Strategic Research Agenda

WG3 Network and Information Security (NIS) Platform

Draft v02.80

Last modified: May 2015

Contents

1 Executive Summary

This document describes the Strategic Research Agenda (SRA) in the area of secure information and communication technologies (ICT). It is the result of more than a year's work by the Working Group on Secure ICT Research and Innovation of the Network and Information Security[1] (NIS) Platform that was launched by the European Commission in spring 2013.

This SRA complements and underpins the EU NIS Directive, and provides input to the secure ICT Research & Innovation agenda at national and EU level, including the Horizon 2020 programme. It is the main outcome of NIS WG3 on "Secure ICT research and innovation" and is intended to be a living document also referred to by other NIS WG (i.e. WG1 on risk management, and WG2 on information exchange). Other deliverables attached WG3 (i.e. Secure ICT Landscape, Snapshot of Education & Training landscape for workforce development and Business Cases and Innovation Paths.) were used as input to shape this SRA, each of them providing insights on relevant topics and so added value.

Cybersecurity is an important topic for each and every of us but also our organizations, societies and we all know now that we are not sufficiently protected against cyber attacks. This is even more true for our global economy where *risk alone undermines trust and confidence in the digital economy, reducing its potential value by as much as $3 trillion by 2020.*

The following vision guided the SRA's development.

Individual needs and fundamental rights should be placed at the very centre of how we design, manage and control network technologies and ICT. Networks and ICT should be designed to take into account, from the perspective of the individual, each of the following characteristics: diversity, control (e.g. user empowerment), privacy, fairness, democracy, freedom of expression and safety. The concept of individuality includes being able to 'individualise' according to people's differences. Individual rights (and duties), for example of ordinary people and consumers, must be respected, while transparency (without intrusiveness) must be provided at all times. The social, legal and regulatory aspects of security and privacy need to be investigated through interdisciplinary research.

Future digital technologies and the internet will become even more embedded in our lives than they are now. This will take us closer to a global digital civilisation that can bring benefits to all. Resilience is key for a functional digital civilisation. This civilisation must be empowered to manage and balance the risks it faces according to its own requirements, in the same way that physical civilisations do. Resilience also involves empowering people collectively to make decisions on trade-offs on security and privacy. Such trade-offs could concern privacy requirements, for instance, and be based on the preference of a group of people. Instead of working out their own preferences, many people will rather choose to trust those of a particular group. Protecting the collective interest of organised individuals, institutions and businesses in digital interconnected societies is hence crucial. This can be thought of as the 'supply side' of the digital civilisation.

Finally, as far as the vision is concerned, future infrastructure processes and resources will themselves be based on ICT infrastructures. They will be adaptive, decentralised, collaborative and efficiently controlled. Such infrastructures must be safe, reliable, predictable and always available. They must also operate confidentially, protecting privacy by resisting and reacting to cyber incidents in real time. Furthermore, users should have permanent access to information enabling them to check the trustworthiness of the infrastructure and its services (even if partly compromised).

---

[1] According to the European cybersecurity strategy published in 2013, network and information security, also referred to as cybersecurity, strives to preserve the availability and integrity of the networks, information and infrastructure and the confidentiality of the information they contain.

In this document, 'end user' refers to all those who use ICT with a view to making cyberspace more trustworthy in the context of existing legal frameworks. They include consumers, private individuals, industry, small and medium-sized enterprises (SMEs), law enforcers and national security agents. In this respect, the technologies envisaged in the SRA are aimed at delivering the vision set out above while preserving European values.

The result of empowering end users — from the individual, through SMEs, to the national security agencies — through technology will be a more trustworthy cyberspace. Legal frameworks will have to adapt and evolve together with new technology.

Thus, the SRA covers the whole Cybersecurity spectrum from different but complementary socio-technical perspectives. It is thus structured around 3 areas so-called Areas of Interest (AoI), with the titles of 'Citizen Digital Rights and Capabilities' (looking at cybersecurity from an individual perspective), Resilient Digital Civilization (taking a collective/societal perspective) and 'Trustworthy Hyper-connected Infrastructures' (looking at the secure and resilient infrastructure required to enable the other two perspectives). Each of these areas provides a Vision, a list of issues challenges, an inventory of (Technology, Policy, Regulatory) enablers vs inhibitors and ends with an analysis of the gaps where a number actions are recommended (as per nature of the gap) to fill in those gaps and so achieve the Vision (this may range from research action to standardization action going through regulation action).

In addition, to the recommended actions at individual level (i.e. AoI level), there are the recommended actions at collective level that this SRA stresses and which result from the cross-analysis performed of the 3 AoIs.

Indeed they highlight the shared and agreed areas where to put effort without neglecting other areas where to invest even if they remain specific to AoIs.

The current NIS SRA is driven by the conviction that research and innovation focusing on a combination of business, policy, education, societal and usage needs is the best long term strategy. Strategy's effectiveness in current layered model rely on a complete cross-analysis process over commonalities and divergences in order to take effective decisions on priorities for implementing a global competitiveness approach.

This will bring many benefits and stimulate the creation of value from NIS to reach the level that is needed to create jobs and prosperity in Europe at the same time effective resilience remains as a research priority driver to all member states.

Key specific areas either technical and non-technical have been identified as research and innovation priorities however it is noteworthy that the cross analysis has not reported blank areas or totally open fields.

The following common research and innovation priorities emerged:

Assurance. Effective security means that security, privacy and trust considerations should be involved from the very beginning in the design of systems and engineering processes. Engineering, assessment and certification processes as a dynamic, synchronized, complete and effective approach. This process of enabling assurance techniques and processes can be definitely eased by policy regulators. A growing area identified as enabler is cyber insurance. This growing business area needs further research on security metrics, security assessment as well as forensic and related technologies for establishing responsibilities in security incidents and attacks.

Data-centric and system-centric view integration. The ever-increasing amount, value and sensitiveness of data produced either by systems or individuals; need to be effective protected. With data being stored and processed in the cloud, and being exchanged and shared between many previously unknown and unpredictable entities, this protection cannot stop at a single system's border, but need to apply to the data over their full lifecycle, independent of which system is processing, accessing and controlling the data. Hence, a system-centric view, including, among others, secure devices and infrastructures needs to

be complemented with a data-centric view, focusing on data lifecycle aspects by providing mechanisms that allow the data owner to control the usage of their data as a prerequisite of a secure and privacy-preserving digital life.

Secure execution environment in untrusted platforms. As a matter of fact all ICT based instruments for gaining trust depend from a secure execution environment for the respective software. Any loss of integrity in these processes is an opportunity for manipulation and possibly corruption. With more and more information being processed outside of secured premises the need for secure execution environments and corresponding devices is rising. This holds for institutions in the public administration as well as for other critical infrastructures such as the health care sector, smart grids, and industrial control systems for water, food/agriculture, nuclear, and chemical operation. Secure execution environments are then even a critical factor for public safety and essential services provision.

Establish privacy enhancing technologies (PET) and digital identities. Cost effectiveness, interoperability, usability/simplicity, accreditation and mutual recognition of levels of assurance (LoA). As an example, the interoperability between "notified eID" and commercial internet-scale eID schemes is still an open issue partially tackled by groups such as Kantara, or OIX trust framework.

Trust management. While technology oriented communities often see security as a basis for trust, social-science oriented communities see trust as a something that is needed, when no security can be assured. This difference in the understanding of basic terminology leads to frequent misunderstandings on the role of trust and security. Indeed individuals need to be empowered to develop trust into digital services and/or apps for them to make informed decision. This calls for methodologies and tools to not only focus on Security and Privacy by design but also Trustworthiness by design. As an example,Trusted (Cloud) Services to be developed in any layer (IaaS, PaaS, SaaS) in order to reduce the consequences of the vulnerabilities at each layer.

Standardisation and interoperability. The exponential explosion trend and availability of new ICT products as well as the diversity of components, applications and services, created, integrated and deployed from anywhere in the world, may need an extra effort of standardisation if we want any end-user to trust cross-boundary interoperable and privacy guaranteed communications as an example. First, better political and regulatory support is needed for a cross-border effective approach, and secondly, an industrial transparency of hardware and software components and functionalities used may happen. There is a business opportunity for the European Industry to be the reference in privacy and security-by design to end users by the standardisation, the transparency and a stronger coordination and cohesion of stakeholders groups. It can drive a faster adoption of R&I results by the Industry as well as a proactive approach by policy makers which enable a more effective industrial policy avoiding societal mistakes before they happen.

Managing complexity of systems; risk assessment and management. New developments in ICT technology and its applications are increasing the complexity of systems and provide a challenge for management. The increase of complexity is caused by the amount of devices and components that are interconnected, the amount of data that is generated and processed, the number of people and objects that are interacting, the diversity of protection needs of individuals and organisations, the variety in attacker motivations and targets, and more. Clearly, the time taken for detection, diagnosis, remediation planning, and action is critical in limiting the impact of an attack. In the future, we can expect the sophistication and speed of execution of attacks to increase, and the difficulty of formulating a timely response to become correspondingly more challenging. A capability for autonomous response will become essential, because there will simply not be enough time to have a man in the loop. However, an inappropriate response may be more damaging than the original attack, so that the controls need not only to be speedy,

but also trustworthy. Despite the automation, people must remain in ultimate control, being able to set and modify policies that govern the actions of the autonomous agents. Establishing effective means of man-machine co-operation will be a research challenge in itself. Furthermore, network topology could morph dynamically to make itself more difficult to attack.

User–centricity. If privacy protection demands users to be in control of their data and systems and services to provide transparency about their data processing, users need to be able to express their preferences and to assess the risk that relates to the decisions they make related to their data. Users need to be empowered to manage their digital identities by defining their policies and preferences in an intuitive way. While many security and privacy relevant aspects of systems and services can be technically accessed, configured and maintained already today, such configuration and maintenance should not be manageable by technology experts only. With the increased penetration of ICT, everyone must be able to do so. How this can be achieved while at the same time technology gets more complex, remains a challenge. Meeting this challenge is a prerequisite to avoid a digital divide.

Education and awareness. As a main challenge, our future needs a reinvention of our education. It is not a matter of standard recycling but a real multidisciplinary, coordinated and coherent approach. The ICT has changed our lives and the way we understand the problems and how to address them effectively. We must teach the teachers in cybersecurity as never before. Awareness raising initiatives are more important than ever, by using new training models like MOOC (massive open online courses) we can expand the impact, but understanding the issue is far from effectively addressing it. It is not enough for top level management to simply understand the problem, at least they should react. The more proactive and multi-faceted European top managers we may have, the more business opportunities for European Industries. The cybersecurity often seen as a cost driver, may produce new business cases and innovation paths. The situation is changing continuously and it is clear that cybersecurity skills is more and more a requisite by employers in a multi-faceted approach (i.e law, industrial engineering and so on). As a challenge and opportunity, the better coordinated and coherent approach by all member states the better European situation for resilience and competitiveness we may experience. Today the educational programs are so fragmented, lead by specific mainly international companies for their own purposes, the knowledge is not shared as it should be and none of them address a dynamic up to date light weight process (aligned with the cybersecurity dynamic nature). There are lots of new disciplines and skills training opportunities as enablers, some examples are cybersecurity insurance, awareness in values (particularly among the youngest), user empowerment and control of personal big data, digital legal education, cybersecurity risks and practices, security engineering, agile security management and so on.

All AoIs put a strong emphasis on non-technical aspects of security and privacy, in particular, requiring a stronger role of organisations in the uptake of security and privacy enhancing technologies and of regulations to emphasise on European tradition and values. The debate on whether trustworthiness of ICT should be subject to market conditions and developments or seen as a societal responsibility needs to be conducted. This observation is understood as recommendation to continue and intensify multi-disciplinary research (technology, economy, society, and jurisdiction) in the field. Important aspects driving the related business aspects, including adoption, innovations, and market, need to be considered.

Since information and communication technology and business have faced major disruptions just recently, in many cases without considering security and privacy from the very beginning, it is not surprising that the majority of challenges and, hence, research priorities are driven by responses to those disruptions. Still, it seems to be worthwhile to look into future potential disruptions, taking into account that the speed of technology developments is not expected to decrease.

The SRA also reports on the analysis of the Cyber security market. If the market is estimated to record a steady growth (CAGR of 10.3%) it also reports on a number of challenges that also need to be addressed: lack of market knowledge, research into product transfer, lack of awareness of the offering, regulation and legislation not yet harmonized, and sensitivity for end-users.ICT is ubiquitous, critical and pervasive. While this document focuses on digital security, a secure and trustworthy cyberspace is also required in many other areas, from crisis management to urban security.

