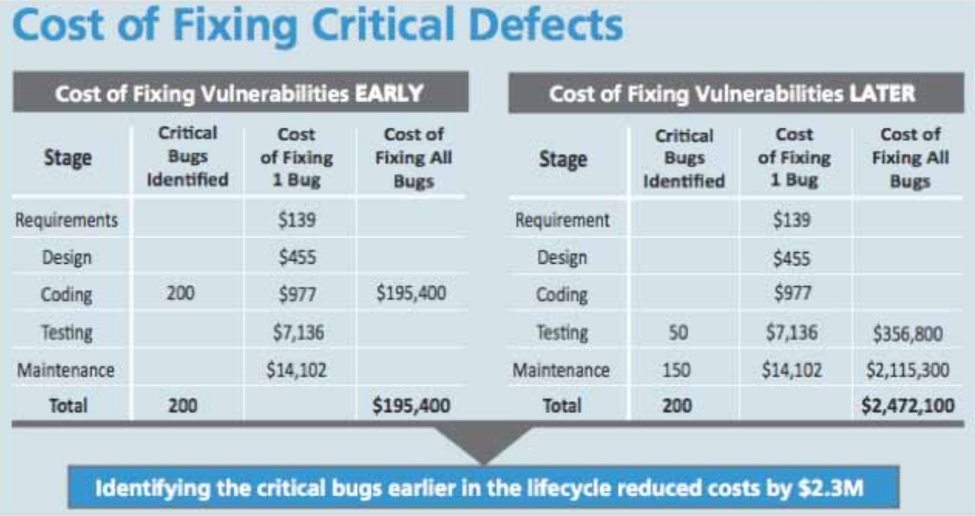
Security-by-design has different methods. On the one hand it means the consequent analysis of new software – such as apps – for vulnerabilities using tests against known hacking techniques such as XSS. Several vendors already offer advanced scanning tools for apps and Web applications – like e.g. the IBM Security AppScan[24] tool family. Extensive tool references are provided in the CYSPA overview on technologies and solutions.

Scans can be conducted by simulating test users to the web application that conduct different known attacks. But there are further possibilities to scan for known security vulnerabilities already at the level of the source code. The security scanning supports here different phases of the software lifecycle and needs to become an integral part of the development process similar to other forms of testing such as usability testing or performance testing.

Similar vulnerability scanning methods also exist – not only for software – but also for other elements of the ecosystem e.g. for networks configurations. Also, third party components, code libraries etc. have to undergo systematic security scanning.

Also, an important business consideration supports security by design. Not only does the proactive search for security vulnerabilities lower risks of later damage caused by attacks, it is also much cheaper in earlier phases of the software development cycle to fix vulnerabilities than in later ones.

Figure 9: Costs of fixing security vulnerabilities in different stages of the software development cycle. Source: cigital[25]



Cost of Fixing Critical Defects

Cost of Fixing Vulnerabilities EARLY

Stage	Critical Bugs Identified	Cost of Fixing 1 Bug	Cost of Fixing All Bugs
Requirements		$139	
Design		$455	
Coding	200	$977	$195,400
Testing		$7,136	
Maintenance		$14,102	
Total	**200**		**$195,400**

Cost of Fixing Vulnerabilities LATER

Stage	Critical Bugs Identified	Cost of Fixing 1 Bug	Cost of Fixing All Bugs
Requirement		$139	
Design		$455	
Coding		$977	
Testing	50	$7,136	$356,800
Maintenance	150	$14,102	$2,115,300
Total	**200**		**$2,472,100**

Identifying the critical bugs earlier in the lifecycle reduced costs by $2.3M

5.2. Security oriented governance of the development process

An even more systematic way is to install a dedicated governance including processes and quality gates to ensure that the required levels of vulnerability scanning and security testing at each step of the development process are observed.

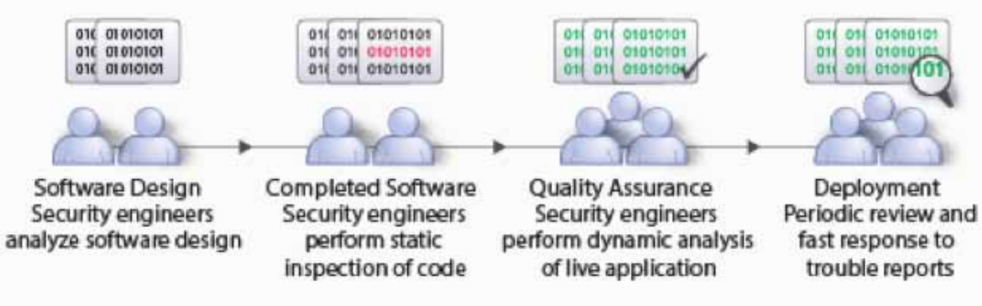
Governance is significantly more complex when the development – as it is often the case in larger development projects – is distributed globally and includes many external contributors and suppliers. A way to address this is via standardization and community sharing of practices as well as agreeing on commonly accepted rules for compliance to different levels of security.

In particular large software vendors or web firms with a significant developer capacity have engaged in designing own governance models for security by design. They have further spread these into their external developers and solution partner communities.

Microsoft started e.g. in 2004 with the Security Development Lifecycle Initiative[26] that was first applied in the Windows Vista Development. IBM launched the Secure Engineering Framework[27]. These frameworks are useful, however they also demand to be embedded in a common and overall systematic way to manage the software development.

Google is an example for an alternative approach[28]. Google generally offers their developers wide choices in development methods according to what fits to a specific project. Correspondingly, Google has organized the security screening independently from a specific software development method. Google builds on a combination of developer education and spreading of a quality-driven-engineering culture that sets itself clear principles for software quality (including aspects such as robustness, maintainability and security). This is verified on the one hand via peer code reviewing and on the other via dedicated teams of Software Design Security Engineers working together with other developers to inspect and improve code from a security perspective. They also conduct multi-layered security testing.

Figure 10: Teams of Software Design Security Engineers interacting with software development teams at different stages. Source: Google.


Software Design
Security engineers analyze software design
Completed Software
Security engineers perform static inspection of code
Quality Assurance
Security engineers perform dynamic analysis of live application
Deployment
Periodic review and fast response to trouble reports

In smaller, dynamic environments like small to mid-sized software firms (SMEs), web start-ups etc. it is difficult to instantiate such governance models. Also it will be difficult for such firms to recruit specific software design security experts in the same way as the big industry players. Even more, this applies to organizations that are merely IT users and that only have a limited amount of development capacity or those that in-source software development via freelancers or small agencies.

It is an open challenge to transfer the same capacities for security-by-design into the hands of such smaller organizations or individual developers. The Open Web Application Security Project[29] is an example for an open-source-style community initiative to support the spreading of security-by-design competences. Another approach has been piloted by the Open Source Hardening Project[30] funded by the U.S. department of homeland security. In this approach, a team of security experts from industry (Symantec and Coverity) and research (Stanford) interacted with over 260 open source projects and helped to fix over 7.800 security vulnerabilities in the code base of these projects.

5.3. Security hardening of platforms and legacy systems

A complementary topic of security-by-design is to security harden legacy software as well as widely used operating systems and software platforms. While security hardening demands of course a lot of individual analysis, several characteristics of security hardened platforms can already be derived. Gaining a better understanding of such principles and agreeing on common characteristics will further ease the process of security hardening platforms.

In the following, some examples are given for typical objectives in security hardening platforms:

5.3.1. Device OS level

Techniques like application sandboxing and integrity control of data flow between applications support the security principles of isolation and fine-grained access control at the level of single devices. In return this serves to ensure that applications may only execute actions on a device or access data within the limits of explicit permissions.

5.3.2. Cloud platform level

Future cloud services will interact with vast amounts of diverse devices. Trusted authentication and secured matching to the security and privacy policy requirements for specific users and devices will be one essential element.

Typically, clouds serve a multitude of tenants and devices in parallel. For this purpose, they allocate physical resources (such as storage or compute capacity) in a dynamic way using virtualization.

This again demands specific care for verifying isolation among the different tenants in a platform – e.g. to prevent from leaking sensitive data or allowing intrusion across tenants. Complementary elements are verification of integrity of nodes in the cloud infrastructure and secured monitoring and logging mechanisms – e.g. to be able to retrace insider activities without potential for manipulation.

6. Gap V: Integrating software and hardware security

6.1. A trusted computing base

A trusted computing base is a pre-requisite for security. However, the integrity of lower layers e.g. of critical operating system elements, security patches or configuration files – is often just assumed. Malware that attacks the system layer below the operating system, such as stealth rootkits, makes use of this integrity assumption and may silently compromise the operating system configuration as well as prevent security mechanisms on the application layer such as anti-virus software or firewalls from functioning. The potential to infuse security risks on the entire software stack of a computer, makes the integrity verification of the computing base a critically important concern.

The same applies for the integrity of the hardware itself. Cambridge University security researcher Sergei Skorobogatov[31] proofed in a 2012 study the existence of malware in military-grade FPGA chips of the Chinese manufacturer Actel/Microsemi. These were sold to U.S. military and used in other critical applications.

While often, the intention is simply to use infected computers for botnets and as compute resources for criminal activities, rootkits or chip-level malware can also of course open backdoors for specific spying or other targeted attacks to the individual machine. Also, a compromise of the compute base provides hackers or state-sponsored-teams with a perfect basis for advanced persistent attacks as the traces of attacks can effectively be hidden.

Several approaches have been developed to address the critical problem of a trusted computing base. Within the hardware purchasing and assembly process, chip-level security scanning ("silicon scanning") can reveal security vulnerabilities and hidden malware such as backdoors in computer chips. Silicon Scanning is also the technique[32] that Skorobogatov used in the example provided above.

Intel and McAffee have presented with its DeepSafe Technology[33] in 2012 an approach specific to Intel Core-i processor based systems that is able to detect rootkits and other compromises below the operating system level. DeepSafe builds here on the hardware support for virtualization as implemented in the latest Intel chips (Virtual Machine Extensions – VMX) and exploits the fact that the VMX technology allows microprocessor level virtualization on 2 levels of hierarchy – a root and a non-root VMX level. This effectively is used to run root level security protection on a root VMX level, whereas the stealth rootkit can only access the processor on a non-root VMX level.

The Intel/McAffee approach provides an interesting direction and shows that closer collaboration between hardware manufacturers and security firms is needed. Also complementary approaches are needed for different device and microprocessor categories.

6.2. Software integrity attestation

A complementary approach developed since already a decade by the Trusted Computing Group and now standardized by ISO/IEC uses an external module – a Trusted Platform Module (TPM) to perform measurements of software and platform metrics to ensure the integrity of the computing base including its software integrity (e.g. against unauthorized manipulation or unauthorized software installations). It can also be used to detect unauthorized hardware.

The TPM includes the possibility to establish a trusted channel to an external management unit using hardware-based cryptography of its communication and may verify the system from remote. This technique known as "remote attestation" may e.g. be used in data centres where a large number of servers is controlled, by cloud services or by other trusted third parties. Other applications include sensitive networks that may want to verify that only known devices with a trusted software configuration can connect. Also, the inbuilt cryptographic capabilities may be used to safely store certificates by other applications e.g. in support of hard disk encryption or software licence management. TPMs can further be integrated in the authentication process and hence provide a continued security support starting from safely booting to network connection and authentication.

TPM modules are widely implemented in most Windows laptops and PCs (including those from Acer, Dell, Lenovo, HP, Samsung, Fujitsu, Sony and Toshiba). Also Google has adopted the TPM technology in their Chromebooks. Further adopters include popular game consoles like the XBOX360, Nintento Wii and Sony's Playstation. According to the Trusted Computing Group[34], as of mid 2014 already over 2 billion endpoint devices are equipped with TPMs which makes them one of the most widely deployed hardware security token technologies in addition to mobile phone SIM cards.

Figure 11:
Infineon Trusted Platform Module.
Source: Infineon

However, trusted computing has also received criticism and is facing privacy concerns for the possibility to remotely verify system state and software configuration e.g. by hard- and software vendors. Also the openness of the system itself has been criticized. Users of Linux e.g. found that PCs designed for the Windows 8 secure boot process (enabled by TPM) did no longer allow the installation of the Linux kernel.

Also, the TPM approach is not free from vulnerabilities. In 2010, former U.S. army security expert Christopher Tarnovsky demonstrated a hack[35] to the Infineon SLE 66PE TPM, one of the most widely used TPMs at that time. The Microsoft BitLocker disk encryption that also uses the TPM has been hacked in multiple ways e.g. boot passwords have been retrieved directly from BIOS buffer memory[36]. Many TPMs in enterprise environments - e.g. data centre servers - are also intentionally de-activated by administrators in order to avoid specific configuration efforts and potential problems.

6.3. Securing embedded devices

Not all compromised devices on system- or even hardware-level are PCs, servers or at least smartphones. Proofpoint, a silicon valley based security firm demonstrated[37] in 2014 the potential of system level attacks in the Internet of Things - including detected malware examples from all kind of consumer appliances such as television sets, home routers, multi-media centres and even a smart refrigerator.

It seems likely that in the future most smart devices and things will include a hardware security token of some sort that supports hard- and software integrity verification as well as trustworthy authentication.

In particular with the development of the Internet of Things and scenarios like Bring your own Device, the necessity to manage an ever growing and massive number of devices is arising fast. It is important to closely align and integrate in this context the further development of security hardware with the software-based security protection on higher levels. At the same time, there is a need to take into account concerns about privacy and openness of such systems and reduce dependency from single large vendors.

7. Gap VI: Securing our future networks

7.1. IPv6 and securing the Internet Domain Name System (DNS)

The current Internet is since several years in a transition phase to the IPv6 protocol and its extended 128-bit IP address space. While the protocol suite has already been standardized a decade ago, it has taken time to implement IPv6 support. As of now, most actual endpoint devices and operating systems already include support for IPv6, but the IPv6 support and readiness by websites and web-based services around the globe is only emerging. According to Google Statistics[38], the real-world deployment of IPv6 in the U.S. was in mid 2014 at 9,56% and in Germany at 11,13%.

This process is however accelerating as the number of Internet connected devices is massively growing and the registration of new 32-bit IP addresses based on IPv4 reaches its limit in many geographies including Europe. Google – as one of the most widely used services in the Internet – shows e.g. an exponential growth of user requests over IPv6 in the past 3 years (see figure), while still the absolute percentage is below 5%.

Figure 12:
Spreading of IPv6 adoption per world region. Scale from 0% to minimum 10%.
Source: UN and Asisa Pacific Network Information Center (APNIC)[39]

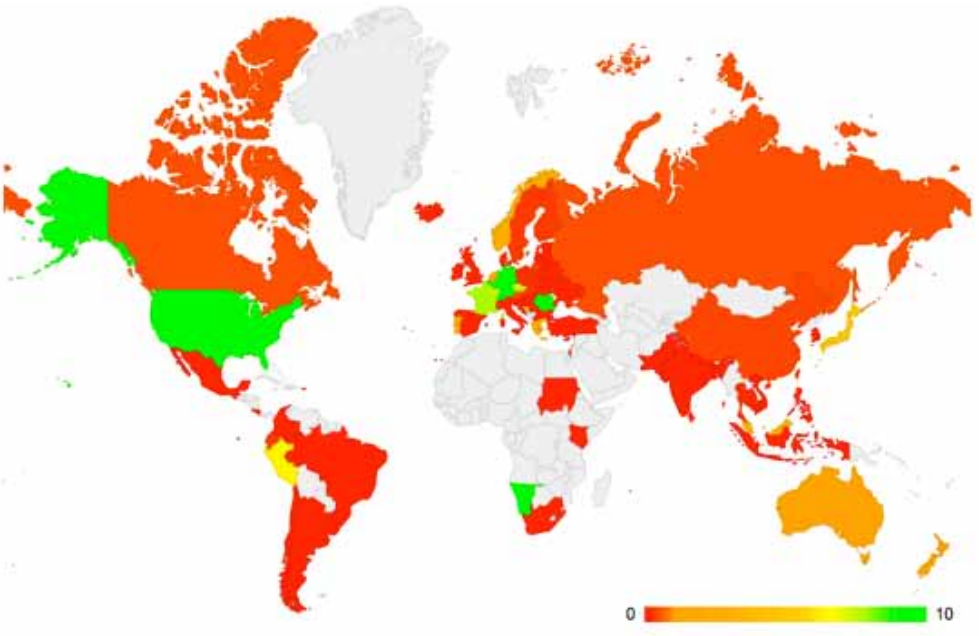
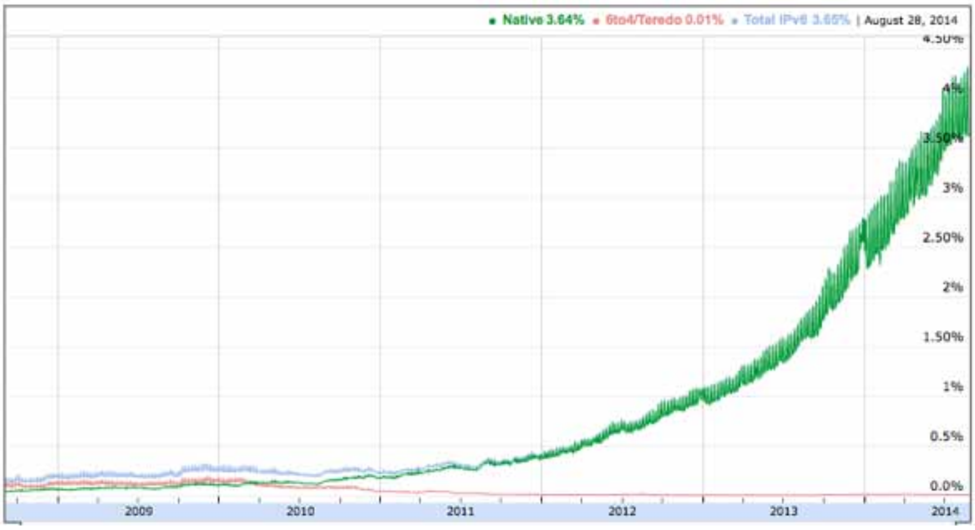


Figure 13:
Percentage of users accessing Google over IPv6.
Source: Google Statistics[40]



As discussed in more detail in the CYSPA guide on “Understanding and Managing Cyber Risks”[41], IPv6 has many advantages from a cyber security perspective – with protocol innovations like e.g. the IPsec security protocol as well as network technologies such as multicast or quality of services.

Another important aspect is the securing of the Domain Name Service (DNS) of the Internet. DNS attacks have become popular and exploit the distributed and open nature of the Internet’s DNS system. The DNS is an essential Internet/web building block as it resolve domain names into IP addresses and hence points users from a website’s name to the IP address of the server that will actually fulfil the request to the website (such as sending content or performing a service). The current DNS is generally considered to be severely insecure. Cache poisoning[42] is an example for a DNS attack that aims to redirect users from legitimate sites to malicious websites. Also DNS servers have been hijacked and misused in the context of distributed denial of service (DDoS) attacks.

The IPv6 Domain Name Security Extension Security (DNSSEC) is an improved standard to verify the authenticity, integrity and origin of domains. While DNSSEC is still under discussion with regard to its compliance to all national data privacy regulations (e.g. the German one) it provides an important contribution to the future securing and trustworthiness of the DNS.

However, IPv6 also poses many challenges to cyber security – such as the availability of very large spaces of IP addresses that allow fast fluxing e.g. for spammers which make tracing based on IP addresses or blocking of senders more difficult. Many attacks also exploit the fact that in the Internet currently IPv4 and IPv6 parts co-exist and security vulnerabilities are directly emerging from the necessary tunnelling between these parts.

It is important to create awareness on the security aspects of the IPv6 transition that organizations will have to undergo in the upcoming years. As well as the need to guide organizations through this process. Many insecurities around IPv6, the parallel use with IPv4 and the different elements like IPv6 DNS, IPv6 mail, DNSSEC etc. still exist on the side of adopters.

7.2. 4G and 5G Mobile Networks

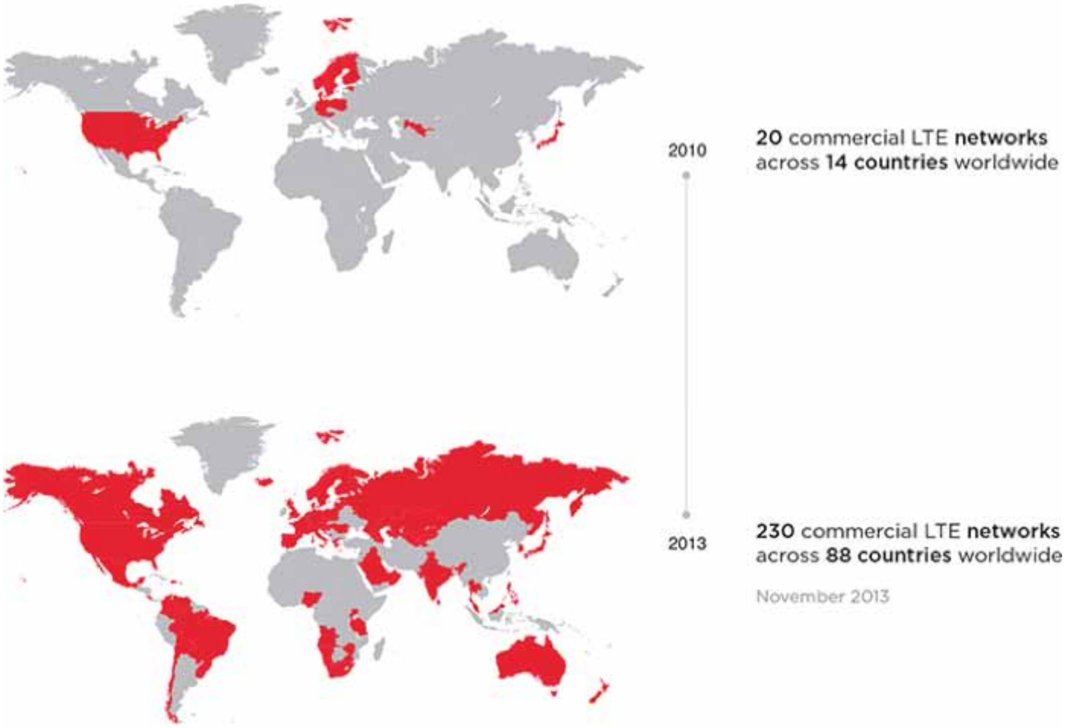
One of the most important trends of the past years has been the rise of the mobile Internet and the success of connected smartphones, tablets and other mobile devices. With the rise of the Internet of Things, the range of connected devices is further growing.

The success of the mobile Internet is closely linked to the availability of fast, ubiquitous mobile networks. The current real-world distribution of mobile Internet access is based on technologies and networks using 3 generations of digital networking standards from the early 2G/GPRS with a downlink rate of approx. 40 kbps to the latest 4G/LTE[43] networks with peak rates of 300 Mbit/s. The next generation mobile network (5G) that is currently under development will again provide a speed increase in the range of a factor 100. Once technical equipment to install a new generation of mobile networks is available, the commercial spreading is fast. We can expect the next network generation to start spreading commercially by the end of the decade (2020).

From an end-user perspective, the available mobile network bandwidth and minimal latencies will soon be sufficient for even the most demanding applications. Already in 2014, the absolute number of Internet users from mobile devices is surpassing those accessing the Internet from the desktop[44]. Mobile Internet use had a continuous annual growth (CAGR) of 146% between 2006-2012 outperforming even the CAGR of fixed IP-traffic in the years 1997-2003 (127% CAGR) – the first peak time of global World Wide Web and Internet adoption[45].

The evolution of the mobile Internet and each generation of new network standards has gone along with a growing convergence of fixed-line and mobile Internet. At the same time, 4G is the

Figure 14:
Growth of commercial adoption of 4G/LTE between 2010 and 2013.
Source: GSMA Intelligence


2010
20 commercial LTE networks across 14 countries worldwide
2013
230 commercial LTE networks across 88 countries worldwide
November 2013

first generation of mobile networks that is all-IP based. The first collaboration agreement[46] between the Internet Engineering Task Force (IETF) and the 3d-Generation Partnership Project (3GPP) – the core organizations in charge of the Internet protocol development respectively the mobile network standards – was already done in 2001. This agreement implied that the Internet protocol would be adopted as far as possible without specific changes or additions for mobile networks. Compared to the past generation, this applies in 4G now not only to data transfer but also to voice communication and any other service over the mobile network. 4G also implements IPv6 protocols as described before and uses the IPv6 128 bit address format.

The use of all-IP however also implies, that attack types known from the Internet – in particular those that exploit protocol weaknesses – will further pervade into mobile networks. Also, previous mobile networks have used confidential specifications whereas the IP protocols are fully open which make it easier for potential attackers to find and test protocol weaknesses. Included in the 4G specification is also the use of the IPSec protocol. However, it is not fully implemented by many LTE providers[47] – for reasons of cost and performance concerns.

In return, 4G is introducing a range of security improvements[48] such as mutual authentication between base station and the mobile device (to prevent from attacks using rouge stations), integrity protection of the signal as well as secure storage of user credential on the SIM card. In contrast to fixed Internet equipment, are the network appliances, antennas and other equipment also under embargo and it demands specific efforts by attackers to get access to these.

For the development of the 5G networks several innovations are suggested including a more network centric approach with technologies such as multicasting or support for mesh networks. This will allow to reflect usage models better in the network and allocate resources more flexible (e.g. a large number of devices accessing the same content from a provider or multiple devices communicating in geographic proximity). In return, this might also allow a new category of advanced-persistent attacks that exploit such mechanisms.