Stakeholders in one or more of the areas described may find insights for their own specific interests in the corresponding sections of this document.

2 Introduction

2.1 Context and motivation

This document presents the Strategic Research Agenda (SRA) in the area of cybersecurity, as developed by Working Group 3 (WG3), on Secure ICT Research and Innovation, of the EU Platform on Network and Information Security (NIS).

In 2013 the EU launched its cybersecurity strategy[2] to increase Member States' preparedness for possible cyber attacks capable of harming the EU and its economy. It is estimated that, worldwide, over a million people fall victim to cybercrime every day.[3] The global cost of cybercrime could have reached Euro 313 billion in 2011. According to a recent survey in Europe,[4] 75 % of the businesses contacted say cyber attacks have been a concern for some time or that they are an increasing concern. The majority of respondents believe that their organisation has been the victim of a targeted attack, with 30 % reporting a significant business impact.

In this document WG3 identifies the key challenges and desired outcomes in terms of innovation-focused, applied research as well as for cybersecurity. It proposes new ways to promote truly multidisciplinary research that fosters collaboration between researchers, industry and policymakers, and recognises the difficulties faced by some segments, such as SMEs in engaging with traditional research mechanisms.

Given the variety of the challenges and the diversity of the players involved in cybersecurity, privacy and trust research, WG3 also served as a facilitator for the coordination of related activities.

Beyond the scope of the Horizon 2020 research and innovation programme (H2020), WG3 should also help identify the elements of a possible European industrial strategy for cybersecurity. In addition it should look at ways to increase the impact and commercial uptake of research results in the area of secure ICT, including the use of innovative financial instruments and funding methods as well as new business models.

WG3 currently has more than 180 members. Its membership is balanced between industry representatives and scientific and academic researchers, on the one hand, and representatives of the Member States and stakeholders on the other.

The main objectives of WG3 are:

1. To map the current research landscape by identifying relevant stakeholder groups, national and EU research and innovation programmes in cybersecurity, trustworthy ICT and privacy, and prospective markets. This has resulted in two products:

   a. A comprehensive report on the state of the art in secure ICT and the research landscape

   b. An extensive report on business cases and innovation paths.

2. To produce an analysis of the higher education and training courses in cybersecurity available in Europe and beyond. produced report shall be released in summer 2015:

2

Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace /* JOIN/2013/01 final */

[3] http://europa.eu/rapid/press-release_IP-12-317_en.htm.

[4]http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-exercises/exercise-survey2012.

       a. A snapshot of the education and training landscape for workforce development.

3. To identify the possible scenarios for cybersecurity in the medium-to-long term (e.g. to 2020); to investigate the research, innovation, technological and educational challenges involved in addressing these scenarios successfully from technical, social and economic perspectives. This document represents the fourth product, i.e.

       b. The Strategic Research Agenda (SRA) of the NIS Platform. This contains input from the above reports. It is intended to be a dynamic document.

2.2 Methodology of the SRA

The findings in this document have been obtained in various ways. WG3 organised several expert meetings to structure its activities and prepare the main products in line with the objectives set out above. In particular, SRA brainstorming sessions were organised where WG3 members were asked to set out their visions of developments they hoped to see in the period to 202.

The initial material produced was processed and three main areas of interest (AoIs) emerged, with the following (tentative) titles:

1. Individuals' Digital Rights and Capabilities (Individual layer)

2. Resilient Digital Civilisation (Collective layer)

3. Trustworthy (Hyperconnected) Infrastructure (Infrastructure layer)

Three subgroups were formed to elaborate the AoIs. They were asked to address the following questions:

1. What is your vision for your AoI in the long term?

2. What are the main issues and challenges for your AoI?

3. Who are the enablers/inhibitors of the vision (from a technological, policy, organisational perspective)?

4. What research gaps need to be covered in the coming years?

In an initial phase, the three AoI groups worked in parallel to formulate their respective outcomes. Each group identified the main challenges and research gaps from its own perspective. The findings by AoI can be used in several ways by 'single-interest' stakeholders.

The initial drafts for each AoI were cross-analysed to identify common enablers/inhibitors/gaps across the different areas as well as possible conflicts (for example, an enabler for one AoI becoming an inhibitor for another).

It is recommended that the main findings of the cross-analysis are used to prioritise the research and innovation gaps to be covered on the basis, for instance, of the criterion of commonality.

The results of the subgroups' work and of the cross-analysis phase have been validated through open consultations within and outside WG3.

2.3 Structure of this document

The structure of this document reflects the methodology used. The three following sections describe the main findings for each AoI and answer the main questions raised above.

Section 6 describes the cross-analysis outcomes and presents the possible prioritisation of the research activities.

Section 7 considers a broader perspective that also takes policy, economic, social and educational aspects into account, since innovation is key for H2020. This section summarises the main outcomes of the other WG3 products, namely the report on business cases and innovation paths and the report about education and training. Overall it is recognised that enhancing cybersecurity is a complex process that concerns the EU on several levels, not just in technological terms.

Section 8 contains some concluding remarks.

It is also worth noting that this document is complemented by WG3's three other products.

2.4 Status of this document

This document should be considered a **draft** version provided by NIS-WG3 for wider consultation also outside NIS WG3 community.

3 Area of Interest 1: Individuals' Digital Rights and Capabilities (Individual layer)

3.1 Description of the AoI 1's vision

Information and Communication Technologies (ICT) and related services are coming ever closer to people under paradigms like mobility, ubiquity, and personalization [RAN13]. Related and partially overlapping paradigms are universal connectivity, thin client cloud computing and the Internet of Things. All these paradigms are triggering the creation of more and more data about users, e.g. movement and other behaviour profiles. People notice, that it is increasingly difficult to lead one's life without generating data of one or the other kind, often without exactly knowing, where the data are selected, stored and processed.

At the same times attacks by large state organisations on security and privacy protection of ICT services and infrastructures of all kind are discussed more openly, especially since the recent disclosures of international spying activities. For some experts the revelations were no news, but for many people the dangers of undetected tampering and manipulation of information are now becoming so obvious, that their trust into ICT infrastructures and their operators is massively reduced.

This lack of trust is not only an individual problem of the people not trusting ICT, ICT services or the respective providers. It is also not just a problem for the providers, who feel the lack of trust as a loss of customer acceptance and revenue. The problem is one for the democratic function of society. In several European countries, the fundamental right of "Informational Self-Determination" has been assured and it has been warned to beware of a "chilling effect" on citizens' participation in democratic processes: A person who is uncertain as to whether unusual behaviour is being taken note of, used, or transferred to others will attempt to avoid standing out through such behaviour. Persons who assume, for example, that attendance of an assembly or participation in a citizens' interest group will be officially recorded and that this could expose them to risks will possibly waive exercise of their corresponding fundamental rights. This would not only restrict the possibilities for personal development of those individuals but also be detrimental to the public good, as self-determination is an elementary prerequisite for the functioning of a free democratic society based on the freedom of action and participation of its citizens. These concepts are echoed by the Charter of Fundamental Rights of the European Union [EC00], especially its Articles 6, 8, 11, and 21 on liberty and security, protection of personal data, freedom of expression and information, and non-discrimination.

Civil security is not only to be an important pillar of these fundamental rights, it is also dependent on them. Individuals, who do not know, what is known about them, are easily prone to blackmailing by, e.g. organized crime to other forms of corruption. Only citizens with the courage to stand out if needed, e.g. to make a statement as part of a police investigation and to keep it up in court later, are a reliable partners in protecting the values and the security of their society.

Consequently AoI 1's vision is that individuals' needs and fundamental rights are placed at the very centre of how we design, manage, and control network and information and communications technologies. Networks and ICT should be designed to take into account each of the following from the perspective of the individual: diversity, control (e.g. user empowerment), privacy, fairness, democracy, freedom of expression, safety. The concept of individuality includes being able to 'individualise' according to the differences of people. Individual Rights (and duties) of e.g. citizens and consumers must be respected and transparency (without intrusiveness) must be provided at all times. Social, legal and regulatory aspects of security and privacy need to be investigated in an interdisciplinary research context. There is the need for thorough research addressing some fundamental weaknesses in current ICT architectures, e.g. the difficulties to control information flows. Also there is need for infrastructures that are resilient against overly swift actions from large

actors, which can be achieved by storing less data or by being distributed wisely. In any case, the subject of trust and the relation between trust and security needs to be researched more thoroughly.

3.2 Description of the issues and challenges

3.2.1 Technical challenges

Eight major technical challenges were identified. In the following, they will be discussed using the example of a smartphone device, as these devices tend to be the most popular devices to access the Internet:

1. **Interoperability issues**: Technical challenges consist at first glance mainly of interoperability issues. Therefore technical standards need to be improved, e.g. for the following two aims:

   a. **Proper protection of contactless (and at the same time seamless) communication by mobile phones:** For example Near Field Communication (NFC) is designed to enable users to seamlessly share content between digital devices, pay bills wirelessly, or even use their mobile phones as an electronic travel ticket via existing contactless infrastructures already in use for public transportation[5]. However only some of the underlying technologies are standardized, e.g. in ISO/IEC 14443 providing the physical layer for contactless communication over a very short range and in ISO/IEC 7816 providing the respective logical layer. So the implementations of NFC and RFID are in general not implemented in a fully compatible manner. Moreover there are more and more standardisation bodies active in the field: While RFID standards are coming from classic standardisation bodies, NFC standardization is performed in so called "industry for a" as the NFC forum. Consequently, the plethora of standardisation organisations and standards causes additional interoperability issues.

   b. **Proper protection of applications transferring data from one device to another device across boundaries:** Smartphones make it easy to load new applications "Apps"), which are then heavily used for data communications. The applications deployed there must guarantee privacy and integrity of the information they handle to protect the data of their users. Hence, their integrity and compliance needs to be protected.

2. **Protection of individual communication between citizens of different countries**: Besides the interoperability issues the individual communication between citizens of different countries needs to be protected. A smartphone user is exposed to various threats when they use their phone. Just in the last two quarters closing 2012, the number of unique mobile threats grew by 261%, according to ABI Research. These threats can disrupt the operation of the smartphone, and transmit or modify the user data. For these reasons, the applications deployed there must guarantee privacy and integrity of the information they handle. In addition, since some apps could themselves be malware, their functionality and activities should be limited (for example, restricting the apps from accessing location

---

[5] Bluetooth communication is another already well-used communication method between mobile phones. The significant advantage of NFC over Bluetooth is the shorter set-up time. Instead of performing manual configurations to identify Bluetooth devices, the connection between two NFC devices is established at once (under a 1/10 second). Due to its shorter range, NFC provides a higher degree of connectivity than Bluetooth and makes NFC suitable for crowded areas where correlating a signal with its transmitting physical device (and by extension, its user) might otherwise prove impossible. NFC can also work when one of the devices is not powered by a battery (e.g. on a phone that may be turned off, a contactless smart credit card, etc.).

information via GPS, blocking access to the user's address book, preventing the transmission of data on the network, sending SMS messages that are billed to the user, etc.).

3. **Scaling (up & down) of storage systems**. Scaling (up & down) of storage systems and how it relates to interoperability needs to be understood better. Scaling up a storage system in a mobile phone may imply the use of virtualization techniques, which are already e.g. used for ARM Platforms in the context of Android mobile phones. As well the storage system could be partly remote, e.g. by use of a cloud service. All of these scaling options have security and privacy implications that need to be analysed and addressed.

4. **User friendliness**: User friendliness (interoperable user interface) has to be an issue for standardization. This must also take into account accessibility requirements.

5. **Security and Privacy by default**: Assurance of security and privacy related properties should be accomplished by the system, so that the end user does not need to be aware and familiar with the protection measures. Smartphones are devices for data management; therefore, they may contain sensitive data like credit card numbers, authentication information, private information, activity logs (calendar, call logs as well as regarding availability. By attacking a smartphone, one can limit access to it and deprive the owner of the service.

6. **Avoid that users are spreading their identity all over the web, instead enable partial identities**: Users need to be able to separate their identities for different aspects of life into different partial identities (cf. ISO/IEC 24760). However, smartphones are highly customizable, so the device or its contents are often associated with a specific person. So users need to be able to split these custom profiles in a way, that keep their partial identities partial.

7. **Avoid the correlation of data so that individuals' data cannot be correlated or subsequently analysed** (avoid the Big Data problem). Correlation of data and subsequent analysis can lead to unwanted profiles and have a chilling effect on citizens exercising their democratic rights.