Securing the new generation of all-IP mobile networks and general cyber security – these are increasingly overlapping objectives and will share many technological and solution elements. This also makes mobile network operators important stakeholders in the overall cyber security debate.

7.3. Local and ad-hoc networks

As a third network technology category that increasingly needs consideration – apart from the converging fixed IP and mobile all-IP networks – are technologies specific to the near-field and for establishing local networks between devices.

In the CYSPA report on "Understanding and Managing Cyber Risks"[49], several risks related to using local and ad-hoc network – based e.g. on WLAN and the IEEE 802.11 standard or on Bluetooth – are discussed. Those networks serve many purposes. They can ensure fast local connectivity to an Internet gateway point or locally connect a number of devices – like sensors or other smart items.

At the same time, they allow multiple possibilities for attacks such as eavesdropping into non encrypted communication, session high-jacking or re-routing communication to rouge network nodes. While there are many solutions to further secure local networks, a particular problems arises from the fact that mostly the network may include uncontrolled nodes (as in the case of ad-hoc networks) or is itself out of control of those who use it (as in the case of public WLAN).

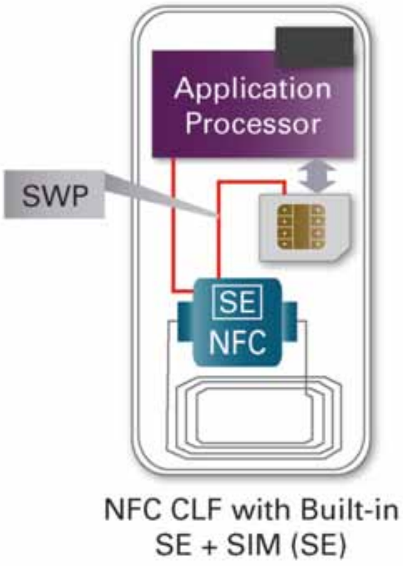
End-to-end security solutions are needed to cope with the inherent security challenges of uncontrolled local or ad-hoc networks – in particular when they shall be used to access critical services. While Virtual Private Networks (VPN) provide an element in creating such solutions they are in general not sufficient to protect the entire interaction within the network.

7.4. NFC

An interesting development has more recently emerged around the use of Near Field Communication (NFC) chips which increasingly become deployed in mobile phones (e.g. by Samsung). One aspect that contributes to the security of NFC is that it requires a very short range (a few centimetres).

This makes it almost impossible for hackers to intervene or eavesdrop into the NFC connection and transfer of data in an NFC based transaction (like a mobile payment or an authentication). NFC implementation in mobile phones is combined into a security architecture. This includes a secure element to securely store data and serve as a secure executive environment for NFC applications. This is further connected using the secure Single Wire Protocol with the SIM card to retrieve information securely stored in the card as well as the main processor. This architecture allows to execute NFC applications, store and process the necessary data (e.g. credit card data for a payment transaction) in a secured environment.

Figure 15:
NFC Secure Architecture including NFC Chip, the Secure Element (SE), the SIM Card and the Single Wire Protocol connection.
Source: EETimes[50]



The NFC security architecture is an example for several of the principles that have been discussed in the previous Gaps. It is a further demonstration for the value of a close integration of hard- and software elements in cyber security. It further has a behavioural element due to the limitations of the short distance. It also provides an interesting authentication technology which could be combined with other authentication factors as discussed in Gap II.

7.5. Beacon Networks

A further emerging category of network connections is used e.g. for indoor navigation or location based services where the GPS resolution is not sufficiently fine grained or where a GPS signal can not be accessed.

Bluetooth Low Energy (BLE) has been introduced in 2006 by NOKIA as a technology to network devices in the range of 10 meters. It can therefore address distances below the GPS resolution. BLE has become widely supported within Android, iOS and more recently Windows Phone 8. Apple has introduced the term iBeacons in 2013 as a new standard for indoor navigation based on BLE in 2013. While the Apple iBeacon technology includes some propietary elements, its general principles are already realized with BLE devices in open approaches.
Beacons are sender modules based on BLE that produce a signal in regular intervals. Beacons identify themselves with the device via a universally unique identifier (UUID). Through the triangulation of several Beacons, locations can be determined very precisely. This implies the installation of a relevant array of Beacons in a particular location. Multiple beacon networks are already available in areas such as airports, hospitals or shopping streets. Other application domains are connected home or personal asset tracking. Analyst firm ABI Research estimates that by 2009 beacon shipment will already break 60 million units[51].

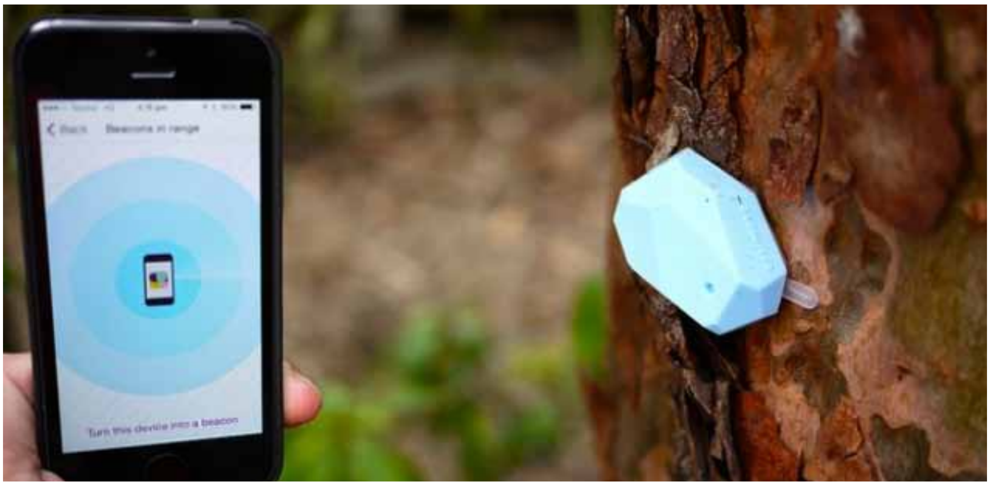


Figure 16:
Connection of a mobile phone to a beacon.
Source: Wired Magazine[52]

As the connection of the beacon to the mobile device is bluetooth based and implies pairing between the mobile device and the beacon over a longer distance, mutual attack possibilities – that are already known from bluetooth – are possible. Further to this, the UUID of the beacon – and hence the beacon location – needs to be passed through to an Internet based service in order to trigger location based services. This further raises issues of tracking- and privacy protection. The analyst firm Forrester[53] has already warned that security and privacy concerns will become major roadblocks in the adoption of this promising technology.

In return, beacons can also be used as a security enhancing technology e.g. to adapt the security policy of a mobile device according to different zones of an office building or campus area. Beacon networks can therefore contribute to the intuitive multi-factor authentication – as already discussed in Gap II.

8. Gap VII: Improving real-time cyber threat detection

The Cyber threat landscape is rapidly evolving, albeit at an accelerating pace. In the CYSPA report on "Understanding and Managing Cyber Risks" we have provided an overview on major areas and trends in this landscape as of 2014 – while still a threat analysis can never be complete or exhaustive. And continuous monitoring of the emerging threat landscape is necessary,

Nation-state threat actors, well-funded attack campaigns, professional and highly motivated adversaries, and advanced persistent threats (APT) have become regular headlines. The new generation of APT attackers are highly skilled and technically well equipped. Also, they are focused on acquiring something valuable and specific in a governmental organization or business, such as sensitive personal information, intellectual property, or insider information. These targeted attacks occur across all industries, and are stealthy and persistent enough to go undetected by traditional security technologies, such as next-generation firewalls, traditional IPS, anti-virus, and secure email or Web gateways. Hence, classical information security is not sufficient to protect an organization against such APT attacks.

In this context, we witness a shift towards commercialization of digital spying and a burgeoning third-party online-surveillance market. Historically, this kind of technology has been the reign of capable nation-states with the capacity to develop their own boutique capability. Targeted online real time surveillance typically involves a software "implant" surreptitiously installed on a user's machine allowing complete control of, for instance, a mobile device or laptop. The large governmental intelligence agencies in the U.S., U.K., Russia, Israel, China, etc. have developed own custom versions of these tools and had to invest a lot expertise and funding. But over the last years, Hacking Team and other players have begun selling this type of capability. Nations who lack the ability to create their own tools can now accelerate their online targeted surveillance programs relatively cheaply.

As for private sector companies and SMEs this means that unless they themselves augment their cyber security capabilities, they remain dependent of external patch solutions and tactical solutions. While at the same time they have little control about their individual protection. This demands public-private partnerships and collaboration models to jointly improve cyber resilience in an ecosystem.

The challenge lies in increasing and expanding real time detection capabilities, while at the same time decreasing or possibly avoiding false alarms altogether.

A striking example of the scale of the current real-time threats has been just recently exposed by Articles in The Intercept and The Washington Post[54]:

Commercial network injection appliances are actively targeting Google's YouTube and Microsoft's Live services in order to install surveillance implants on targets across the globe.

These attacks are large scale and highly sophisticated, so that resilience against such attacks demands comparable sophistication on the cyber ecosystem side.

8.1. Cyber security alliances

This also demands partnerships to share threat and incident information and pool analytics capabilities. We have seen the emergence of such partnerships on a small scale, as the recent example of a joint cyber protection alliance between Telefonica and Kaspersky has shown. In this case, Telefonica extended threat detection via pooling with the know-how of Kaspersky Labs.

Typical examples for sharing of data and information in an alliance are:

- **Botnet Threat Tracking** – provides real-time detection of botnet attacks targeting users of banking or online payment systems, plus the option of setting up a protection system to block botnet communication with command and control centers;

- **Raw Intelligence Data Feeds** – contain a set of streams with up-to-date information on malware, making it possible to proactively set up the necessary protection solution;
- **Intelligence Reports** that take into account regional and industry specifics to highlight the threats most relevant to certain organizations, and which include interpretation of statistical data and a vulnerability assessment;
- **Cyber-Security Education** to transfer a wealth of hands-on experience to information security officers, effectively equipping them with the tools to counter undesirable cyber activity.

In order to combat APT attacks and persistent adversaries organizations, a Continuous Real Time Threat Detection (and Protection) model needs to be adopted in the ecosystem.

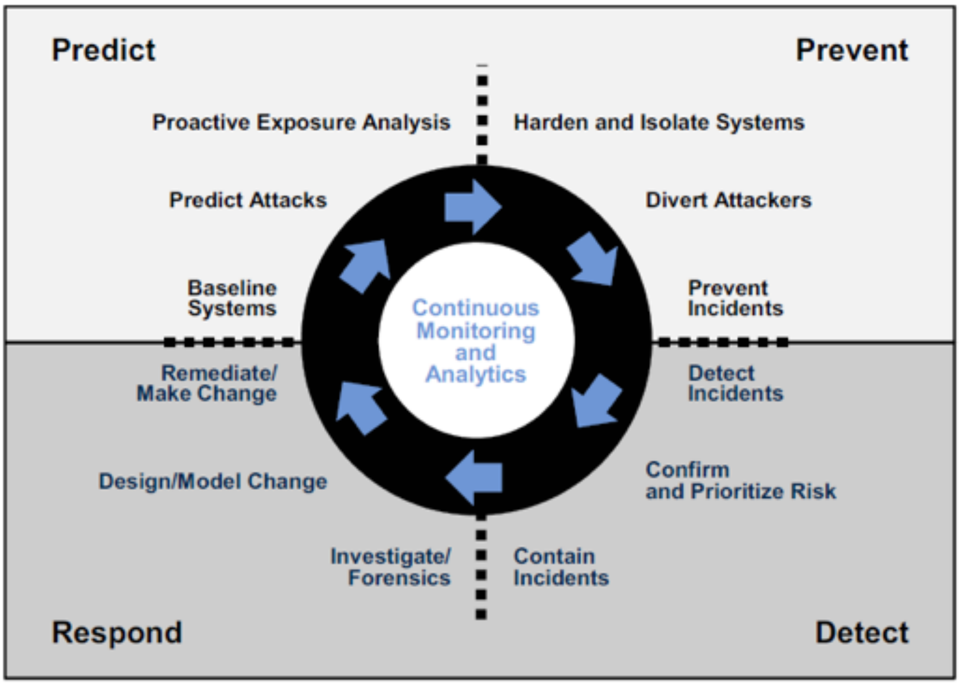
This will however only be possible in the context of an alliance model, because of the highly sophisticated and thus resource intensive efforts needed to share the necessary information and counterbalance threats.

8.2. Core tasks of the alliance: predict, detect, response and prevent

The question of responding to real time security threats is linked to finding out how to best prioritize the present security resources, both organizational and financial, to cope then with APTs. What frameworks will be used to successfully align counter efforts and communicate the impact that those security measures are having to a given organization.

Earlier in 2014, Gartner released a research note called *"Designing an Adaptive Security Architecture for Protection From Advanced Attacks."*[56] The critical capabilities for adaptive security are predictive preventive, detective and responsive in nature.

Figure 17:
Gartner 12 Critical Capabilities of Gartner's Adaptive Security-Architecture.
Source Gartner Research.



This means having the ability to detect threats in real time as well as reduce the time to contain and resolve the threat, thereby preventing or minimizing the business impact of these threats.

This constitutes the need for a platform with a multi-faceted approach to security and an almost real-time sharing of information as well as synchronizing actions. In other word, the platform instantiates the cyber threat detection and response capabilities of the alliance. This includes elements as folllows:

- **Prevent –** Prevention must enable real-time, proactive blocking and provide rich and actionable intelligence to better understand the nature of attacks for a continuous improvement of the security capability.
- **Detect –** Today's advanced threats require an architecture that is aware of the multi-stage and multi-vector nature of attacks. The security platform must be able to detect known and unknown threats in real time and be able to scale with the demands of the network.
- **Respond –** Effective containment demands real-time validation of threats coupled with the ability to rapidly stop the impact of an attack on compromised systems.
- **Predict/Resolve –** To limit exfiltration and serious business impact, security incidents must be investigated, scoped, and resolved in a timely and cost effective way.

8.3. Secure information sharing in the alliance – the organizational side

The alliance represents the governance body and is bound by an agreement between the partners. The platform is a combination of organizational entities that instantiates the governance. And the underlying IT environments serves to support the activities, the information flow and processes.

In this context, the need for a secure information sharing environment have therefore become more and more evident.

It a good reference example, to analyse the efforts the U.S. Dept. of Homeland security has undertaken to construct such a secure information sharing platform by establishing the following entities and initiatives[57]:

Four key elements of the homeland security information sharing architecture bring to bear the strength of the entire homeland security enterprise:

- **National Network of Fusion Centers:** Fusion centers serve as focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information between the federal government and state, local, tribal, territorial (SLTT) and private sector partners.
- **Nationwide Suspicious Activity Reporting Initiative:** Our efforts, in coordination with the Department of Justice, to implement a unified process for reporting, tracking, and accessing [SARs] in a manner that rigorously protects the privacy and civil liberties of Americans, as called for in the National Strategy for Information Sharing.
- **National Terrorism Advisory System (NTAS):** The NTAS, replaces the color-coded Homeland Security Advisory System (HSAS). This system will more effectively communicate information about terrorist threats by providing timely, detailed information to the public, government agencies, first responders, airports and other transportation hubs, and the private sector.
- **If You See Something, Say Something:** The Department's nation-wide public awareness campaign –a simple and effective program to raise public awareness of indicators of terrorism and violent crime, and to emphasize the importance of reporting suspicious activity to the proper state and local law enforcement authorities.

8.4. Secure information sharing in the alliance – the IT architecture side

The platform to build a secure information sharing architecture is necessarily built upon a secure cloud platform, given the need to interface network and connect different stakeholders.

Several national examples exist, for instance in the UK[58]:

The Cyber-security Information Sharing Partnership (CiSP), part of CERT-UK, is a joint industry government initiative to share cyber threat and vulnerability information in order to increase overall situational awareness of the cyber threat and therefore reduce the impact on UK business.
CiSP allows members from across sectors and organisations to exchange cyber threat information in real time, on a secure and dynamic environment, whilst operating within a framework that protects the confidentiality of shared information.

However we strongly believe that a Pan-European, industry and SME focused approach is currently needed, in order to maximize the benefits for European industry organizations that not always share the same requirements with public infrastructures and organizations.

Security economics and risk models Enterprises are overly dependent on blocking and prevention mechanisms that are decreasingly effective against advanced attacks. Comprehensive protection nowadays requires an adaptive protection process integrating predictive, preventive, detective and response capabilities.

8.5. Big data analytics

The analysis of threat data and forensics have increasingly become a task for specialist teams and organization. These can be linked to an alliance.

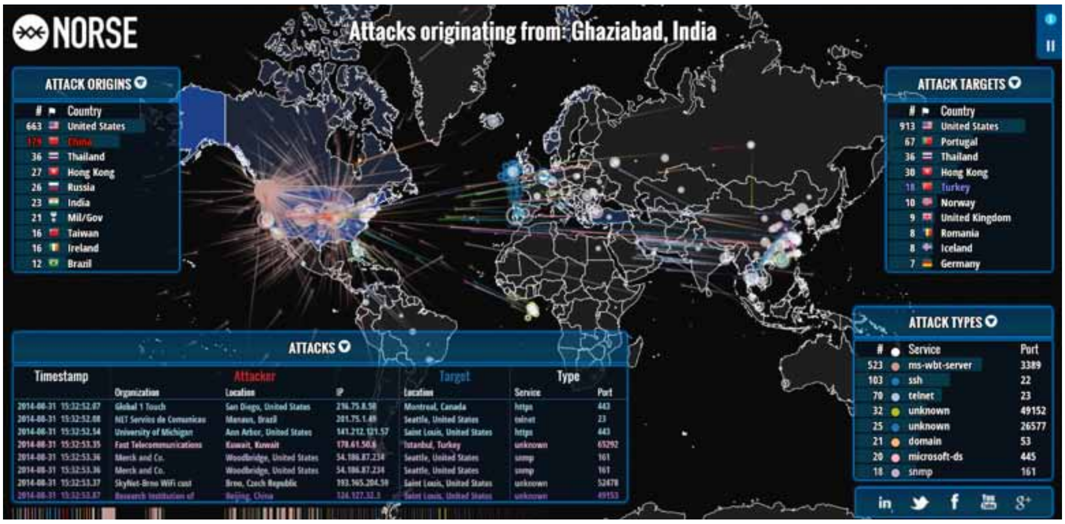
Every second, NORSE e.g. collects and analyzes live threat intelligence from darknets in hundreds of locations in over 40 countries. The attacks shown are based on a small subset of live flows against the Norse honeypot infrastructure, representing actual worldwide cyber attacks by bad actors. At a glance, one can see which countries are aggressors or targets at the moment, using which type of attacks (services-ports).

There are a number of such real time information providers on cyber threats, as can be seen from the few examples below. However, further integration effort is needed to link the appropriate provider and data analytics capabilities with an alliance.

An example of a Threat defend technology that takes advantage of a secure cloud environment, is IBM's Virtual Patch Technology[59].

According to a SANS network study by James Tarala[60], the process of using IT security expertise to manually analyze unstructured data sets from different security systems, applications and network traffic sets is costly, inefficient and error-prone. Cyber threat monitoring will therefore likely evolve towards a Big Data Cloud model where organizations can tap on pooled data and analytics capability.

Figure 18:
Example of real time threat visualization.
Source Norse.com



ATTACK ORIGINS

#	Country
663	United States
179	China
36	Thailand
27	Hong Kong
26	Russia
23	India
21	Mil/Gov
16	Taiwan
16	Ireland
12	Brazil

ATTACK TARGETS

#	Country
913	United States
67	Portugal
36	Thailand
30	Hong Kong
18	Turkey
10	Norway
9	United Kingdom
8	Romania
8	Iceland
7	Germany

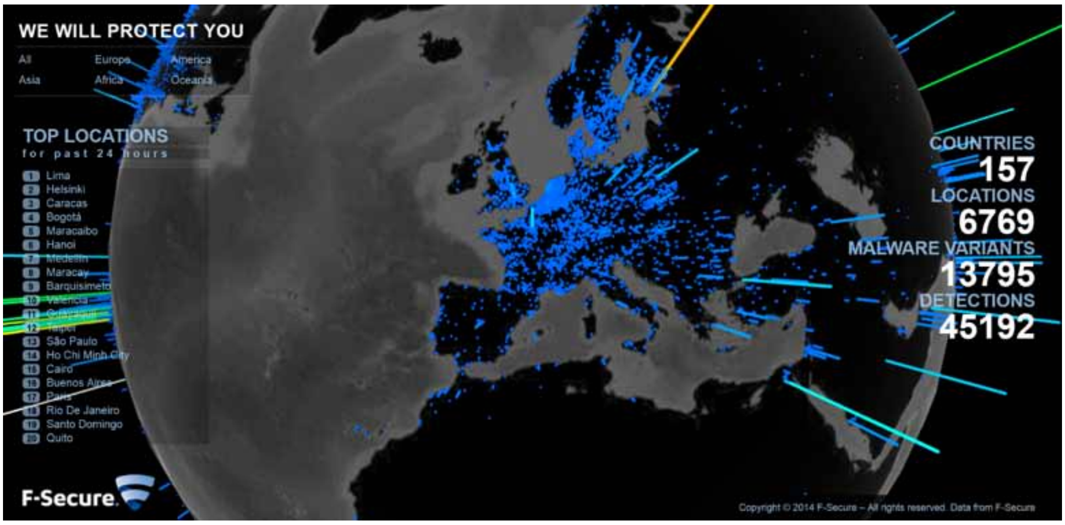
ATTACKS

Timestamp	Attacker			Target	Type	
	Organization	Location	IP	Location	Service	Port
2014-08-31 15:32:52.07	Global 1 Touch	San Diego, United States	216.75.8.58	Montreal, Canada	https	443
2014-08-31 15:32:52.08	NET Servios de Comunicao	Manaus, Brazil	201.75.1.49	Seattle, United States	telnet	23
2014-08-31 15:32:52.54	University of Michigan	Ann Arbor, United States	141.212.121.57	Saint Louis, United States	https	443
2014-08-31 15:32:53.35	Fast Telecommunications	Kuwait, Kuwait	178.61.50.6	Istanbul, Turkey	unknown	65292
2014-08-31 15:32:53.36	Merck and Co.	Woodbridge, United States	54.186.87.234	Seattle, United States	snmp	161
2014-08-31 15:32:53.36	Merck and Co.	Woodbridge, United States	54.186.87.234	Seattle, United States	snmp	161
2014-08-31 15:32:53.37	SkyNet-Brno WiFi cust	Brno, Czech Republic	193.165.204.59	Saint Louis, United States	unknown	52478
2014-08-31 15:32:53.87	Research Institution of	Beijing, China	124.127.32.3	Saint Louis, United States	unknown	49153

ATTACK TYPES

#	Service	Port
523	ms-wbt-server	3389
103	ssh	22
70	telnet	23
32	unknown	49152
25	unknown	26577
21	domain	53
20	microsoft-ds	445
18	snmp	161

Figure 19:
Example of another of real time threat visualization.
Source: F-Secure



TOP LOCATIONS
for past 24 hours

1. Lima
2. Helsinki
3. Caracas
4. Bogotá
5. Maracaibo
6. Hanoi
7. Medellin
8. Maracay
9. Barquisimeto
10. Valencia
11. Guayaquil
12. Taipei
13. São Paulo
14. Ho Chi Minh City
15. Cairo
16. Buenos Aires
17. Paris
18. Rio De Janeiro
19. Santo Domingo
20. Quito

COUNTRIES	157
LOCATIONS	6769
MALWARE VARIANTS	13795
DETECTIONS	45192

Copyright © 2014 F-Secure – All rights reserved. Data from F-Secure

8.6. Cognitive computing

Current threat analysis engines combine advanced statistical analysis techniques with cutting-edge computer security procedures, using multivariate analysis to distinguish cyber threats from legitimate Internet traffic. Previous generation methodologies used to detect cyber threats rely on asymptotic normality and independence assumptions. Errors in these assumptions cause automated detection algorithms to fail or produce large false-alert rates. Multivariate analysis proposes to analyze cyber traffic to correctly account for the distribution and covariance structure. Accounting for these attributes increases the detection capability by an order of magnitude and decrease the false-alert rates.

Multivariate analysis is used to create an analysis methodology that will compare each piece of cyber traffic to all other cyber traffic. The method will build upon current statistical literature so that millions of data points can be compared and accounted for simultaneously. In effect, the procedures allow to create and update a continuous real-time model of legitimate cyber traffic and use the model to detect anomalous behaviour.

Next generation systems will employ cognitive computing AI models to further increase the detection capability and discern between real time threats and false alarms. An independent database for getting access to a large, diverse, and continually expanding database of threat patterns will be key.

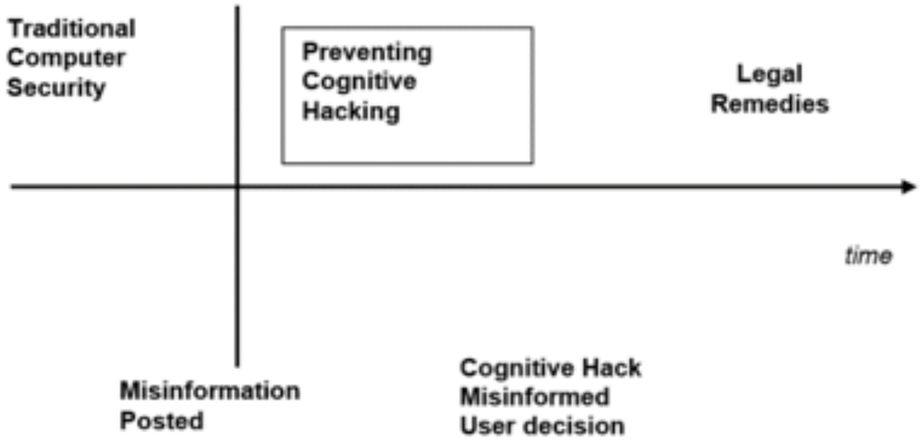
The recent successes of IBM's Watson[61] platform show the potential of tapping – via a cloud model – into next generation analytical and self-learning capabilities including the processing of vast amounts of unstructured and textual information.