8. **Classification of security levels with a basic provable interoperable level for all communications devices**: There is a need for a classification of security levels with a basic provable interoperable level for all communications devices:

    a. For example, the EU (eIDAS) regulation on electronic identification and trust services for electronic transactions in the internal market from 2014 [EP14] defines (in Article 8 (2) of this regulation 3 security levels for eID tokens, namely low, substantial, and high. In Reasoning 16 these 3 levels are roughly mapped to the three highest levels of ISO/IEC 29115:2013 (namely medium, high, very high). It needs to be investigated whether one of these ISO/IEC 29115 levels could be the appropriate level for setting the basic security level for all communication devices or whether more analysis is needed to ensure mutual acceptance across all Member States. Moreover, the meeting of ISO/IEC JTC 1/SC 27/WG 5, which is responsible for ISO/IEC 29115, has started a Study Period to improve, among other issues, applicability.

    b. In addition, the evaluation level of assurance as defined in ISO/IEC 15408 could be used. This standard is published as well by the Common Criteria Project Sponsoring Organizations as "Common Criteria for Information Technology Security Evaluation".

3.2.2 Societal challenges

Four major societal challenges were identified:

1. **Digital divide/inclusion**: The digitalization of society moves forward at an ever increasing pace. With the rapid spread of digital communication, mobile devices, mobile internet and the Internet of Things, more and more services become possible and are integrated into our normal life. This concentration of (often very complex) technology increases the risk of a digital divide and the exclusion of parts of the society. While there has been significant progress in terms of user-friendliness of technology in recent years, many challenges remain, e.g.:

   a. **Usability and Manageability**: Technology that is relevant for ordinary individuals needs to be usable and manageable without a specialized education and needs to be accessible for people with disabilities as well. This also refers to information security since the level of achievable security should not depend on technical skills, educational background, or any impairments of a user.

   b. **Freedom to opt out of specific technologies**: Since it is part of the freedom of an individual to choose how intensively digital technologies will be used, there should always exist alternative, i.e. non-digital options for using modern services. As an example, filling out tax forms by hand and returning paper copies should still be available for citizens who prefer this. The state should not raise the burdens for citizens who want to communicate with the state in alternative ways. Individuals should have the freedom not to use all technology and still be able to live a normal, unrestricted life.

2. **User empowerment over personal data**: One of the fundamental assumptions of every modern privacy policy is the user-centric control over personal data. Users shall be enabled to decide if and how their personal data will be used for a specific service and they should be in control over the usage and spread of their data at any time. No processing of personal data should occur without the explicit user consent. This requires a very high level of transparency and includes the possibility for the user to opt-out at any time during a communication or transaction. While this principle is heavily propagated on a regulatory basis (e.g. the new EU privacy regulation proposal), the actual enforcement in everyday life remains a challenge. This includes issues concerning user awareness, transparency, cross-border enforcement (e.g. which jurisdiction applies for worldwide available services), the impact of search engines and Big Data technologies and the "right to be forgotten". In the context of Big Data technologies, the information content of metadata is one example where the principle of user-centric data control can be undermined significantly. User awareness is a fundamental prerequisite for enabling individuals to manage their personal data properly. While the use of many "free of cost" services seems attractive for the user, the actual value of personal data and possible consequences of their spread may not be transparent. This is partly due to missing personal and societal experience on personal data usage in the digital age as well as a missing educational background.

3. **Balance of "digital rights" vs. "classical rights":** With the new possibilities of digital technology the balancing, ranking and enforcement of individual rights has seen a dramatic transformation. Social networks, blogs, forums and other communication channels have put classical rights like freedom of speech and privacy into a new context. This leads to the need to balance these rights in a way that did not exist before. As an example, the "right to be forgotten" in the context of removing entries with personal data from a search engine has triggered an intensive discussion about a potential violation of the freedom of speech and the freedom of the media. As another example, the intensive discussion about intelligence service activities in the internet has revealed the need to balance individual rights, like privacy, against societal requirements like security. The same applies on a lower level for each individual digital service where a balance between anonymity on the one side and trust and security on the other side has to be found. Other rights, like the copyright, are harder to enforce in the digital context and require new security technologies to enable proper law enforcement without significantly limiting the usability of the services and the privacy of users. These balances are complicated further across a Union of 28 Member

States, where national legislation and even variations in the transposition of European Directives can cause discrepancies between the prioritisation of rights amongst nation states relying upon each others' mutual assistance in the preservation of rights.

4. **Establishing trust into electronic services**: Many classical transactions of the analogue age like handwritten signatures and cash payments have built up significant trust over a long period. On the other hand, their digital equivalents like electronic signatures or mobile payments still need to establish a comparable trust level in large parts of the society. This is due to missing long-term experience and lack of knowledge on the user side as well as due to the complexity and missing transparency of the technologies. Individuals need to be empowered to develop trust into these technologies and services and need to develop an awareness of their security.

3.2.3 Political and governance challenges

Four major political and governance challenges were identified:

1. **Preserve rights and societal values of the physical world in the digital world, where appropriate:** Rights and societal values of the physical world have shaped society since the beginning of civilisation. Some of these rights and values are difficult to protect in the digital world. Still they should not be removed or replaced in a merely accidental process, but be considered appropriately. Relevant issues are:

    a. Consider, that concepts like "ownership", "means of production", and "copyright" may be different in the digital world compared to the physical world.

    b. Understand the potential effect on digital rights.

    c. Consider the impacts of public goods, creative commons, open source, and crowd sourcing.

2. **Trust in governance of surveillance systems:** Surveillance systems are not trusted by European citizens, as it is unclear, what purposes they really serve and where the data are delivered. As a minimum the two following changes are to be met, if one wants to gain more trust:

    a. Personal data and information will not be captured/analysed without the knowledge and consent of lawful citizens;

    b. Technology, that is inherently able to perform permanent surveillance (such as computers and networks with storage capabilities including Internet, pervasive computing, mobiles, apps, sensors and CCTV) is to be built in a way, that it helps people and does not harm people.

3. **Concentration of strategic ICT resources outside of Europe**: In many fields of ICT (e.g. operating systems, encryption schemes, production of chips, operation of mail servers) major resources are concentrated outside of Europe. The challenges are to regain or maintain European influence in these areas to avoid, that the European ICT infrastructure is dependent from building blocks, Europe cannot influence.

4. **Need for agile policy making based on flexible and harmonized governance structures:** Policy making must take into account the fast pace of change of ICT based solutions and applications. Deployment of ICT solutions often causes societal problems that are not anticipated and when they are addressed, it is often too late to really fix the problem. For instance, it is well known that IP addresses cause privacy issues but it is also known that it is virtually impossible to fix this. Another issue is harmonization between policy makers when their jurisdictions cover ICT infrastructures only partially.

3.2.4 Educational challenges

Three major educational challenges were identified:

1. **Education on privacy and associated issues adapted to stakeholders:** Stakeholders dealing with ICT must understand the associated privacy issues, e.g. kids that use smart phones and social networks must understand what is at stake, policy makers must understand privacy issues, and associated ICT measures, ICT designers must understand privacy-by-design. We are in a situation where we must teach the teachers, i.e. school teachers must be educated, policy making professors must be educated, ICT teachers must be educated.

2. **Responsibility for continuous education and raising awareness campaigns:** Continuous education and raising awareness campaigns seem to be of major importance, as ICT and its applications are changing so quickly. It is however unclear, who can take responsibility for these activities and would have the resources needed.

3. **Bringing Massively Open Online Courses (MOOCs) to the same level as real-life in-class courses:** MOOCs are often seen as a chance to improve the level of education, especially in educationally disadvantaged areas, where not much education is provided. However, building the necessary trust and learning about trust issues is not trivial if communication only takes place in a mediated form. Therefore bringing Massively Open Online Courses (MOOCs) to the same level as real-life in-class courses is a challenge from quality and certification perspectives.

3.3 Identification of Technology, Policy and Regulation enablers / inhibitors

3.3.1 Enablers (Technology, Policy, and Regulation)

3.3.1.1 Public authorities and regulation

Four different types of enablers related to public authorities and regulation were identified:

1. ISPs, public authorities, and the Internet

2. Transparency, clear regulation, enforcement

3. Awareness on values, particularly among the youngest generation

4. Encouragement of privacy/security by design (via the typical "toolbox": prescription, financial support, public procurement etc.)

3.3.1.2 Technologies for privacy and security

1. Policy-based technologies for improving compliance with the respective policies (e.g. policies demanding the appropriate use of encryption techniques):

   a. Built-in security, privacy & safety where possible;

   b. Tools for analysing the degree of compliance;

c. Methodologies for refining policy-based requirements, in case the technological development demands such a refinement;

d. Scalable security levels or flexible security profiles of the respective technology to allow options for policy-makers and to enable policy-based decisions.

2. Personal Identity Management

a. Avoid, that users are spreading their identity data all over the web;

b. Partial Identities appropriate for the respective context and not giving more identity data (attributes) to the respective Relying Party than needed (e.g. not giving away the data of birth, when only assurance is needed that a user has reached the legal age);

c. Derived credentials (Privacy-ABCs), so that users can (re)calculate the credentials they need by themselves based on the basic credentials they received from their identity service providers (to reduce the dependence from identity service providers).

3. Data usage control, that enables individuals to control the use of "their" data

a. Sticky Policies (policies that accompany data sets, when they are transferred from one data processor to another data processor) to enable users to define which use of data they allow and to enforce this even beyond the boundaries of one data processor.

b. Technologies to disable the correlation of data and ensure, that individuals' data cannot be correlated or subsequently analysed via e.g. Big Data mechanisms.

4. Technologies, that reduce the chances and the impact of users giving up their privacy involuntarily

a. Privacy by default so that the end user does not need to be aware and familiar with the security measures but that the sys-tem ensures privacy related properties;

b. Tangible security technologies secured by e.g. hardware protection, that people can easily recognize and understand (like classic home keys);

c. Protected messaging, e.g. an easy-to-use system, that enables sending email and similar message without the risk to be tapped.

5. Methodologies and tools to enable Privacy/Security by design

a. Tools to explain the trade-offs and privacy impacts of demands to achieve some security goals (e.g. access control), that contribute of privacy impact assessment documentation;

b. Tools to enforce the principle of minimum-privilege, e.g. need-to-know;

c. Tools for accountability and auditability.

6. Downscaling-engineering of existing systems

a. Tools and Methods to reduce complexity

b. Reduces the probability of errors and undetected system weaknesses

c. Makes evaluations easier

7. End-to-end trustworthy networks, products, and services or apps

3.3.1.3 Standardisation and evaluation

Three different types of enablers related to standardisation and evaluation were identified:

1. Good standards & common norms as the basis for development:

    a. Improving standard services to improve the security level of online services e.g. in banking or retail;

    b. Defining a basic security level, that can be proven and is interoperable for all communications devices;

    c. Promoting privacy, security, and trust through standards & government procurement;

    d. Making standardization a more participatory and transparent process where individuals' concerns and priorities can be included in addition to companies' and governments' preferences.

2. Ease evaluation by downscaling-engineering of existing systems to reduce complexity.

3. Ecosystem for products and services (including online services) to enable effective feedback loops on the quality of the respective products and services.

3.3.2 Inhibitors (Technology, Policy and Regulation)

3.3.2.1 Public authorities and regulation

Nine different types of inhibitors related to public authorities and regulation were identified:

1. Lack of incentives for companies

2. Lack of regulatory framework to support ecosystem

3. Lack of regulation and enforcement

4. National Regulatory conflicts between preservation of privacy and requirement to report

5. Intra-jurisdictional regulatory conflicts between Member State interpretations of rights

6. Surveillance by governments may lead to surveillance by design rather than * by design

7. Profitability of violating security & privacy (market failure because of wrong incentives)

8. Identity economics not respecting the rights of the identity holders

9. Cost benefits analysis, expectation for free

3.3.2.2 Technologies for privacy and security

Four different types of inhibitors related to technologies for privacy and security were identified:

1. Complexity of systems (TLS/https works in principle, but is difficult to understand for non-expert individuals, and difficult to implement and test even for experts)

2. Complexity of individual security

3. Lack of social aspect in computer security. As a general point, lack of multi-disciplinary practice.

4. Data usage control: it is not clear which data are collected by whom without transparency, accountability, responsibility.

3.3.2.3 Standardisation and Evaluation

Three different types of inhibitors related to technologies for privacy and security were identified:

1. Lack of awareness, political support for cross boarder interoperability

2. Standard chaos, need of EU crypto standards: One issue is the lack of pre-standards, or specifications that are not yet fully standardized but already benefit from some consensus within a community. For instance, a new Privacy Enhancing Technology (PET) that is still at a proof-of-concept level could be pre-standards that would be used by a wider community of research projects.

3. No transparency of functionalities.

3.4 Gap analysis (tech., policy, regulation, and competences) for achieving the vision

3.4.1 Technical, security, standardisation gaps

Eight technical, security, and standardisation gaps were derived from the analysis of the challenges, enablers and inhibitors. They are discussed in the following subsections.

3.4.1.1 Gap 1: Secure computing in untrusted platforms

Given the many legacy systems in wide use today one technology gap is the aim for secure computing in untrusted platforms. This gap is discussed using the example of mobile phones and possible enhancements of those phones. The rationale for this example is that as mobile phones have to be considered insecure, but are important and wide-spread platforms for individual users for accessing the Internet and even for organizing their lives. Four specific aspects need consideration:

1. Availability of seamless connectivity. Connectivity needs to be guaranteed between all the different types of NFC Devices, e.g. smartcard (ISO/IEC 14443) and smartphone (NFC Forum), as the NFC forum only worked with simplified versions of ISO/IEC 14443, which cannot support the transmission of more complex data structures, like certificates. Some only specific smartphones happen to be able to support ISO/IEC 14443 in full; others cannot transmit more complex data structures such as certificates. So for many NFC phones there is no chance, that they can be equivalent partners to smart cards and can e.g. be used as fully functional readers for smart cards. So official test specifications (like in the passport scenarios) are needed to operate the (more demanding) security protocols over the NFC interfaces and to check, whether certificates and other more complex data structures are really transmitted.

2. Research and standardization of the appropriate basic security levels for communication devices used for serious transactions, e.g. mobile phones used as devices for identity management. Given the global nature of this problem a possible platform would be the ISO/IEC JTC 1 Subcommittees 17 and 27 on smartcards and Security or a joint project of both.

3. Availability of a trusted user interface for all mobile phones by a standardized Trusted Execution Environment (TEE) API for loading trusted applets providing a

    a. Trusted key pad and a trusted display to be assured by the TEE (to be used by all applets on a mobile phone using the TEE);

    b. Stable available NFC / contactless interface between mobile phone and Secure Elements (SEs), which may benefit from the trusted display and keypad, see ISO/IEC DIS 18328-2 (ICC-managed devices);

    c. Generally available interface from the TEE to embedded SEs in the mobile phone, e.g. by OpenMobile API, e.g. to secure Private keys PINs.

4. Provision and availability of a third party of trust in the secure services ecosystem, e.g. a Trusted Service Manager (TSM) according to GlobalPlatform. The main role for the TSM is thereby to manage and administrate over the air the different secure elements and trusted services within a mobile device. The role may need expansion and complement by a trustworthy ecosystem of operators of Software ("App") markets, so that users get better information on the properties of the Apps they are downloading.

3.4.1.2 Gap 2: Provision of a secure personal device based on a secure core

This section discusses an alternative provision to the approach of secure computing in untrusted platforms that was discussed as Gap 1. Secure personal devices based on a secure core are to function as a reliable root of trust under control of the individual. They need to provide two main functionalities:

1. Sufficient usability for citizens and services using them;

2. Separate interfaces to run more or less secure applications on them.

Three main technology approaches can be used to fill this gap:

1. Trustworthy mobile platforms and app-ecosystems: Smartphones could be a great platform for credentials and other personal assets, but their operating systems and applications have so many security and privacy weaknesses, that many users don't dare to consider them trustworthy (in the first sense), even though they use them. For these mobile platforms, more research is needed to enable technologies and architectures that European democratic governments can understand well enough to give a realistic assessment whether their citizen's data and cyber activities are protected appropriately. An approach to overcome the app-side of the problem (e.g. apps that leak their users' personal data to their developers or elsewhere) is to enhance the app ecosystem (e.g. the app-markets). App markets are to provide useful privacy information about individual apps in all the phases of apps' life cycle, but especially during app discovery, installation, and usage. Crowdsourcing may be used to protect against privacy-invasiveness of apps by influencing the rankings in (alternative) app-markets.

2. Strong sovereign assurance tokens and wallets: Assurance tokens (e.g. authorisation certificates) tend to contain more and more sensitive information, e.g. birth dates or authorizations for specific services or activities. Therefore they need special protection against undue transmission and exploitation. This protection can be provided either directly or via digital wallets. Examples are advanced smart cards or mobile devices with trustworthy secure elements that enable their holder to influence the character and degree of identification and the type of identification information. These devices are also to enable meaningful communication between the assurance token holder and the assurance token. Last but not least, assurance tokens and wallets must be able to protect themselves. For

example, they need to be able to verify their respective controllers (readers) by e.g. an extra communication channel. Therefore, a portfolio of communication mechanisms is needed, also to provide some redundancy. Moreover an independent clock, a sufficiently powerful access control mechanism to protect relevant data, and enough processing power for complex (crypto) operations are needed.

3. Trustworthy engineering processes: Trustworthy engineering processes can evidence (transparently) the trustworthiness of a platform, e.g. by showing, who takes responsibility for which part of the system. The evidence could then also be used to monitor trustworthiness at runtime.

3.4.1.3 Gap 3: Sufficiently advanced security and privacy enablers

Security and privacy enablers are not yet advanced sufficiently. They often lack user friendliness and are not well enough integrated into the respective work flows, so often security and privacy mechanisms stand in the way of people trying to do their work.

This advancement is needed for all enablers listed above, but especially for those where users need to make decisions, e.g. on personal identity management and use of personal data.

3.4.1.4 Gap 4: Mitigating privacy risks from involuntary user actions

To mitigate privacy risks from involuntary user actions one needs technologies that reduce the chances and the impact of users giving up their privacy involuntarily. The most important approaches are the following three:

1. Privacy by default so that the end user does not need to be aware and familiar with the security measures but that the system ensures privacy related properties;

2. Tangible security technologies secured by e.g. hardware protection, that people can easily recognize and understand (like the can understand e.g. classic keys home);

3. Protected messaging, e.g. an easy-to-use system, that enables sending email and similar messages without the risk to be tapped.

3.4.1.5 Gap 5: Policy-based technologies for improving policy compliance

Improving compliance with the policies is still an open issue. A typical policy that is often hard to comply with is the demand for the appropriate use of encryption techniques. The following approaches were identified to help the issue and deserve further research:

1. Built-in security, privacy & safety where possible;

2. Tools for analysing the degree of compliance;

3. Methodologies for refining policy-based requirements, in case the technological development demands such a refinement;

4. Scalable security levels or flexible security profiles of the respective technology to allow options for policy-makers and to enable policy-based decisions.

3.4.1.6 Gap 6: Downscaling-engineering of existing systems

Reducing the complexity of running systems is often the only practical way to address security issues in grown (legacy) systems that are too complex to be fully understood. In these cases, reducing the complexity means reducing the probability of errors and undetected system weaknesses but also makes evaluations easier. It is important to address the following issues:

1. How to provide a suitable abstraction specification which takes into account transversal concerns (resilience, privacy …)?

2. How to provide viewpoints that are adapted to various types of stakeholders (e.g. legal viewpoint, social viewpoint, policy making viewpoint, business viewpoint, engineering viewpoint, forensic viewpoints…)?

3.4.1.7 Gap 7: Good standards & common norms as the basis for development

Four examples for missing good standards & common norms as the basis for development are the following:

1. Improving standard services to improve the security level of online services e.g. in banking or retail;

2. Defining a basic security level, that can be proven and is interoperable for all communications devices;

3. Promoting privacy and security through standards & government procurement;

4. Making standardization a more participatory and transparent process where individuals' concerns and priorities can be included in addition to companies' and governments' preferences.

More agile management of standards is also needed to match TRL (Technology Readiness Level) needs. Pre-standards are needed in pre-deployment which later need to mature into standards.

3.4.1.8 Gap 8 Research on trust related terminology in different disciplines

While technology oriented communities often see security as a basis for trust, social-science oriented communities see trust as a something that is needed, when no security can be assured. This difference in the understanding of basic terminology leads to frequent misunderstandings on the role of trust and security. Therefore more research on terms like "trust" and "trustworthiness" and their meaning and relation in different disciplines is needed, e.g. to create more mutual understanding. It should be documented in a way that stakeholders can easily access the result. This gap corresponds to Gap 7 in the Section "Technical, security, standardisation gaps".

3.4.2 Social, political, and governance gaps

From the analysis of the challenges, enablers, and inhibitors seven social, political and governance gaps were derived. They are listed below.

1. Align regulatory and technological developments;

2. Demand and support user friendliness of technical and IT security interfaces;

3. Provide privacy (e.g. message confidentiality) in a heavily controlled world;

4. Control of surveillance;

5. Assurance in the digital world: we currently have car/house insurance and need the respective assurance, e.g. services providing an embedded level of security via insurance;

6. Public support for open source technology production and evaluation tools;

7. Research on the terms "trustworthiness", "trust" and their meaning and relation in different disciplines: This gap corresponds to Gap 8 in the Section "Technical, security, standardisation gaps".

4 Area of Interest 2: Resilient Digital Civilisation (collective layer)

4.1 Description of the AoI2's vision

"The future will be the same, the future will be different."

Virtually without exception, predictions of future society, economy, and individual life stress that digital technologies and the Internet will become even more embedded in our lives than they are now. There is a broad consensus that another ten years of investment, research, development, innovation, and adoption will move us closer to a worldwide, global digital civilization that can bring positive benefits to all.

Four technological macro-trends underlie the next ten years of evolution of the internet:

1. Everyone is connected – most people in the world will be connected to the internet and no society, no country, no individual will be unaffected[6];

2. The explosion of data – *The amount of* data *being produced will grow 10 times over the next six years, reaching 44 trillion gigabytes of data by 2020* [TIM14] that can be stored and analysed to give unprecedented insights at macro and micro scale enabling us to understand and predict global trends and markets and individual behaviours and responses;

3. According to many sources, electronics will be embedded in everything enabling us to monitor and control every aspect of our world, blending both the physical and digital worlds in an unimaginable way[7];

4. The Internet of Things (IoT) becomes mainstream[8] – the network effects that drove adoption of internet by people and businesses now apply.

Predicting the consequences of the relentless march of digital technologies is notoriously difficult. The Huffington Post[9], reporting on the Pew Research Centre's report on Digital Life in 2025[10] noted that "Predicting the future of technology is a fool's errand. But that certainly hasn't stopped us from doing it". We know our future is a digital future. We know that our civilisation will be a digital civilisation.

The pervasiveness of information and communication technology and ubiquity of digital infrastructures means that the Digital civilization is now a fact of Life. Some examples illustrate this: digital Media, digital social relations, critical infrastructures, services, surveillance, industrial control, government, intelligent transport systems, and smart cities, amongst others.

A 'Digital Interconnected society' approach focusses on the Institutions of society, i.e. the organisations that make up our government, business, and civil society, which increasingly rely on digital technologies to operate, offer services, and interact with citizens, with customers and with each other. We look at "interconnected society" because as these organisations use, and are changed by, digital technologies, it raises many challenges, issues and risks.

---

[6] http://www.microsoft.com/security/cybersecurity/cyberspace2025/

[7] http://www.economist.com/blogs/babbage/2014/05/difference-engine-1?_ga=1.187028200.1734560282.1412612630

[8] http://www.pewinternet.org/2014/05/14/internet-of-things/

[9] http://www.huffingtonpost.com/2014/03/11/heres-what-the-internet-c_n_4943051.html

[10] http://www.pewresearch.org/

The 'Digital Interconnected society' theme aims to identify the challenges, issues and risks that organisations face in a digital 'interconnected society' and to identify the technologies and approaches to ensure that they can be trusted, secure, and can meet the obligations imposed on them by society, whilst at the same time benefiting from innovative technology and services.

All this takes place against a backdrop of continuous and rapid change at scale and with depth never before encountered, crossing geographic, cultural and digital borders.

Increasingly interconnected: there are more connected people; an increasingly interconnected business and organisations; greater use of online services and cloud in complex supply chains; and more and more connected devices.

New and innovative services including social networks (some of which are global in scale, others contained within countries or regions), the internet of things which introduces new services that can manage and control the physical world, and more generally the expanding use of ICT to manage more of our lives and controls more systems and infrastructures.

More and more data from increasingly pervasive sensors, cameras creating vast amounts of data being used for all kinds of services combined with much more powerful data analysis that with the power to de-anonymise ever larger datasets.