This also takes into account that APTs may include far more than incident information on a technical level. An example for this is the use of false or misleading information intended to influence reader's decisions and/or activities that were introduce by hackers – a tactic that is also known as "cognitive hacking"

The Internet's open nature makes it an ideal arena for dissemination of misinformation. Cognitive hacking differs from social engineering, which, in the computer domain, involves a hacker's psychological tricking of legitimate computer system users to gain information, e.g., passwords, in order to launch a syntactic attack on a system[62].

Hence, detecting an APT threat will need the real-time analysis of complex patterns of different kind of information.

Figure 20:
Cognitive Attack sequencing


Traditional Computer Security
Preventing Cognitive Hacking
Legal Remedies
time
Misinformation Posted
Cognitive Hack Misinformed User decision

8.7. Simulations

A recent Bloomberg Government study[63] has found that if companies such as utilities, banks, phone carriers want to make their systems 95% attack proof, they would need to spend almost nine times more on cyber security than what they spend now.

This is of course difficult to achieve, however there might be a solution in Simulation, to mitigate those effects.

In fact a great potential to overcome existing Gaps lies also in Simulation. Organizations can benefit from the use of risk modelling and simulation technologies to gain a complete understanding of cyber security risks as well as simulate response opportunities to cyber security problems, relative to their specific domain.

Risk modelling and simulation can be incorporated into day-to-day IT operations – validating planned network changes, confirming that security controls are working, or performing a full compliance audit without affecting the live network.

Using modelling and simulation technologies, a cyber security simulation framework can provide a complete portfolio of automated security risk management solutions. For example, organizations can automatically examine multiple firewalls to find and fix security gaps, troubleshoot complex network access issues, or prioritize vulnerabilities to address before they can be exploited by an attacker.

9. Gap VIII: Improving education and skills for European cyber security

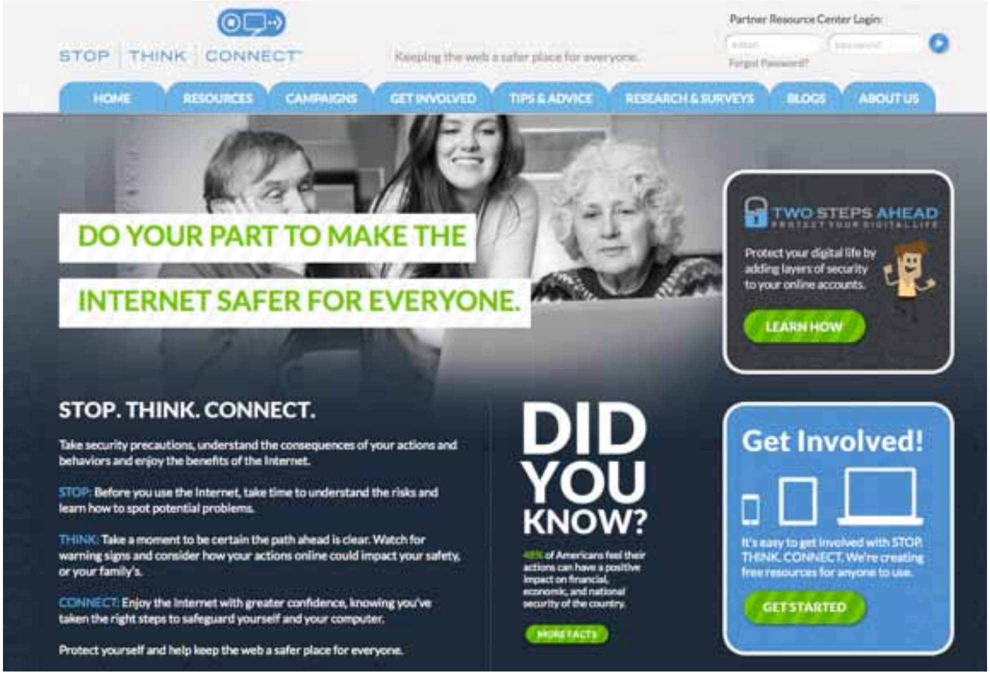
The need for improving education and fostering skills on cyber security in Europe has been mentioned at several occasions in the CYSPA analysis. This has multiple aspects. While cyber security is widely recognized as an important concern for Europe, it is still regarded by the general public as a complex and predominantly technical expert topic. The CYSPA analysis of existing solutions[64] shows that, compared to this, the U.S. is already addressing cyber security education as a national priority and on a broader scale.

Awareness raising on cyber security has started early in the U.S. with the first National Cyber Security Awareness Month in October 2004[65]. Cyber security education is now further promoted by the *National Initiative for Cybersecurity Education (NICE)*[66] under the lead of the National Institute of Science and Technology as well as the *National Initiative for Cybersecurity Careers and Studies (NICCS)*[67] under lead of the Department of Homeland Security.

A characteristic of both initiatives is that they address a wide range of stakeholders including the general public, students, educators and parents. At the same time, they also address the cyber security workforce: like cyber security professionals, cyber security mangers as well as human capital managers that are involved in the recruitment of cyber security experts.

Linked to this is the *Stop.Think.Connect*[68] awareness campaign. The campaign addresses not only the general public but also organizations and businesses in several segments. From the organizational viewpoint, the campaign is organized by a public-private-partnership with founding industry partners such as Microsoft, Google, AT&T, Facebook and others. *Stop.Think.Connect* also promotes dedicated toolkits for different groups of the population (e.g. by age group, or specific minority groups) as well professional segments (industry, small business, government).

Figure 21:
U.S. cyber security awareness campaign Stop.Think.Connect



Protect your digital life by adding layers of security to your online accounts.

STOP. THINK. CONNECT.

Take security precautions, understand the consequences of your actions and behaviors and enjoy the benefits of the Internet.

STOP: Before you use the Internet, take time to understand the risks and learn how to spot potential problems.

THINK: Take a moment to be certain the path ahead is clear. Watch for warning signs and consider how your actions online could impact your safety, or your family's.

CONNECT: Enjoy the Internet with greater confidence, knowing you've taken the right steps to safeguard yourself and your computer.

Protect yourself and help keep the web a safer place for everyone.

48% of Americans feel their actions can have a positive impact on financial, economic, and national security of the country.

It's easy to get involved with STOP. THINK. CONNECT. We're creating free resources for anyone to use.

The European Union has piloted in 2012 the first European Cyber Security Month coordinated by ENISA (the European Union Agency for Network and Information Security).

In 2013, the European Commission has adopted in its "Cybersecurity Strategy of the European Union"[69] the European Cyber Security Month as a yearly event. Also the Commission has proposed further education activities:

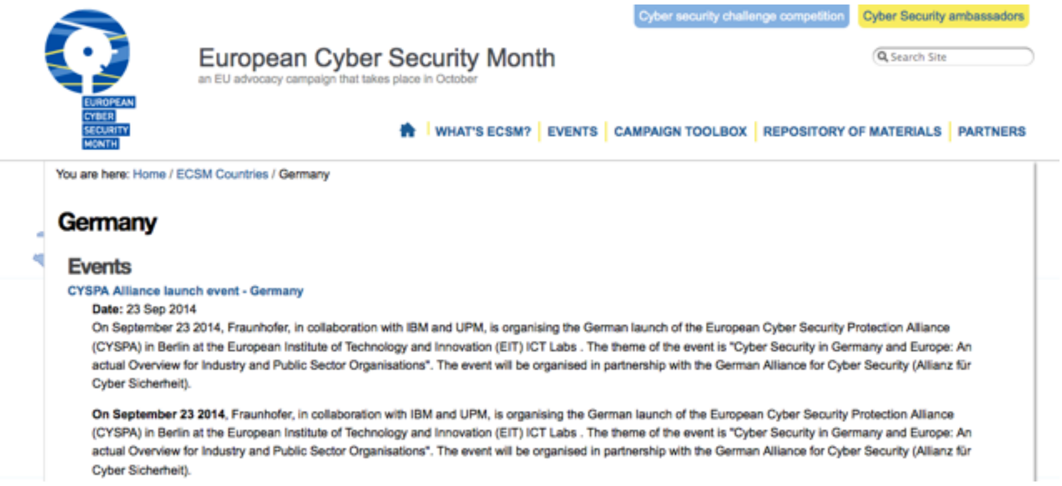
- the organization of a yearly Pan European Cyber Challenge (currently planned for 2015)
- development of a roadmap for a "Network and Information Security driving licence" as a voluntary certification programme to promote enhanced skills and competence of IT professionals

Further to these direct actions at European level, the European Commission has invited member states to step up national efforts on cybersecurity training and education. Also industry is invited to promote cybersecurity awareness at all levels.

9.1. Aligning national and European initiatives on cyber security education

According to the CYSPA analysis[70], as of 2014 several EU member states[71] have included cyber security education in national strategies. However, there is only limited transparency of the relative efficiency and impact of national initiatives so far – e.g. which of them could be considered as European lighthouse initiatives and serve as role models on cyber security education for other countries.

At the same time, have several initiatives at national level developed innovative approaches. Examples are the Cyber Security Challenge UK[72] or the eSkills UK initiative that has in 2013 created the first European cyber security apprenticeship programme[73] with partners like Atos, Cassidian, IBM and Capgemini.


Cyber security challenge competition
Cyber Security ambassadors
EUROPEAN CYBER SECURITY MONTH
European Cyber Security Month
an EU advocacy campaign that takes place in October
Search Site
WHAT'S ECSM? | EVENTS | CAMPAIGN TOOLBOX | REPOSITORY OF MATERIALS | PARTNERS
You are here: Home / ECSM Countries / Germany

Germany

Events

CYSPA Alliance launch event - Germany

Date: 23 Sep 2014

On September 23 2014, Fraunhofer, in collaboration with IBM and UPM, is organising the German launch of the European Cyber Security Protection Alliance (CYSPA) in Berlin at the European Institute of Technology and Innovation (EIT) ICT Labs . The theme of the event is "Cyber Security in Germany and Europe: An actual Overview for Industry and Public Sector Organisations". The event will be organised in partnership with the German Alliance for Cyber Security (Allianz für Cyber Sicherheit).

On September 23 2014, Fraunhofer, in collaboration with IBM and UPM, is organising the German launch of the European Cyber Security Protection Alliance (CYSPA) in Berlin at the European Institute of Technology and Innovation (EIT) ICT Labs . The theme of the event is "Cyber Security in Germany and Europe: An actual Overview for Industry and Public Sector Organisations". The event will be organised in partnership with the German Alliance for Cyber Security (Allianz für Cyber Sicherheit).

Figure 22: European Cyber Security Month. Example: Event in Germany in collaboration with CYSPA[74]

An instrument that was created to support the European sharing of practices and a coordination of industry activities is the European Network and Information Security (NIS) platform which was launched as a direct consequence of the EU Cyber Strategy. In the NIS platform the topic of education and training for workforce skills is a subtopic of the Workinggroup 3 "Secure ICT Research and Innovation". CYSPA is also active in this group.

However, the NIS platform currently only addresses a part of the entire scope of European cyber security education and training (that also needs to include the general public, students, parents, schools, specific age groups – like the elderly etc.). For this purpose, a wider collaboration with European initiatives is needed including the eSkills initiative, Open Education Europa and the new initiatives just developing around the Horizon 2020 societal challenges on the young generation and digital skills, learning and inclusion.

Compared to the U.S. where the cyber security education programmes are largely centralized, the situation in Europe is therefore more fragmented and determined by the interplay between national and European level. A European platform could bring these different strands together and better align European cyber security education with benefit to all national initiatives.

9.2. A European awareness and education campaign on cyber security

The European Cyber Security Month (ECSM) initiative provides a campaign toolbox for member states to be used in individual national campaigns and has started to collect a repository of materials. Also it has produced a small number of videos on cyber secure user behaviour.