A Digital Civilisation is desirable to society due to a number of key drivers such as: ease, convenience, economisation, speed, information access, optimization, proximity, and others. However, the Digital Civilisation is exposed to new risks and threats as the vulnerabilities and exposure of the digital interconnected society to this digital infrastructure, which is continuous evolving, can have issues related to accessibility, invisibility, profiling, connectivity, complexity, and others. Coupled with the trust issues arising from a constant concern of surveillance and/or potential loss of personal data could eventually diminish the digital infrastructure's image, and consequently change the future architecture of the infrastructure by necessity of barriers, filters and inspections at all stages of usage and operation. Moreover, an architecture based on shared platforms and infrastructures increase the impact of incidents on civilization.

Resilience is key for a functional digital civilization, and civilization must be empowered to manage and balance their own risks according to their requirements, similar to how it is done in the physical form of civilization. These concepts and solutions must also be addressed in a fashion that is not localized in pockets, but can it translate to a "world scale" taking into account the different aspects of civilization as it will be in 2025.

Resilience also implies that people will need to be empowered collectively to make decisions on trade-offs regarding security and privacy. Such trade-offs could be on privacy requirements e.g. the preference of a group of people. Instead of working out individual preferences, many citizens will rather choose to trust the preferences of a group of citizens.

The focus of this **AoI Resilient Digital Civilisation (collective layer)** is the protection of the groups/society/organizations (we will call this 'Digital Interconnected society') as it represents the collective interest of the organized citizens, institutions, business, etc. This can be thought of as the 'supply side' of the digital civilisation.

These groups and organisations operate under a whole series of obligations – regulation, contracts, societal norms, and to manage risks, ensure security, and handle information securely and respecting fundamental rights of the customers/citizens.

The AoI 2 will focus on ensuring that digital institutions of society will be trusted and secure, as trusted in their digital forms as they would be in physical form. If indeed it would be possible to translate the digital institutions of 2025 back to what they were 15 or 25 years previously, such is the nature and scale of the transformation to a Digital Interconnected Society.

4.2 Description of the issues and challenges

4.2.1 Technical challenges:

To achieve the goal of a society in which the institutions are trusted in their digital form, means first to achieve the basic resilience and security of their ICT systems:

1. **Security and Resilience of the Cloud**: As we go forward, the Cloud is becoming the dominant form of ICT consumption – whether as Infrastructures, Platforms or Software as a Service, the Cloud will be the way in which customers both private and public consume new ICT. Ensuring cloud services are secure and resilient is in itself a significant challenge given the complexity, scale and interconnectedness of cloud ecosystems. This means having security metrics and a maturity model, employing security by design across the entire ecosystem, and for resilience, ensuring interoperability and adaptability of systems at all levels.

2. **Cyber crime/Cyber terrorism prevention**. Confidence in digital institutions depends on our ability to prevent the bad people doing harm to individuals or institutions to societies at large – potentially at a scale not even faced before. There are numerous technical challenges here, for example how to balance surveillance and fundamental rights (surveillance in a privacy protecting, transparent, and responsible way), to prevent any data and information leakage to cyber-criminals, and the ability to detect and bring them to account.

3. **Trust Management in the Digital Society**. Assurance and accountability will become competitive advantages for services in a future digital society. Is it possible to move beyond self-certifications towards metrics for trust and accountability, and ways to validate assurances and certifications automatically?

4. **Privacy in the Digital Society:** as information held and controlled in the cloud by organisations public and private becomes ever more comprehensive, the challenge of implementing Privacy by Design (and by Privacy by Default) becomes more difficult. The PRIPARE project[11] identified the following sub-challenges; generic integration in the many domain specific engineering design practice; multi-disciplinarity of the design practice; customisation techniques to take into account specific legal and socio-political parameters. The deployment of Privacy Enhancing Technologies continues to be problematic and the introduction of transparency and accountability techniques become important (who is using what data and when – refer to A4Cloud project[12]).

5. **Digital identities** remains a challenge for a heterogeneous and decentralized digital society, including the development of Global/interoperable ID systems, perhaps involving biometrics technologies that are at the same time privacy preserving and based on minimum disclosure principles, enabling and / empowering civilization to be based 'globally' and still empowered to carry out their local duties e.g. e-voting from abroad.

6. **Risk management** for the digital world is still a challenge for digital societies. As we go to ever large scale interconnected systems, and the development of new risk management models and systems for cyber societies is necessary.

7. **Social networks security and privacy** becomes challenging as social networks become embedded in the fabric of society and even become instruments of democracy. Cultural

---

[11] http://www.pripare.eu/
[12] http://www.a4cloud.eu/

norms change more slowly than technology. How do we protect citizen's security and privacy when the technology that exploits social networks is advancing so rapidly?

8. **Big data analytics.** Lastly, the technical challenges to manage and control what can be understood about us from the vast pools of data available when the whole world is profiled are immensely challenging. Is it possible to manage what can be inferred from data gathered in the course of our daily lives? What happens if this spreads into the political sphere?

4.2.2 Political / Societal challenges:

Policy & Regulation faces a number of challenges to put the appropriate laws and governance around the new style of information technology.

1. Typical policy and regulation processes take years if not decades, whereas the process must have a flexibility and agility that matches the fast pace of evolving digital civilization. Digital civilization should ensure a digital interconnected society that is fair, democratic, safe, and transparent, avoid censorship, and maintain a balance the citizen rights and duties.

2. Control - individual vs. collective – to ensure that individuals can manage their individual digital presence in a way that's balanced with collective needs form business, state, society, community. The values and rights of human societies should be reflected in the digital world. The challenge is for organisations, public and private, to operate in a way that implements the vision outlined in section 3, Individuals digital rights and capabilities.

3. Empowerment of groups of citizens and the exercise of political and economic power online may be transversal to country policies and governance. In some circumstances, this may be a strong barrier to the advent of such empowerment. Certainly, there will be differences across the globe between nations and cultures.

4. Allow (digital) diversity - not treating everyone the same, enabling differences, supporting the different cultures, approaches perspectives online. Still we should avoid discrimination based on different digital abilities.

5. Security and trust in future digital societies can be supported through regulatory approaches that enable security certification as well as for approaches to insurance against cyber risks. Specific attention should be devoted to data protection principles.

6. In the pursuit of the above, addressing the international aspects of the digital civilization requires international cooperation amongst the global players, in which the European view should be fostered. Considerable groundwork has already been laid on aligning these international efforts in the EU DG CONNECT Framework Programme 7 projects, INCO-TRUST and BIC[13], but this work must have a mechanism to enable continued coordination of international efforts within H2020.

4.2.3 Economical:

1. The underlying economics of security and privacy are not well understood. ICT systems and ecosystems incredibly complex and risks are not well understood. Firms and public sector organisations invest in security without a clear model of what the return in that investment will be. Risk based approaches to security are problematic – the cost of a

---

[13] http://www.inco-trust.eu and http://www.bic-trust.eu/

vulnerability being exploited are not quantified which makes it difficult for organisations to focus on high-risk vulnerabilities – they have to focus on everything.

2. Secondly, organisations are reluctant to share information amongst themselves regarding security vulnerabilities and incidents that would be of benefit to all parties out of concern that this will expose them to further attacks, reputational damage, or other disadvantage with respect to their competitors. Identifying the incentives and striking the right balance between cooperative and regulatory approaches to information sharing regarding incidents and vulnerabilities presents a challenge and there is a need for tools and techniques that facilitate and encourage information sharing addressing confidentiality, security and respecting data protection. This topic supports the activities of NIS WG2 which is addressing information sharing

3. Finally, there is great disparity in the ability of organisations to invest in securing their ICT systems. Large organisations may have the capacity to employ full time security professionals - SMEs rarely have that luxury. This is in some extent mitigated by the shift to cloud computing in which companies have no need to run their own computing infrastructures but instead rely on large cloud computing services providers that will have the resources and expertise to provide better security.

4.2.4 Educational:

1. One key challenge in increasing cyber security is to engage end-users in ensuring that they are secure online. Organisations may pick up the blame for breaches that involve poor password security by end-users, yet those same end users are reluctant to use more techniques that are effective. A better understanding of the risks and practices through bringing about greater public education in cyber security is a challenge.

2. In the digital civilization, new things have to be integrated in a matter of years (see for instance the advent of social network); raising the awareness of teachers is a major bottleneck. School teachers must learn before teaching kids. Law professors must learn before teaching law students. Engineering professors must learn before teaching students on privacy-by-design practice. The practice of cyber-security is multi-disciplinary which runs counter to the structure of most institutions.

4.3 Identification of Technology, Policy and Regulation enablers / inhibitors

4.3.1 Enablers (Technology, Policy and Regulation)

4.3.1.1 Technology

1. **Privacy Enhanced Technologies (PET)** should be available in a broad spectrum of products and services, with usable, friendly and accessible safeguards options: it is important that end users control their own privacy by having usable activation methods and robust crypto features in built-in services and widespread applications like for example the e-messaging systems. PET should be developed having also cost effective solutions. Comprehensive and consistent Privacy Risks Management Framework should be available, in order to allow people to understand their privacy exposure.

2. **Identity Management** solutions should be promoted by fostering flexible, robust, weakness free, certified, scalable (as of IoT) and specialized identity providers. End users should trust identity providers by having control about the level of security they get by each

provider. Easy password policies (e.g. date of birth for reset a password or similar simple questions), should not be an option anymore by default as it provides a trigger for identity fraud.

3. **Trusted** (Cloud) Services should be developed in any layer (IaaS, PaaS, SaaS) in order to reduce the consequences of the vulnerabilities at each layer. Technologies, processes and mechanisms that allow verifying regulatory compliance, data traceability, privacy, security and auditing accessible in order to avoid trust erosion along the time.

4. **Trust models** for the digital civilizations (Trust areas for the "cyber world"). Trust managements frameworks are often used in e-commerce and other on-line applications. Trusted e-services should be expanded and trust management engines should enable pervasive management of trust relationships for several purposes. Trust for social communities should be a main enabler.

5. **Dynamic Risk management** approaches should be developed by using methodologies and techniques to assess how secure an organization is, enabling different security options to be compared, as well as changes in the levels of security over time (which show the effectiveness of security measures). New techniques are also needed to enable more consistent and appropriate security decision making as well as allowing aggregation and composition of different pieces (Software and Hardware) without losing the control of risks as well including other factors like legal and economic aspects.

6. **Security certification** schemas and standards. It is of primary importance to have mechanisms to be able to certify the security and the correctness of the complex ICT services that Future Internet offers. Security is an inherently difficult problem. We need new certification technologies especially for complex systems that can evolve with the system evolution in order to avoid re-certification needs. These certification approaches and procedures should be made automatic as much as possible, including the simple automation of the data shared. In this ambit, there is a great need of mechanism for studying asserting and certifying the security of cloud infrastructures as well as of complex services built on top of those. The sharing of information, the trust among the involved stakeholders are also elements to be considered. All the certification should be standardized in order to maximize the impact of the results.

7. **Security engineering** is a main enabler to achieve *security and privacy by design*. In these areas, improvements in the security requirements languages and techniques are planned, and as well as new security, design and architecture principles should be investigated. Embedding properties as security, privacy and trust, compliance in the very early phases of system and services design is mandatory to increase trustworthiness of systems.

8. **Assurance** techniques are also necessary to ensure that the system is secure and being in the position to prove it to third parties (*provable security*). We can envision several aspects. Just to mention programming for verifiable security: The Future Internet will reinforce the prominence of highly distributed and concurrent applications, increasing the need for methodologies that prevent security holes that exploit the computational infrastructure. The objective is to develop a discipline of secure programming based on verifiable security, using program analyses and verification methods. We need to develop enforcement mechanisms that combine different verification methods and allow enforcing a wide range of policies (of information flow and resource usage). Automatizing proof techniques for cryptographic protocols is another challenging task, since cryptographic proofs are quite complex the automation of the verification process should be of interest.

9. **Quantitative aspects** for cyber security. Most of the cases, good enough security is exactly what one needs to ensure, i.e. that the security mechanisms are appropriate for the protection of the assets. This requires security mechanisms that *fit the purpose* and are able to allow security managers to trade-off between cost and risk. New *security metrics*

frameworks able to be easily computed should be envisaged. These security metrics could be merged with risk analysis methods to decide the appropriate security controls to be put in place. This is in relation to risk management aspects.

10. **Forensic** technologies able to cope with the new (digital) crimes/frauds. The society is relying on the ICT. These technologies are means for (cyber-) crime as well as witnesses of (cyber-) crime. In order to ensure the personal and societal security we need to ensure that the crime committed can be traced, and persecuted. Thus appropriate forensic methodologies are necessary. Those should consider that there are several stakeholders involved in the process of evidence acquisition. Forensic methods identified (in particular the proactive ones) should be however aware of privacy issues and considering the issues related to maximal control and minimal disclosure of private information (considering also post-incident mechanisms).

11. **Situation awareness** technologies. For ensuring the security of the society, we need situation assessment mechanisms able to cope with the enormous amount of data coming from several sources (including internet, mobile devices, social networks, vehicular networks) able to identify the trusted and usable information and then take proactive actions through proper actuators, including the usage of those media. Secure societies as secure communities will benefit such technologies. Managing crisis and emergency situations will also demand advanced simulation and training frameworks.

12. **Cryptography.** In a highly interconnected digital civilisation, cloud services are the dominant way to access and consume information technologies. Data will usually be stored and processed by other parties as cloud Infrastructures and software services. Stronger encryption, enhanced cryptographic techniques that enable encrypted processing and policy based decryption techniques are the only way to ensure that data remains opaque in transit, at rest, and during processing and accessible only those persons with legitimate access.

4.3.1.2 Policy

1. **State interventions (e.g. due to lawful exceptions) to access information must be clearly defined and understood by citizens and society.** In many cases, the capture of data and information between citizens and public administrations, governments, banks, etc. is potentially done without taking into proper account the consequences for the privacy of the citizens. As a result, the citizens in their digital lives are growing more uncomfortable. The lack of clear definitions, the complexity of the ICT challenges, and the lack of national and international coordination, means there is no solid response or common approach to data collection to fight cyber-crime and cyber terrorism. It is, therefore, necessary to tackle this issue to rebuild the trust and confidence of the citizens within the digital civilization by enabling the understanding of this currently very grey area of political and legal exceptions for data and information retention. The multi-disciplinary approach of H2020 can provide this enabler to address these issues.

2. **Regulations to foster economic/business /legal aspects of security / privacy and trust.** The rule of law is a fundamental principle of liberal democracies within the physical and digital society. It is a guarantee against arbitrariness and misuse of powers against the citizens within this society. Today, technological development offers many challenges to the rule of law, especially with regard to transparency and control. Lawmakers ought to pay more attention to the capability of ICT technology when regulating police methods in the digital realm, and developing corresponding control criteria. H2020 should, therefore, be used to enable interdisciplinary activities to combine ongoing legal and technological research to detect similarities and differences relevant to the design of legal rules pertaining to our digital society. The aim is to ensure that important aspects of the rule of

law are indeed upheld and the risk of arbitrariness is minimized in ordinary citizen's digital lives.

3. **Interest in regulations description, analysis, processing for increasing efficiency and compliance checking.** This is necessary enabler, as the Future Internet (FI) needs to maintain end-to-end security and privacy requirements in a very rapidly changing and dynamic environment. Boundaries between design and runtime will shrink, and there will be an increased need for real-time verification, monitoring and assurance to facilitate and ensure security properties such as confidentiality, integrity, and availability. The very traditional model for software development lifecycle (SDLC) will need to be revamped, as all stages of development will be impacted. Indeed, the complexity of FI services requires that security and dependability, up to now considered secondary aspects of system development, will need to be considered in the early stages of the system development life cycle SDLC, just as other functional and non-functional requirements [NIS14].

4. **Ensuring transparency.** Following a period of continual revelations regarding the systemic collection, aggregation, and potential analysis of personal data, concern amongst citizens is at an all-time high with regard to their privacy, use, potential misuse and control of their data. These concerns are also being echoed within the legal and technology research communities. At a number of recent conferences, discussions even emerged on an impending 'doom' or a slightly lesser 'disaster' over the future of our digital lives[14]. The dichotomy between the legal and political safeguards against the use/misuse of personal data needs to be examined as a matter of urgency. It will avoid the 'digital disaster', which could have significant implications on the innovation impact expected from Horizon 2020. Thus, the unique opportunity of the H2020 programme is to bring together the relevant stakeholders from the legal and technology communities across academia, industry and government.

5. **Industry participation/PPP.** Currently, in addition to the NIS PPP, there has long been a strong tradition towards the involvement of industry in the Trustworthy ICT field in the EU. Some examples are the Trust in the Digital Life Initiative (TDL)[15], which was formed by leading industry partners and knowledge institutes that hold trust and trustworthy services to be an essential ingredient of the digital economy. The ethos of TDL falls well within the AoI2: TDL is promoting an "ecosystem that protects data and assets of citizens and enterprises", that "enables affordable cyber security services for SMEs" and where "industry can provide innovative and trustworthy ICT products and solutions across Europe in a level-playing field"; The Digital Enlightenment Forum is another initiative with many industry participants coming together to advance the democratic rights of the citizens in the digital society. In addition, a number of projects have a strong industry backing, including the FP7 SecCord project that runs the annual CSP Forum[16] and the CYSPA project[17], whose objective is the creation of a European Alliance to protect cyberspace for industry. Of course, this list is not exhaustive. The important point is that a coordinated environment for industry participation and PPP must be continued in H2020, especially with the goal of fostering European expertise.

6. **Education.** Projects are already underway looking at the different approaches of how to overcome the education barrier in topics related to security and privacy. For example, the PRIPARE project[18] is looking at education from the perspective of bringing Privacy by Design towards research and industry. In H2020, the recommendations made by projects such as PRIPARE should be taken up as a matter of urgency.

---

[14] http://www.digitalenlightenment.org/

[15] http://www.trustindigitallife.eu/

[16] http://www.cspforum.eu/index.ph/

[17] http://www.cyspa.eu/

[18] http://www.pripare.eu/

4.3.2 Inhibitors (Technology, Policy and Regulation)

4.3.2.1 Technology

Technology inhibitors for an inclusive and trustworthy digital society

1. Intrusive monitoring technologies (i.e. the monitoring of information technologies by law enforcement) are necessary on the one hand for the detection and prevention of cybercrime and cyber terrorism, but are inhibitors on the other hand, leading to significant levels of mistrust and discomfort in the digital society. The lawful users must be included in the processes and procedures if their data and information is being collected for any reason, in order for them to maintain high levels of trust and confidence in the ICT systems they are using.

2. Pervasive sensing technologies (i.e. the ability of information technologies to gather information about the people and the physical world) is another area causing a conundrum of having a great potential to benefit the digital society at large, whilst at the same time causing significant concern amongst potential users of this new and expanding innovation, mainly due to doubts about the security, use and control of the stored data and information.

3. Vulnerable ICT infrastructures - as the Future Internet is becoming part of the Critical Information Infrastructure, having any sort of downtime on these infrastructures is becoming unacceptable to the digital society, and thus an inhibitor. AoI 3 covers this subject in detail.

4. The Digital Divide, a concept that society should not be separated into information haves and information have-nots, is of course an area that needs to be addressed in AoI2 with programmes (technology, policy, and education) to bridge any divide to ensure access to the Future Internet is done without disparity across the digital society.

4.3.2.2 Policy

1. **The lack of a common understanding of Cyber security** is an inhibitor. Governments have attained to build safe online environments through so-called cybersecurity policies. While cyber security comprises several aspects of ICT security in the online and offline world, internet safety is only part of the cyber security agenda. A civil society approach requires a shift in how cyber security is seen, moving from the national security sphere to become part of the public interest. Strategies and policies to secure internet should focus in realising society's wishes in keeping cyberspace open, free and prone to innovation. "As a society the culture of the Internet is much more about openness and experimentation than about safety and security," says academic Steven Weber in the Harvard Business Review. In fact, activists have considered the term security as anathema of a global civil society (Deibert, 2011) and demonstrated their lack of faith in the progressive securitisation of cyberspace (Comninos, 2013). They urge policy-makers to prioritise the security of individual users, civil society and organisations' networks, over excessive regulation and militarisation of the Internet (Comninos, 2013). This debate certainly calls for greater civil society participation and empowerment in the political decision-making, as the cyber security issue has been strategically kept away from society's influence. While some countries fight to keep the cybersecurity strategy control under national authority, reality has showed that despite the public good characteristic of cyber security, individual stakeholders make most information security decisions (Bauer & van Eeten, 2009). This decentralisation has led to sub-optimal security levels (Bauer & van Eeten, 2009), as it answers to the private interests of specific actors and has little regard for public interest.

2. **Market fragmentation** is especially an inhibition key factor for the supply side. The complexity of the interrelationships in networks as well as the complexity and immateriality

of many of the products and services provided by cyber- security and privacy firms, the lack of data and reporting requirements, as well as the existence of confidentiality requirements, hamper the analysis of the market. The cybersecurity market today faces four major challenges:

a. Research into product transfer: Europe has many outstanding research outcomes, yet they often fail to reach the market.

b. Awareness: Existing cybersecurity product sometimes does not reach the customer.

c. Regulation: Each country has specific regulation and legislation toward data and privacy this impacts the pan-European service and product offering. Regulations can encourage innovation (e.g. by creating a more open and dynamic market, or by mandating change), but there is also the danger that innovation may be stifled by regulations that effectively enshrine the *status quo*, make change too slow or risky, or create barriers to entry into the market. Regulators with conflicting remits may issue contradictory requirements, resulting in uncertainty.

d. Sensitivity for end-users: Citizens of Europe are particularly sensitive to cyber security, the impact the digital environment has on personal lives, accessibility and vulnerabilities is unique and thus the risk associated is difficult to measure and mitigate.

3. **Security seen as cost driver**. The reason for that is that security is not usually an investment that provides profit but loss prevention[19]. So what is the right amount an organization should invest in protecting information? In other terms, when you invest in security, you do not expect benefits; you expect to reduce the risks threatening your assets. The R&D projects often do not execute market studies for their technologies and do not consider costs to ensure acceptance of their technology. The business model says security must also be economically viable. Value-driven research might have dramatic implications for the R&D process, turning around how we think about "research to market" process, piloting and trials, placing the issue of "proof of value" at the start of research proposal. As such, value-driven development strategies need support and coordination that considers the ICT security solution/product value proposition, the evidence plan to support that value proposition, and the customer acceptance of that product and evidence when determining registration, price acceptability and market access. Understanding and managing trade-offs among these three components provides a cost, risk and return analysis that can inform research result progression and further investment decisions by individual industrial partners.

4. **Lack of awareness** at top-level management to enhance implementation plans by reducing organizational issues. It is widely acknowledged that there we are at a critical moment, perhaps even crisis, with regard to Network and Information Security, with improvements required in all areas. Traditional security models and controls are proving insufficient in the face of today's threats and trends in technology and usage, yet the way forward is far from clear. The following is an excerpt from an article from McKinsey&Co.:

"Why isn't more being done to protect critical information assets? Senior executives understand that the global economy is still not sufficiently protected against cyber-attacks, despite years of effort and annual spending of tens of billions of dollars. They understand that risk alone undermines trust and confidence in the digital economy, reducing its potential value by as much as $3 trillion by 2020. They understand most institutions have technology- and compliance-centric cybersecurity models that do not scale, limit innovation, and provide insufficient protection. And they understand that institutions need

---

[19]   http://www.enisa.europa.eu/activities/cert/other-work/introduction-to-return-on-security-investment/at_download/fullReport

to develop much more insight into the risks they face, implement differential protection for their most important assets, build security into broader IT environments, and leverage analytics to assess emerging threats, improve incident response, and enlist frontline users as stewards of important information."

5. The importance of cybersecurity is no secret to anyone who has opened a newspaper or attended a board meeting. So, senior executives may ask, what is the holdup? The answer is simple: understanding the issue is quite different from effectively addressing it. A number of structural and organizational issues complicate the process of implementing business-driven, risk-management-oriented cybersecurity operating models, and only sustained support from senior management can ensure progress and ultimately mitigate the risk of cyber-attacks.

6. **Complexity**. NIS solutions must be recognised as complex socio-technical systems consisting of many dissimilar elements that must work together harmoniously. Consequently they require a holistic approach. Currently, technical security measures are largely used independently, with people providing the matrix that integrates the components. In the future, the pace of response required means that the technical systems will need to co-operate directly. This has implications for the dynamics of innovation, as it is more difficult for a radically different approach to penetrate the market due to the need for a new product or service to be compatible with the existing elements with which it must interact. In addition to this, NIS is not a technology itself, but a mind-set and a collection of principles that must be applied in a technical and organisational/social context. The pace of innovation in technology and in the business practices, leisure activities and societal institutions that exploit it, means that NIS must re-invent itself continuously. It is straightforward to list current technical and process innovations that are problematic conventional security approaches (Cloud, Internet of Things, Mobility, etc.) and we can be sure that the years between now and 2025 will bring further challenges. The pace of change in technology, business practice and threats means that any static Cyber Defence Operations (CDO) suite would rapidly become outdated and ineffective. On the other hand, it would be extremely expensive to replace the suite on a regular basis, and the enterprise would be exposed or suffer costly down-time during the replacement activity. The owner/operator will want to combine components from different providers on a best-of-breed basis to obtain the best overall match to its security requirements at any given. We expect continued rapid innovation in defensive technology and weapons and tactics used by threat agents.