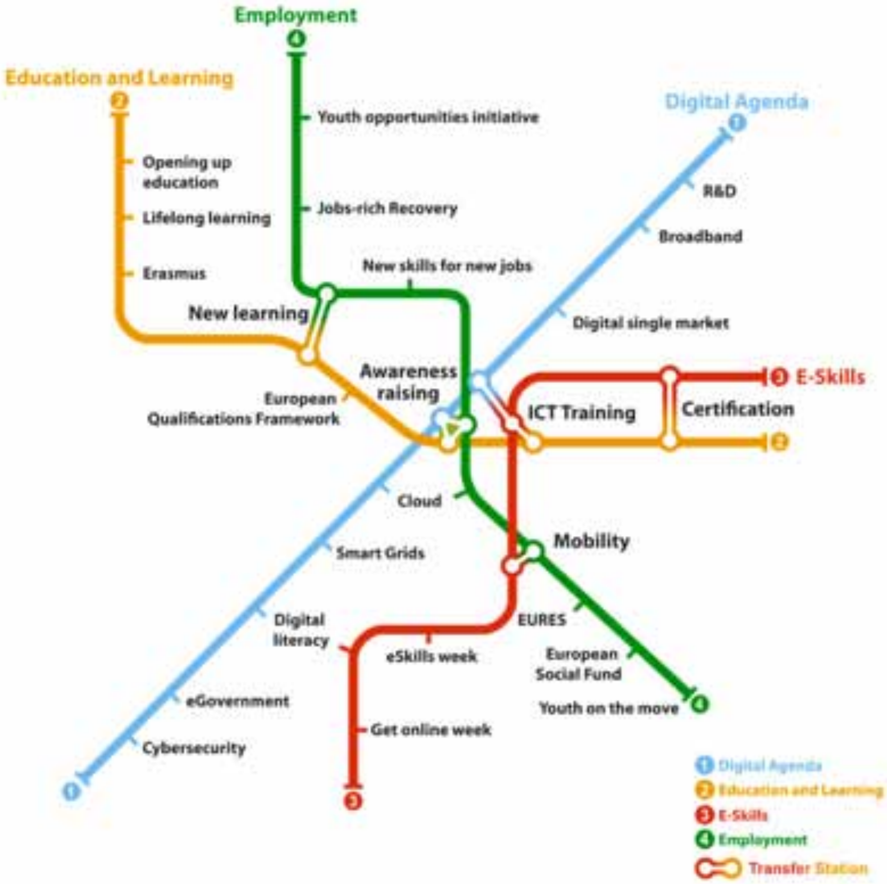
The U.S. Stop.Think.Connect campaign is based on a similar structure, but as of 2014, has already a richer repository of material specific for different target groups. Also it supports educators (e.g. school teachers) with pedagogical advice how to use the material. The combination of educational material and pedagogical advice is important in rolling out the campaign to education institutions.

The campaign provides further a separate portal for comfortable access to these resources sorted by different target groups. In addition to providing open resources, the campaign includes a particular effort to building and growing a community. This includes a large number of academic and business alliance partners as well as state and city governments. It also includes alliances with a large number of non-for-profit initiatives, most of them active in education. This allows further spreading of the campaign activities. Finally, individuals are allowed and the campaign connects to a programme of volunteers.

Stop.Think.Connect further has reached out globally and created partnerships with complementary local initiatives. Three of these global partnerships are located in Europe – in Spain, Belgium and Germany. The German initiative called Botfrei[75] (bot-free) e.g. provides a free portal service to check a computer and IP address against traces of bot activities.

The pedagogical design of the campaign and the extensive support with educational material as well as the growing of a wider community would also be objectives of a European campaign initiative. This could extend the current scope of the ECSM. The same applies for the link to practical tools and free security checking services.

Figure 23:
European Map of e-Education.
Source: European Commission



9.3. Aligning with the European e-skills initiative on cyber security skills

eSkills[76] is a well established European initiative since 2007 to promote workforce skills, training and employment opportunities in the European ICT industry. In 2013 it became part of the Grand Coalition for Digital Jobs launched by Commission President Barroso.

eSkills has several elements including a yearly eSkills[77] week that is run in partnership with the national ICT industry organizations. Also, eSkills is active with a network of European business schools, training providers and universities to define Curriculum Guidelines in several relevant fields related to ICT professions. Finally, this is linked to a certification programm.

Several industrial stakeholders support the eSkills campaign including also the European Learning Industry Group (ELIG)[78] a platform organization of education providers, educational technology firms and content providers.

The eSkills initiative can be an important support in advancing professional skills in the domain of cyber security including also skills at management level. Due to the close collaboration with ICT industry partners, national ICT industry association and professional learning and education providers, it also provides a good network with a European reach into training and educating ICT professionals.

9.4. Open cyber security education and the European Opening up Education Initiative

Open educational resources (OER) and open education approaches – e.g. massive open online courses (MOOCs) – are gaining in popularity. Courses from platforms such as edX, Coursera or Udacity are able to attract thousands of students to enroll and learn online.

The European Commission has reacted to the growing impact of open education by launching in 2013 the Opening up Education[79] initiative. One central element is the Open Education Europa Portal. The portal can be used to share open educational content and provide it with a European visibility.

OER are typically modules for self-paced learning which can include videos, text, presentations and alike. MOOCs combine these into a course of a limited duration (several weeks) and include student networking, assignments and interaction with the team of course facilitators.

This format is interesting for spreading cyber security education and can reach very large numbers of participants. However, the competition in the global market of MOOCs and OER has led to a significant rise in professionalization and quality requirements.

This also implies that developing attractive MOOCs and OER has become effort intensive and today has to include a professional production of audio, video and learning material. Also there is a strong dependency on the quality of the teaching/moderating persons.

The UK Open University receives funding starting in 2014 as part of the UK's National Cyber Security Programme to develop a MOOC on Cyber Security[80]. This has also been included in the official UK Cyber Security Strategy and announced in the House of Commons – which underlines that it is regarded as an important and publicly visible element in the strategy.

MOOCs and OER are an interesting option to pursue in the context of a European education programme on cyber security. But as stated above, launching a high quality MOOC demands a particular development and funding effort which is similar to other professional media campaigns. Also MOOCs will demand continuous moderation and steering effort. At the same time, elements of the MOOC may be used as stand-alone OER.

For a European wide cyber security education initiative another aspect of MOOCs is interesting. MOOCs can be localized to individual geographies or languages with a limited effort compared to producing a MOOC from scratch (e.g. by synchronization in local language or adding local content elements). That would allow to produce a cyber security MOOC and OERs on a European scale while it still could be localized to each member state that likes to adopts it.

9.5. Promoting security by design in software engineering

The importance of promoting security by design has been discussed in Gap IV. From the viewpoint of an educational programme this is however not an easy task as the principles of security by design need to be deeper embedded into the training of programmers, into coding classes and higher education programmes for computer scientists and engineers.

Security by design and the general awareness of cyber risks will be an important element in educating the software engineers and ICT solution designers of the future. This demands a close and longer-term collaboration with universities and training institutions.

The European Institute of Technology and Innovation (EIT) ICT Labs could be a potential partner in further promoting security by design in Europe.

The EIT ICT Labs has already defined “Privacy, Security and Trust in Information Society”[81] as one of its Innovation Areas. The EIT ICT Labs has further created a technical major in “Security and Privacy” as part of their Master Programmes in ICT Innovation and offers a summer school on “Privacy, Security and Trust”. All of the EIT education activities are organized in partnership with European universities. At the same time, the EIT is starting to engage in open education as well.

9.6. Using gamified learning

An interesting combination is the overlap beween simulation and cyber education as seen in the example below. Innovative Computer Gaming techniques enhance information assurance and cyber security education and training through the use of computer gaming techniques such as those employed in SimCity™. In the CyberCIEGE[82] virtual world, users spend virtual money to operate and defend their networks, and can watch the consequences of their choices, while under attack.

Figure 24:
Cyber Security Simulation
Game

10. Gap IX: Supporting innovation, entrepreneurial and venture support in European cyber security

10.1. Cyber security R&D support

In all advanced nations, there is support for R&D in Cyber security. In Europe the new Horizon 2020 program, co-finances Cyber security in various lines such as:

- LEIT – ICT 32 – 2014: Cybersecurity, Trustworthy ICT a. Cryptography b. Security – by – design for end to end security
- Societal Challenge 7 – Secure societies "Protecting freedom and security of Europe and its citizens"– Digital Security: Cybersecurity, Privacy and Trust 1. Privacy, 2. Access Control, 3. Risk Management and assurance models

As the following diagram shows, Cyber Security R&D support is also priority in the overall EU policy for Cyber Security and is closely aligned with other elements of the strategy:

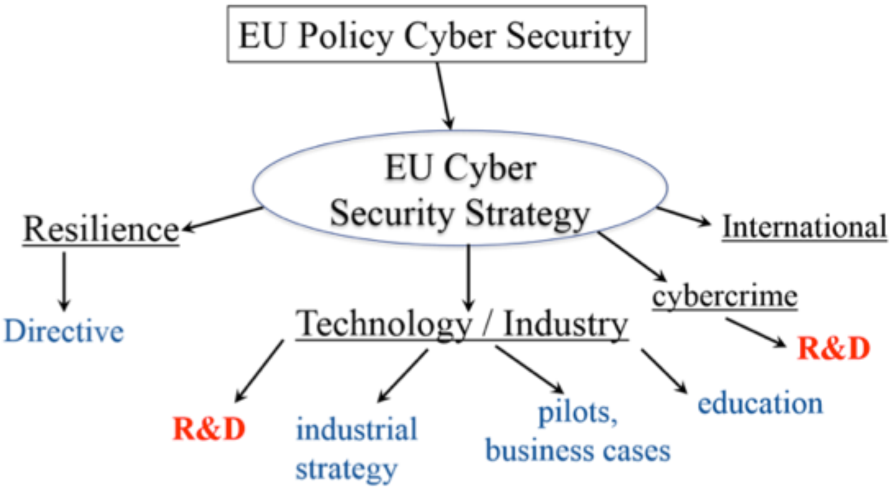


Figure 25:
EU Policy Cyber Security.
Source: EU Commission

Setting priorities for European cyber security research funding should be done in close collaboration with industry. Here, the EU cyber strategy has given a particular role to the Network and Information Security (NIS) platform.

The NIS platform – with involvement of CYSPA – is currently developing a cyber security research roadmap. This is further supported by other groups such as the Cyber Security Research Alliance (CSRA). The CYSPA reports on "Uptake and Innovation Models" and "Analysis of Upcoming Research Results" provide a detailed overview on the current European cyber security research landscape.

As expressed in the previous Gaps, several of the topics touch also other European R&D platforms and constituencies such as the following:

- the European Network Providers – represented in the Net!Works platform
- the European Software and Data-Service Providers – represented in the NESSI and the upcoming Big Data Value platform
- the Smart and embedded Systems Providers – represented in the EPoSS platform
- the Internet Services – represented in the Future Internet Public Private Partnerships

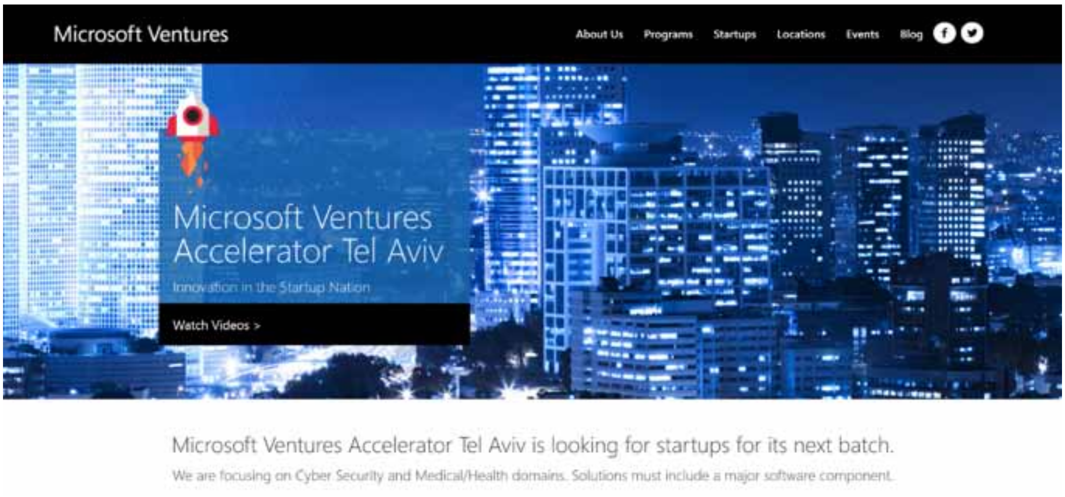
It will be important to position cyber security as a cross-cutting and not a stand-alone issue and trigger related collaboration at EU level with other R&D initiatives in the ICT field. This would also feedback on the cyber security research roadmap.

10.2. Mechanisms to support start-up creation and venture growth in the European cyber security sector

A challenging question is further, how to improve the go to market of innovations that come out of European cyber security R&D. The market of corresponding cyber security solutions is rapidly evolving and Europe should become one of the global hubs for that development.

Start-ups and Venture Capital in the Cyber Security Domain are a very prominent topic in the current evolving landscape for Cyber Security. A sign of the times, just very recently (29 July 2014), Akamai and Microsoft have announced to join forces in the first Cyber-Security focused Start-up accelerator in Israel[83]. Together with leading VC Jerusalem Venture Partners (JVP), they have created a currently unique accelerator in the field of cyber-security. The program is located at the Microsoft Ventures Accelerator in Israel.

Figure 26: Website of the Microsoft Tel Aviv Cyber Security Accelerator. Source Microsoft



Microsoft Ventures Accelerator Tel Aviv

Innovation in the Startup Nation

Microsoft Ventures Accelerator Tel Aviv is looking for startups for its next batch.

We are focusing on Cyber Security and Medical/Health domains. Solutions must include a major software component.

According to a recent analysis of the Wall Street Journal Europe[84], as of 2014 cyber security is among the topics that is fastest growing when it comes to attracting venture capital. In early 2014, C5 Capital launched the first European Cyber Security Venture Fund[85] due to the recognition of the specifics of the European market (e.g. with regard to data protection regulations) and the related business potential.
As such we can only underline the words of the Telefonica CTO who spoke at the European Innovation Convention in March 2014[86]:

“Telefónica believes that it is not solely the role of policy-makers or politicians to make innovation and growth happen, but rather a job for all businesses, schools and universities across Europe. Start-ups, entrepreneurs and intrapreneurs are crucial to Europe’s future growth and critical to providing employment opportunities, particularly among the young.”

The start-up and venture capital approach has a high potential for bringing advanced cyber security solutions to market in Europe and Europe needs to act fast to be a part of this rapidly growing market. Currently, existing mechanisms at EU level for innovation and venture support are relevant but not sufficiently applied yet to the domain of cyber security. Particular support needs to be provided to help bridging this gap between ideas (as e.g. collected in the ICT Labs idea challenge on Cyber security and privacy), technologies out of related R&D projects and actual European ventures.

Figure 27:
Website of the European Cyber Security and Privacy Idea Challenge – organized by the EIT

To highlight specific requirements in this domain, further networking is needed with organizations such as the Open Innovation Strategy and Policy Group (OISPG)[87] that is advising the European Commission on the general instruments and structures of innovation support.

Elements of such specific support could be:

- a European Cyber Security Innovation Prize Scheme linked to seed funding and mentoring by experienced entrepreneurs and business cyber experts

- a European Cyber Security Accelerator to foster networking of start-ups with established industry, VCs and inform on the access to EU innovation funding programmes (such as the SME innovation programme)

- a European Cyber Security Venture fund backed by the European Investment Fund[88]

11. Gap X: Developing incentives to promote cyber security in Europe

Collaboration and the effective sharing of information on incidents and detected attacks are fundamental for the resilience of our cyber ecosystems. In the same way, it is important to motivate organization to adopt a higher level of cyber security that is adapted to the specifics of their business and the criticality of their infrastructure.

However, in particular the private sector has shown resistance to adopt an increased level of cyber security for several reasons. This includes costs concerns. But further to this, it also includes concerns about potential reputation damages if information about critical incidents is leaked.

The RAND Corporation in collaboration with ENISA has investigated in 2010 in a detailed study the barriers and potential incentives for sharing information on cyber security[89]. Also in the EU Cyber Security Strategy multiple references are made to this critical topic and the potential to introduce and highlight incentives for organizations.

The German Government has recently took an alternative direction by making the reporting of critical cyber incidents a legal obligation. However this is not only difficult to enforce and potentially slow, it will also relate only to a limited number of incident categories and organizations. Hence, further efforts need to be put into alternative methods of incentivizing a pro-active attitude and collaboration between public and private organizations on cyber security.

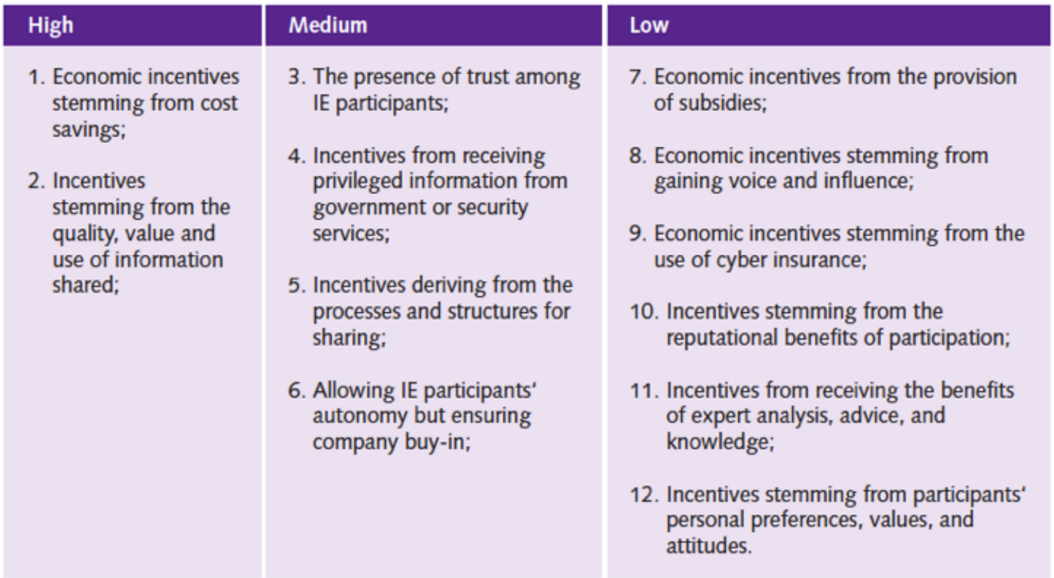
This has different dimensions.

11.1. Incentives for information sharing

The sharing of information is a first and important element. The ENISA-RAND study has already depicted a number of criteria that would be considered as incentives – according to the feedback from organizations they interviewed.

These fall into monetary and non-monetary categories. Non-monetary may e.g. relate to receiving privileged information or other secondary benefits from the networking and partnerships with other organizations (e.g. transferring best practices).

Monetary incentives can directly relate to cost-savings or even public funding programmes that could support the establishing of cyber security practices and cyber information sharing.



High	Medium	Low
1. Economic incentives stemming from cost savings; 2. Incentives stemming from the quality, value and use of information shared;	3. The presence of trust among IE participants; 4. Incentives from receiving privileged information from government or security services; 5. Incentives deriving from the processes and structures for sharing; 6. Allowing IE participants' autonomy but ensuring company buy-in;	7. Economic incentives from the provision of subsidies; 8. Economic incentives stemming from gaining voice and influence; 9. Economic incentives stemming from the use of cyber insurance; 10. Incentives stemming from the reputational benefits of participation; 11. Incentives from receiving the benefits of expert analysis, advice, and knowledge; 12. Incentives stemming from participants' personal preferences, values, and attitudes.

Figure 28:
Incentives for cyber information sharing.
Source: ENISA – RAND Study

11.2. Liability for damages caused by cyber attacks

Cyber risks are also linked to the difficult question of liability. Currently, most providers of critical ICT infrastructure or services such as cloud computing refrain in their legal agreements from any liabilities caused by their services on the side of customers.

However, it is a legal "grey zone" if e.g. insufficient cyber protection could in the future lead to liabilities of the infrastructure or service provider as it could be regarded as a tort of negligence in the case a major cyber incident occurs.

Also large customers are increasingly demanding risk sharing models from their IT outsourcing and cloud providers. Thomas Endres, former CIO of Deutsche Lufthansa, expressed in 2012 in a workshop organized by the European Internet Foundation with European Commissioner Neelie Kroes, that he wants to see cloud providers taking their share of the business risk – e.g. when hosting a business critical infrastructures for Lufthansa like the airline's passenger booking system.

As liabilities will depend on the individual legal context in which the provider operates, a more in-depth analysis of this topic and the current legal conditions in Europe and worldwide and member states would be needed. However, it is obvious that liabilities towards customers could significantly affect the cyber risk case for any organization.

11.3. Cyber risk insurance

A related topic is the potential establishing of cyber risks insurances. These could effectively provide a backing for monetary risks that spring from larger cyber attacks – some of which might be so critical that they could put an entire organization at risk.

Also the costs of the insurance will depend on the one hand on the actual risk in case of a severe cyber attack and on the other hand on the level of protection that the organization could achieve.

11.4. Certification

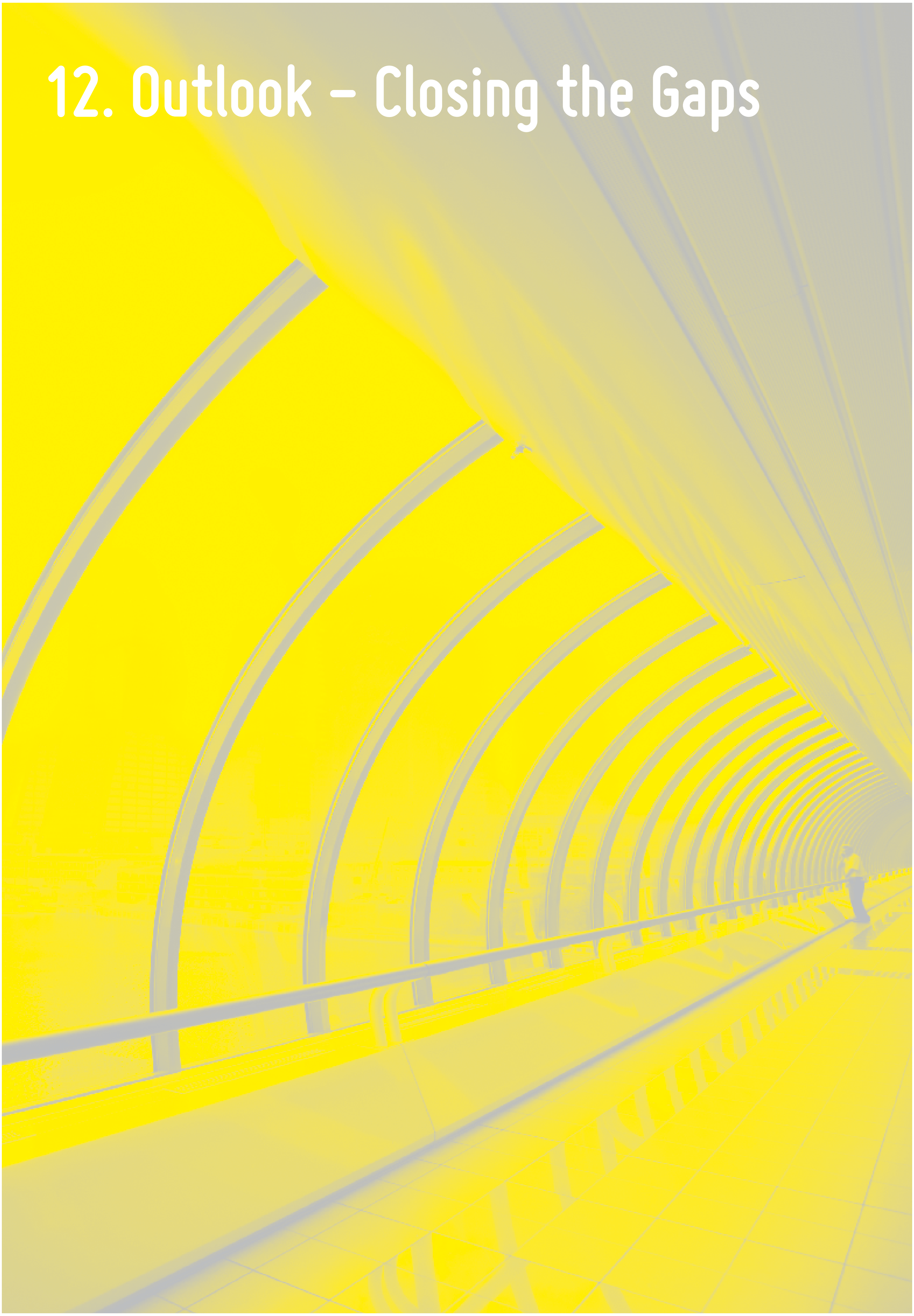
Finally, cyber security certifications schemes are often cited in context of potential incentives. Here, the incentive is primarily seen in the demonstrated and audited level of cyber protection. This should attract and ensure potential customers.

The CYSPA report on "Technologies and Solutions" list a large number of potential certification schemes on cyber security. While of course security standards like the ISO/IEC 27001 family are widely accepted, have not all certification schemes the same level of broad support.

Also, is the value of certification often seen different in the industry. While smaller organizations might see a cyber security certification as a valuable label, larger organizations often question the standards behind the certification scheme and often are in their own practice already advanced compared to the standard demanded by the certification.

Hence, it is questionable if certification should be required or rather be optional and should be obtained by self-initiative.

12. Outlook – Closing the Gaps



The CYSPA Gap analysis demonstrates that European cyber protection is a highly complex topic with multiple facets that range from socio-economic, behavioural, pedagogical and organizational to technical aspects in many areas such as software design, networks and hardware. In addition there is a close interplay between private-sector and public sector organizations as well as national and international governmental agencies and authorities.