7. **Reluctance to share information**. Information sharing is one of the key planks of the European Cyber Security Strategy and is the subject of work in Working Group Two of the Network and Information Security Platform (NIS WG2). This area presents some barriers, as corporations often are reluctant to share cyber vulnerability information with the government because they consider their system vulnerabilities to be sensitive information and do not want proprietary documents and information to be disclosed to the public and competitors. Stakeholders worry that such disclosures could result in reputational harm, competitive disadvantage, lost profits and shareholder derivative actions or other lawsuits. Information shared with the government could potentially be released through government employee error or as the result of a FOIA (Freedom of Information Act) request. Companies also are concerned that an agency with regulatory authority over it could use information about a cyber-incident to pursue enforcement or other unrelated regulatory action.

8. **Privacy risks neglected.** Unauthorized eavesdropping or data collection by the large numbers of Internet-enabled devices as well as civilian surveillance scandals of 2013 showed how Western democracies have used the law to justify restrictions to citizens' right to privacy. In response to the leakage of the National Security Agency international monitoring scheme, the U.S. Justice Department released a legal memorandum explaining why the government believes it is lawful under a provision of the Patriot Act known as

Section 215 for the N.S.A. to collect and store logs of every phone call dialled or received in the country. Although the speech for cyber security can be misused for censorship and social control (and it has been), cyber security should not be interpreted as a tool aimed to restrict citizens' fundamental rights. Personal data is nowadays traded among service providers like other commodities, meriting an analysis of individual transactions in the market place. For example, according to ENISA (2011b: 26–27), 47% of the service providers interviewed treated personal data as a commercial asset; and 48% revealed that they share data with third parties (ENISA[20] 2011b: 26–27). Therefore, it is important to also understand the economic dimension of privacy. By an exponential increase of connected devices (i.e. due to IoT), more privacy related information will be managed by more businesses or economic interests hence higher likelihood of potential privacy mistakes.

9. **Reactive approach**. Good security governance and security culture takes time to develop in an organization. It cannot be obtained quickly as a reaction to an attack. There are some good security tools in existence today, but designing a layered defence takes time. Good security defenders who can utilize these tools are in high demand and hard to hire quickly. A reactive approach to cybersecurity is a critical mistake; there is a need to invest in proactivity including education and training for workforce development.

10. **Lack of agile processes** to encourage early R&D demand for solutions. While the most EU research projects solve problems of the future and the first results are available in 3-4 years, the customer needs and expectations, especially in ICT or cyber security, are close to immediate. This problem deserves special support and treatment, maybe through the open calls managed by individual projects or dedicated platform.

4.4 Gap analysis (tech., policy, regulation, and competences) for achieving the vision

4.4.1 Technical and security gaps:

In this section, we group the technical and security gaps within the topics of relevance.

1. Internet of Things

   a. **Cryptography with high strength**, yet low power requirements for the 2025 world of billions of devices and applications; As the Internet of Things starts to penetrate our everyday lives, we should expect to increasingly interact with smart low-power sensors that should support authentication and encryption.

2. Cloud

   a. **Enhanced cryptography for Cloud Services:** Cloud services need assurances from providers that effective technological solutions have been put in place to manage and mitigate the security risks facing their data stored on the cloud. More work should be done to preserve privacy and the confidentiality of data in the cloud, such as privacy-preserving cryptology including anonymous credentials and practical techniques for processing encrypted data. Furthermore, research into functional encryption such as attribute based cryptography and cryptography in a cloud service context would be of value.

   b. Future research should aim at addressing the **governance of data** and provide stakeholders with the means to exercise appropriate controls on their data so that they may access, validate or delete data when needed.

---

[20] http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/monetising-privacy

3. Privacy

   a. **Privacy protecting, yet trustworthy identification and authentication** technologies for technologies that require top level provenance requirements e.g. biometrics for electronic voting; This is a one-way street: if these authentication technologies do not provide adequate privacy guarantees several applications, such as on-line voting will never catch up;

   b. **Privacy-preserving digital currency**. It is not clear for how much longer we will have "paper" money. If paper money disappears, we would need some other form of digital currency that provides privacy in financial transactions;

   c. **Privacy in Big Data Analytics**: Large scale data processing (e.g. big data analysis) with adequate protection methods with the stress on access control, data confidentiality (e.g. using new cryptographic approaches, methods and technologies) and consequentially adequate privacy protection;

   d. **Privacy-by-design practice** that is generic enough to be integrated in the many application domain design practices (e.g. space application, automotive, internet of things, banking, …) and thus reflects the multidisciplinary viewpoint;

   e. **Every day-anywhere ICT** (e.g. internet everywhere) with adequate privacy protection in terms of cost-effectiveness, user-friendliness, high security (e.g. problem of users' authentication)[21].

4. Data

   a. **Transparency about who has data** at all times and knowledge of what it is being used for; over the past few years, people move an increasing percentage of their lives online: shopping, entertainment, even significant parts of education have moved on-line. As a result, people repeatedly release data about themselves: what they purchase, where they travel, what they read, what they watch. Keeping track of which data have been released to which entities is an important first step on giving people control over their digital lives.

5. Cyber Crime / Law Enforcement

   a. **Fraud protection** more and more financial transactions are digital and new digital currencies emerging. Digital currency, being a sequence of bits, may be copied much easier than paper-based currency. Developing mechanisms to protect from such copies and/or fraud in general will be of paramount importance to the success of digital currency and trust in digital financial systems. **Cyber forensics** that will provide the user with strong security with some level of control over their data usage (assuring transparency on who is using what and for what purpose), while providing protection of their privacy; Users should be able to verify who has access to their data and **revoke** this access if desired (assuming that this does not conflict with any local law)

   b. **Detection and prevention** of potentially harmful things before they are created and used (i.e. while still in a digital form) e.g. 3D printing/Maker Economy;

6. Security

---

[21]   https://www.linkedin.com/today/post/article/20140806095051-206580-the-world-in-2025-10-predictions-of-innovation

a. **Secure data channels** for new applications, including end to end communications security for Internet of things and Internet of Services [SYS13] [22];

b. **Security and dependability of Critical Information Infrastructure** protection (CIIP) will be a major issue in 2025 as the future Internet will be CIIP;

c. **Human connected devices security** (e.g. human implant, full-body sensors) with adequate security measures, techniques, technologies, methods and approaches;

4.4.2 Standards, Social, political and governance gaps:

Balancing the societal needs for authorities providing continual levels of security (e.g. with ICT enabled surveillance with increasing privacy requirements of the citizens); States will probably desire to have an increasing amount of data about their citizens. This "appetite" for data may significantly hurt the digital economy especially from citizens who are concerned with their privacy. Corporations will probably need new security/encryption mechanisms that will make sure that the data of their users cannot be captured by any state without a due process.

Stronger coordination and cohesion of the stakeholders groups: R&I, Industry, government and other policy makers; Measures to ensure timeliness of publicly funded R&I results which must catch up with the faster requirements of the industry stakeholders;

In building a truly global R&I environment, we need to have global standards and agreements on how to carry out R&I in a consistent and effective manner e.g. some countries only fund research and academia whilst the EU funds research, academic and industry.

Good adoption of technical security measures (e.g. through good user awareness and user-friendliness).

Privacy-by-Design practices, which are based on common technical, legal, socio-political principles, takes into account specific national parameters, and which are fully integrated in engineering practice standards.

Transversal Standards: We are coping with the following problem: there are many engineering standards. For instance, if we consider the IEC61508 safety process, it led to a number of variants (EN50128 for railways, ISO26262 for automotive, IEC61511 for process oil/gas) leading to the non-trivial question: How can a transversal standard be integrated and adopted [SMI10]?

---

[22] http://www.pewinternet.org/2014/05/14/internet-of-things/

5 Area of Interest 3: Trustworthy (Hyperconnected) Infrastructures (Infrastructure layer)

This section concentrates on trustworthy (hyperconnected) infrastructures, especially critical infrastructures due to their importance for the European Cyberspace and the European Economy. When speaking of "critical infrastructure", we refer to the definition used by ENISA [MAT13] and that was defined by the European Commission [EC05]:

> *''An asset, system or part thereof located in Member States that are essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact on a Member State as a result of the failure to maintain those functions''.*

5.1 Description of the AoI's vision

The future vision of critical infrastructure (CI) is mainly based on this requirement: infrastructure processes and resources must be more adaptive, decentralized, transparently collaborative and efficiently controlled.

Achieving this vision requires a more and more pervasive usage of Information and Communication Technologies (ICT). ICT will be exploited to support every infrastructure process and service and will empower the capability to make infrastructures, related to different sectors, to interoperate each other (i.e. to be hyperconnected). This way, it will be feasible to improve processes-efficiency and create new added-value services.

For this reason, ICT will become more and more a critical infrastructure itself. As such, ICT infrastructure will be safe, reliable, predictable and always available, it will operate confidentially and in a privacy protecting way, it will be capable to resist and to react to cyber threats in real time. The vulnerability in the ICT equipment, processes and services, and their resilience against malicious attacks will be more and more reduced, monitored and controlled for the security of all future infrastructures and, as such, for the safety of all citizens.

The future ICT evolution will make key infrastructures of modern life, such as energy production sites and transmission systems, storage and distribution, transportation of people and goods systems, information and communication networks, sensitive manufacturing plants, banking and finance, healthcare and public administration systems more secure and dependable. The role of ICT will be fundamental to safeguard all CIs of the future that can be damaged, destroyed or disrupted, by deliberate acts, natural disasters or mismanagements.

ICT, and in particular the cyber-space, will also enable citizens to permanently access information and will enables citizens to be in control of the ICT processes. This development will induce a positive perception of the trustworthiness of the infrastructure and its services (even if partly compromised). A key aspect in the development of trustworthy hyperconnected infrastructure will be the surrounding of citizens by network devices in the context of ubiquitous computing. Ubiquitous computing brings changes (e.g. ambient assisted living, AAL) but also challenges (e.g. privacy threats). For instance, future cities for European citizens will depend on CI and compete for human resources as each city must be optimized to use its CI in order to motivate skilled people to stay in the city and to move to the city. We expect a worst-case failure of critical infrastructure to cause catastrophic consequences.

5.2 Description of the issues and challenges

The AoI contributors highlighted a number of challenges during the first two plenary meetings, held in September and December in Brussels, and via e-mail. The major aspects mentioned are the integration of confidentiality and security by design in infrastructure (incl. cars, trains, buildings, Internet infrastructure, …); realizing achievable solutions/engineering of more secure and trustworthy infrastructure environments; incident/vulnerability handling; providing trust for partly compromised infrastructure components; the communication between stakeholders (e.g. industry and research) as well as the education of end-users (e.g., to improve the protection against Advanced Persistent Threats [CYS13]); the migration of legacy systems and protocols; the scalability increase of infrastructure and its data; the handling of a rapid growth in the sophistication of threats across the whole spectrum of the cyber ecosystem and the linked increase of the risk of disruption; the decreasing available time to respond to attacks; the global competition (i.e. establish a security industry for the necessary products in Europe); the creation of ways to measure security; the creation of user-friendly/user-tailored security solutions; secure inter-connectivity of infrastructure components; and the introduction of improved standards.

5.3 Identification of Technology, Policy and Regulation Enablers/Inhibitors

5.3.1 Enablers (Technology, Policy and Regulation)

Key aspects mentioned multiple times serving as enablers are the education of users/companies, the implementation of constructive security/privacy regulations and standards on different levels (also governmental / cross border), the improvement of security features on different levels of security; the integration of security by design, improvement/utilization of formal methods, empirical studies, privacy enhancing global PKI, and machine learning to improve security, the presence of an un-fragmented and compact research community in Europe (on trusted devices). A forum with research institutions and industry on industrial themes could also serve as an enabler.

5.3.2 Inhibitors (Technology, Policy and Regulation)

Inhibitors on the other hand were mentioned to be the production of infrastructure components outside of Europe (linked to backdoors/hardware Trojans in existing and upcoming products), the lock in old business models and the fragmentation of the market, the problem of understanding the particular technologies/lack of awareness, the problem that research does not drive European standards, the presence of complex systems, the lack of regulation (leading to market failure), transparency, enforcement, communication between stakeholders, and suitable standards, the lack of more intense European lobby work, the difficulty and complexity of security problems (e.g. complexity of SCADA systems), the lack of trust in infrastructure, and the workload of network edge services.