Further to this, there is an important dependency on fundamental technologies of the Internet, the web, next generation mobile and fixed line networks and hence also the need to interface with the standards and other organizations that are driving these developments.

Still, there are multiple dimensions by which the protection of cyber space can be addressed: from security hardening devices OS, to safer access and authentication technologies, to highly protected networks and data centres. From simulations and cyber risk models to threat monitoring, big data analytics and preventive measures in near real-time. From organizational alliances to awareness programmes, education and skill building.

The value of the CYSPA alliance springs from its role as a hub for sharing information, for bringing partner organizations together, for raising awareness, or relating to policy makers in all these areas. A strong public-private partnership is essential to make progress in the protection of European cyber space. Industry has a particular role here as industry organizations are close to the technical and solutions development on the one hand, as well as to the consumers, their customers and solution markets on the other hand. Industry is also developing the products and digital services of tomorrow. The value of CYSPA is that it provides an industry centric perspective on European level in the cyber security debate while being fully embedded into the wider overall public-private-partnership efforts in Europe on cyber security (e.g. in the European NIS platform).

CYSPA also brings together wide technical expertise and a broad portfolio of cyber security solutions We have therefore in this gap report also argued that the actual development trends on the cyber security solution side need to be taken into account in the European cyber security debate. At the same time are our cyber ecosystems developing and they are developing increasingly fast. The Internet of things, the still exponential growth of the mobile Internet, cloud computing, cognitive computing, social computing, big data analytics – all these are trends that shape our digital future.

The perspective of looking at gaps as long-term challenges is helpful here, rather than as "problems" that could be solved in a limited timeframe. We need to take into account that the development of cyber protective solutions runs in parallel with the broad trends mentioned before that are shaping our cyber ecosystems overall.

Complementary to our CYSPA report on "Understanding and Managing Cyber Risks", this document should therefore serve to understand the evolving solution side of cyber protection in term of where we are know and where current development is headed. Closing these Gaps might be a goal that is not possible to obtain but with each progress that we make we are advancing our level of cyber protection.

Footer

1 http://www.spiegel.de/netzwelt/netzpolitik/de-maiziere-it-sicherheitsgesetz-mit-meldepflicht-fuer-cyberangriffe-a-986621.html

2 http://www.bka.de/nn_205924/DE/Presse/Pressemitteilungen/Presse2014/140827__BundeslagebildCybercrime.html

3 http://www.tclouds-project.eu/downloads/TClouds_12_final_150dpi.pdf

4 http://www-935.ibm.com/services/us/en/it-services/security-services/2014-cyber-security-intelligence-index-infographic/

5 see e.g. section 6.5 (pp. 50) in the CYSPA report on “Understanding and Managing Cyber Risks”

6 http://blogs.msstate.edu/ored/2012/04/fonash_presents_cyber_ecosyste_1.html

7 http://www.google.com/ideas/projects/digital-attack-map/

8 for a recent example weakness see: http://www.wired.co.uk/news/archive/2013-02/05/weakness-in-tsl-protocol

9 further examples of vulnerabilities related to the specific OpenSSL library implementation of the SSL protocol can be seen here: imhttp://en.wikipedia.org/wiki/OpenSSL

10 http://www.dwavesys.com/

11 http://www.1qbit.com/

12 for the case see: http://en.wikipedia.org/wiki/DigiNotar

13 http://www.cnet.com/news/google-yahoo-skype-targeted-in-attack-linked-to-iran/

14 http://www.idquantique.com

15 http://www.battelle.org/media/press-releases/-first-commercial-quantum-key-distribution-protected-network-in-u.s

16 http://www.networkworld.com/article/2172821/security/quantum-crypto--standard-private-key-blended-for-first-time.html

17 http://www.mobbeel.com/

18 http://www.forrester.com/Personal+Identity+Management+Success+Starts+With+Customer+Understanding/fulltext/-/E-RES61039

19 see e.g. the demonstration by security expert Daniel Cid in his blog: http://blog.sucuri.net/2013/07/from-a-site-compromise-to-full-root-access-bad-server-management-part-iii.html

20 http://www.zdnet.de/88194086/cross-site-scripting-luecke-auf-ebay-entdeckt/

21 http://www.informatics.indiana.edu/xw7/papers/privilegescalationthroughandroidupdating.pdf

22 http://www.zurich.ibm.com/security/idemix/

23 https://ict-rerum.eu/rerum-has-started/

24 http://en.wikipedia.org/wiki/Security_AppScan

25 Vorgang, Blair R.; Karry, Alec: Addressing Software Security in the Federal Acquisition Process
. Cigital White Paper, https://www.cigital.com, 2011

26 http://www.microsoft.com/security/sdl/default.aspx

27 http://www.ibm.com/developerworks/library/se-framework/

28 http://www.google.com/enterprise/apps/business/resources/docs/security-whitepaper.html#introduction

29 https://www.owasp.org/index.php/About_OWASP

30 http://searchsecurity.techtarget.com/definition/Open-Source-Hardening-Project

31 http://de.scribd.com/doc/95282643/Backdoors-Embedded-in-DoD-Microchips-From-China

32 http://link.springer.com/chapter/10.1007%2F978-3-642-33027-8_2

33 http://www.mcafee.com/us/solutions/mcafee-deepsafe.aspx

34 http://www.trustedcomputinggroup.org/

35 http://www.theregister.co.uk/2010/02/17/infineon_tpm_crack/

36 http://www.ivizsecurity.com/security-advisory-iviz-sr-0801.html

37 http://www.proofpoint.com/about-us/press-releases/01162014.php

38 http://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption

39 http://labs.apnic.net/ipv6-measurement/Regions/

40 http://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption

41 see section 3.4 “Specific threats to next generation web standards”

42 https://developers.google.com/speed/public-dns/docs/security?hl=de

43 Source of data: wikipedia – http://en.wikipedia.org/wiki/LTE_%28telecommunication%29

44 http://www.engagemobile.com/public-relations-and-the-mobile-space-engage-mobile-at-the-kc-prsa/

45 http://www.statista.com/chart/1009/mobile-internet-traffic-growth/

46 http://tools.ietf.org/html/rfc3113

47 http://the-mobile-network.com/article/MTM4/4G-hype-leading-to-LTE-security-shortcuts.html

48 http://business.verizonwireless.com/content/b2b/en/4glte/4gltefaqs.html

49 see section 5 “Threats to Networks”

[50] http://www.eetimes.com/document.asp?doc_id=1278938

[51] http://www.businesswire.com/news/home/20140708006124/en/iBeaconBLE-Beacon-Shipments-Break-60-Million-2019#.VALzHkhw7n1

[52] ghts.wired.com/insights/wp-content/uploads/2014/05/ibeacon_660.jpg

[53] http://www.mediapost.com/publications/article/231883/getting-privacy-right-is-key-to-beacon-deployment.html

[54] https://firstlook.org/theintercept/2014/08/15/cat-video-hack/

[55] http://www.kaspersky.com/about/news/business/2014/Kaspersky-Lab-and-Telefonica-join-forces-to-improve-cyber-protection-for-European-and-Latin-America-customers

[56] https://www.gartner.com/doc/2665515?ref=SiteSearch&sthkw=adaptive%20security%20architecture&fnl=search&srcId=1-3478922254

[57] https://www.dhs.gov/topic/information-sharing

[58] https://www.cert.gov.uk/cisp/

[59] http://www-01.ibm.com/support/knowledgecenter/SSB2MG_4.6.0/com.ibm.ips.doc/concepts/virtualpatchtechnology.htm

[60] SANS Analyst Program 11 A Real-Time Approach to Continuous Monitoring http://www.sans.org/reading-room/whitepapers/analyst/real-time-approach-continuous-monitoring-34950

[61] http://www.computerweekly.com/news/2240212242/Watson-powers-IBMs-1bn-cognitive-computing-business

[62] Cognitive hacking and intelligence and security informatics. Paul Thompson, http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.87.6587

[63] http://www.bloomberg.com/news/2012-01-31/cybersecurity-disaster-seen-in-u-s-survey-citing-spending-gaps.html

[64] CYSPA Report D3.1 – Section 6 Cyber Security Related Training and Education

[65] http://www.dhs.gov/national-cyber-security-awareness-month-2014

[66] http://csrc.nist.gov/nice/education.htm

[67] http://niccs.us-cert.gov/

[68] http://www.dhs.gov/stopthinkconnect

[69] http://ec.europa.eu/digital-agenda/en/news/communication-cybersecurity-strategy-european-union-%E2%80%93-open-safe-and-secure-cyberspace

[70] see chapter 6.2. Education & Training Programmes in the CYSPA report D3.1 on "Technologies and Solutions"

[71] for an ovreview on national cyber strategies, see: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

[72] http://cybersecuritychallenge.org.uk/about-us/

[73] http://www.e-skills.com/news-and-events/march-2014/employers-create-specialist-cyber-security-apprenticeships/

[74] http://cybersecuritymonth.eu/ecsm-countries/germany

[75] https://www.check-and-secure.com/portcheck/_de/

[76] http://ec.europa.eu/enterprise/sectors/ict/e-skills/index_en.htm

[77] http://eskills-week.ec.europa.eu/about

[78] www.elig.org

[79] http://europa.eu/rapid/press-release_IP-13-859_en.htm

[80] http://www.computing.open.ac.uk/8025700300414AE8/httpNews?ReadForm&unid=FE3DFAE38A126C4B80257C400036C5CE

[81] http://www.eitictlabs.eu/innovation-areas/privacy-security-trust-in-information-society/

[82] http://cisr.nps.edu/cyberciege/

[83] http://www.akamai.com/html/about/press/releases/2014/press-072914.html

[84] http://blogs.wsj.com/venturecapital/2014/08/06/the-daily-startup-venture-funding-soars-for-cybersecurity-startups/

[85] http://www.ft.com/intl/cms/s/0/1acb22e0-f63b-11e3-a038-00144feabdc0.html#axzz3C4Zu4NuS

[86] http://blog.digital.telefonica.com/?press-release=eduardo-navarro-ec-innovation-convention

[87] http://ec.europa.eu/digital-agenda/en/open-innovation-strategy-and-policy-group

[88] http://www.eif.org/what_we_do/equity/venture/

[89] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/information-sharing-exchange/incentives-and-barriers-to-information-sharing

Imprint

LEGAL NOTICE

BY THE EUROPEAN COMMISSION DIRECTORATE GENERAL FOR COMMUNICATIONS NETWORKS, CONTENT AND TECHNOLOGY.

NEITHER THE EUROPEAN COMMISSION NOR ANY PERSON ACTING ON ITS BEHALF IS RESPONSIBLE FOR THE USE WHICH MIGHT BE MADE OF THE INFORMATION CONTAINED IN THE PRESENT PUBLICATION. THE EUROPEAN COMMISSION IS NOT RESPONSIBLE FOR THE EXTERNAL WEB SITES REFERRED TO IN THE PRESENT PUBLICATION.

THE VIEWS EXPRESSED IN THIS PUBLICATION ARE THOSE OF THE AUTHORS AND DO NOT NECESSARILY REFLECT THE OFFICIAL EUROPEAN COMMISSION'S VIEW ON THE SUBJECT.

YOU ARE FREE TO

NOTICES

DISCLAIMER

THIS REPORT REPRESENTS THE VIEWS OF THE AUTHOR, AND IS NOT THE OFFICIAL POSITION OF THE EUROPEAN COMMISSION SERVICES.

EDITED BY ELMAR HUSMANN UNTERNEHMENSBERATUNG
KINDLY SUPPORTED BY IBM
WWW.CYSPA.EU

THE CYSPA PROJECT HAS RECEIVED FUNDING FOR THE PREPARATION OF THIS PAPER FROM THE EUROPEAN UNION 7TH FRAMEWORK PROGRAMME UNDER GRANT AGREEMENT NUMBER: 318355

PHOTOS COVER ISTOCK, THINKSTOCK
DESIGN ASTRID GROBORSCH, WWW.NEODC.DE
1ST CIRCULATION NOVEMBER 2014

OUR MODERN SOCIETIES HAVE BECOME CRITICALLY DEPENDENT ON INFORMATION AND COMMUNICATION TECHNOLOGIES, ON NETWORKS, SERVICES, DIGITAL COMMUNICATION AND DATA. CYSPA IS A EUROPEAN INITIATIVE FOUNDED BY 17 PARTNERS FROM ACROSS INDUSTRY AND RESEARCH. CYSPA AIMS TO INCREASE THE SELF-PROTECTION CAPACITIES OF OUR DIGITAL SOCIETIES AND ECONOMIES AGAINST CYBER RISKS AND DISRUPTIONS. CYSPA PROVIDES CONCRETE SUPPORT AND EDUCATION TO USERS AS WELL AS ADVICE AND RECOMMENDATIONS TO EU AND NATIONAL AUTHORITIES.

WWW.CYSPA.EU