5.4 Gap analysis (tech., policy, regulation, and competences; for achieving the vision)

Participants recognized end-to-end security, studying/managing the behaviour of complex interconnected systems, and data leakage protection (DLP), protection and secure refines of OSS/well-known platforms/APIs and secure computing in hostile environments as technological research gaps. Moreover, the lack of education, usability, trust, and key management was found to be research gaps. Another gap highlighted was to understand the impact of architecture and

design on governance/policy as a service and agile inter-operability. Other mentioned research gaps lie in the M2M authentication, vulnerability analysis, resilience of energy supply, mobile security solutions, surveillance sensors, and in the lack of measurable indicators of trustworthiness as well as in the combination of safety and security means for infrastructure.

In addition, gaps lie in the implementation/regulation/enforcement of standards and inter-networking, in the question of how properties (of technologies and services) can become more transparent, and in the regulation of the handling of historic data.

5.5 Structure of this Section

In the remainder of this section, challenges and issues, technological inhibitors and enablers, and gap analyses are discussed separately for each particular sector of infrastructure. First, the three fundamental sectors ICT, Energy, and Transportation are covered. Afterwards, we focus on sectors that depend on these three sectors.

5.6 ICT Infrastructure

5.6.1 Issues and Challenges

ICT infrastructures have become pervasive in our modern life. We rely on them for services that have become intensely critical for many aspects of our modern life, such as obtaining basic services (energy, water, transportation, …) or easing our activities (computing faster routes on the road, entertaining ourselves everywhere, etc.).

As stated by ENISA, "citizens expect national authorities to be fully aware of the possible interdependencies" in the context of technical and geo-political threats to the Internet infrastructure" and that the authorities "put in place all possible measures to ensure the security and resilience of their communications" [MAT13]. We can assume that the same sentence can be stated for all relevant security-sensitive infrastructure, including communication and telecommunication infrastructure, especially for international (mobile) telecommunication.

However, many security issues remain unanswered:

1. Understanding and visibility of risk and security measures. In many cases, security imposed in ICT infrastructures is seen as a constraint and a loss of functionality. For example, we have known for a long time that JavaScript and Adobe-flash are dangerous attack vectors that can be served by a malicious web site to attack the browser. On the other hand, a web without JavaScript and Adobe-Flash is very hard to navigate. Therefore, people arbitrate and prefer functionality to security. Part of this arbitration process is because users do not perceive or understand the risk, while they immediately perceive and resent the absence of the functionality. We should endeavour to both make security protection measures more acceptable by formally securing pivotal components, offering alternatives to dangerous functionality, and by clearly informing the user of the risk that he has to accept.

2. ICT infrastructures are highly interconnected. This means that there is a very high probability that a security incident will propagate from place to place (unless the attacker specifically targets a given organization). Yet, the granularity at which we are currently able to validate networking activities, the flow level (addresses and ports source and destination) is highly insufficient to provide the required level of control that would facilitate the deployment and management of security measures that would provide fine grain control over the exchanges (both in and out) in which a specific ICT infrastructure is involved.

3. ICT infrastructures contain components whose failure will systematically compromise their integrity. From cryptographic protocols to operating functions, this "trustworthy core" provides the foundation for flexible and powerful higher-level application layers. Recent attacks[23] have shown that subtle defaults in the implementation of such components can have a major impact on the systems that rely on them. In addition, while high-profile vulnerabilities are patched in a matter of hours, there is no guarantee that less visible threats are not remaining. There is a need for tools and methods that provide developers, integrators, and validators with strong and demonstrable confidence in the mission-critical components of their infrastructure.

4. ICT infrastructures are highly complex. This means that there are many entry points, and that these entry points are run by people with different capabilities and needs. Even though the organization running the ICT infrastructure may have defined a global security policy, it is very hard to ensure that all policy enforcement points will effectively interpret and implement the same security rules (or their appropriate share thereof). As such, it would be possible for an attacker to find the weakest spots and to penetrate the ICT infrastructure even if protective measures have been implemented. There is a significant lack of measurements and metrics that would enable a central authority to assess its security posture, and to point out these weakest policy enforcement points.

5. Many attacks against ICT infrastructures could be detected much earlier than they currently are. In many cases, owners of ICT infrastructures are alerted after the compromise has taken place (and sometimes significantly later, in a matter of months) and by the outside world receiving deviant behaviours. Yet, in a large number of cases, internal detection and protection systems sent to their management platform the right alerts. This means that even though there has been a lot of progress in detecting attacks, the analysis that leads to the risk evaluation and mitigation remains faulty. This is a significant area of progress, both on the technical side (accuracy of alerts needs to be better, explanations need to be clearer, time from detection to mitigation needs to improve) and on the human side (security alert analysts need to be better at assessing the information they receive).

6. Security remains oriented towards the protection of the physical (or virtual) components of the ICT infrastructures. The basic assumption is that if the technical infrastructure is secure, what it is used for (information processing) will be as well. Yet, in many cases, the most valuable property is the data itself, and service-level or data-level attacks (for example SQL injection or Cross-Site Scripting) easily bypass the protection layer of the ICT infrastructure to get access to the data. Protection and detection mechanisms, as well as security policy formalisms, need to become better at specifying the security needs that are tied to the actual information, and not just to the protection of the physical equipment.

7. Mobile Equipment: Mobile equipment in ICT context is linked to various challenges such as loss of devices, jailbreaks, BYOD, and mobile malware [CAP14]. Also important in this regard are challenges linked to Big Data, such as data mining using all kinds of ICT-related data while preserving privacy [CAP14].

8. According to AV-Test[24] there have been around 80 million new, unique malware samples in 2013. Thus, we are in urgent need for fast and reliable malware analysis capabilities. Currently, the majority of these malware samples are targeting end-user pcs, server systems or smartphones. With our security mechanisms, detection and analysis capabilities for today's malware evolving we have to expect malware authors not only adapting to changes in the ICT landscape but also to our evolving capabilities. Thus, there will be changes in malware's behaviour and capabilities we have to adapt our analysis

---

[23] http://heartbleed.com/
[24] http://www.av-test.org/en/statistics/malware/

capabilities to (cf. gap analysis for a list of list of features we have to expect from future malware that research should take into account in for better analysis capabilities).

9. Competition with High-tech Players: Currently the EU is not competing any more with ICT high-tech players, but newcomers like China, India, etc. The current mass surveillance can be seen as a wake-up, what will be lost when dependency and legislations are misused towards EU. We see that there are three challenges which are needed to overcome:

    a. build European assets for ICT and ICT security

    b. protect European ICT assets and ICT security instruments from unfair competition

    c. allow European member states to build their ICT protection according their own foreign policy

10. Compliance with privacy and security laws, as well as ethical concerns, in managing privacy and cybersecurity risks associated with the collection, use and disclosure of information handled by ICT systems.

Shortly:

1. We have a clear shortage with European ICT assets, which means that the EU is heavily depending on foreign ICT components. We need to improve this situation by the Horizon2020 program in the way that this funding is targeted to European companies, which will then also build the ecosystem competences in this area for European utilization.

2. As we have seen, European ICT players need similar support as US companies when building their ICT security and business. In the EU, we have been concerned with unfair competition that we have seen in passenger plane and shipyard industry. However, the EU focus should be broadened also to cover ICT and ICT security industry. When Google has been under investigation here in the EU, NSA has been taken immediate actions to influence and mitigate this kind of investigation which is targeted to US ICT industry players. This means in other words that the EU needs to protect the ICT industry in a similar way as Shipyards and passenger plane industry.

3. Part of the NIS work is risk assessments (WG1), which happens only if real information is available to make risk assessment. This information to make justified decisions from risk area cannot be done only trough political or commercial justifications. WG3 should take in agenda, how in long run EU could make security assessments to ICT components (Hardware or Software) used in EU networks. In this, we should perhaps look to US as well, while they have already a working program on how to utilize foreign ICT components in their networks.

5.6.2 Identification of Technology, Policy and Regulation enablers/inhibitors

5.6.2.1 Enablers

1. The increasing diffusion of mobile devices that enable ubiquitous computing and enlarge the number of ICT users.

2. The establishment of the new EU General Data Protection Regulation.

3. The growth of available services on the Cloud.

4. The extension and inter-connection of the Internet to the real-world, by means of sensors, actuators and, more in general, smart-networked-appliances, make the ICT more pervasive and involved in any human activity.

5.6.2.2 Inhibitors

1. The ICT user set is made of many entities, including many people with different capabilities and levels of awareness about security threats, each running an entry point to the ICT infrastructure. It is thus very difficult to ensure a measurable and reliable enforcement of security policies.

2. The usage of ICT products, made outside Europe, rise the security and privacy risks for the ICT-based European business.

3. The fear to lose control and power makes many organizations and individuals against the sharing of information they owns and dramatically reduce the opportunity to enhance the level of interoperability of their ICT systems.

5.6.3 Gap analysis (tech., policy, regulation, and competences) for achieving the vision

A major aspect in the context of ICT infrastructure gaps is the sophistication of malware due to the following aspects:

1. **Cloud-based malware.** With the evolution of cloud-based services, we have to expect malware targeting and leveraging the cloud infrastructure. That leads to malware authors shifting their focus from targeting end-user PCs running Windows OS on bare-metal machines to virtualized server systems. Accordingly, we have to be prepared for challenges coming with malware running in virtualized environments (e.g. prevent malware to escape from the virtual environment gains importance).

2. **IPv6 ready malware.** Most malware is still communicating using IPv4. Since many countermeasures still do not take into account IPv6 traffic malware will move its communication to IPv6. Thus, we should research how this affects our today's countermeasures.

3. **Deep system mobile malware.** Currently most malware for mobile systems are malicious android apps. In the future, we might see malware trying to get deeper than the Dalvik Virtual Machine. Thus, malware targeting the OS or device drivers directly.

4. **Hardware & close-to-hardware Trojans.** At the latest since the Snowden, documents are online, we know that there already exists a multitude of possibilities to leverage ICT components (e.g. routers, switches) for spying purposes. Unfortunately, there are multiple additional possibilities leveraging hardware or close-to-hardware software (e.g. device drivers or firmware) to infiltrate systems. Thus, we should research possibilities to detect and analyse such infiltrations.

H2020 clearly identifies the need of preventing cyber-attacks on any component of the digital society (networks, access devices, IT services, ….), including intangible assets like intellectual property and privacy. The H2020 legal basis include between the others the EU Data Protection Directive 1995/46/EC, replaced by the new EU General Data Protection Regulation that is a privacy law applicable to all organizations that collect and process personal data in the European Union.

Thus, the concepts behind such Regulation (along with any EU legislative source on this field) need to be acquired and applied through a multi-disciplinary approach, including the legal, ethical, social and technical aspects.

New challenges will arise as consequence of that analysis to be handled by ICT infrastructures using any methodology and tool (e.g. Privacy by Default, Privacy by Design, Privacy Impact Assessment, etc.) in order to adequately protect privacy and personal data, check processing activities against requirements from privacy regulations, track incidents that lead to unauthorized disclosures (investigation, remediation and reporting), and deter data misuse.

New principles will be adopted as, for instance, people will be able by default to (i) access their own personal data and rectify any wrong or incomplete information; (ii) control the privacy of communications and content (graphical as well as textual); (iii) control the life cycle of shared content having the opportunity of objecting their data processing on legitimate grounds; (iv) verify the identity people accessing their data; (iv) manage the contractual commitment to maintenance of their data. Moreover, people will give their explicit consent for the collection, use, dissemination, and maintenance of personal data and they will be able to keep track of and communicate what they are saying in the context in which they are saying it.

5.7 Smart Grids

5.7.1 Issues and Challenges

A Smart Grid can be defined as a process, rather than a product. It is the digitalization of the electricity infrastructure and it is the transition from a closed, centralized, analog infrastructure to an open, largely decentralized, digital infrastructure. A Smart Grid is the transition from a system where generation, based on fossil fuel, adapts to users consumption, to a system where user consumption must be flexible enough to adapt to the fluctuations of the renewable based generation. Finally, a Smart Grid is a system where electricity is traded as a commodity on international marketplaces.

A Smart Grid provides energy on demand from distributed generation stations to customers. The grid intelligently manages the behaviour and actions of its participants using information and communication technologies (ICT). A novelty compared to existing energy networks is the two-way communication between consumers and electric power companies. The benefits of the Smart Grid are envisioned to be a more economic, sustainable and reliable supply of energy. However, significant security concerns have to be addressed for this scenario, due to the possible dangers of missing availability of energy for customers, as well as threats to the integrity and confidentiality of customer's data. These concerns are of particular relevance, because energy grids have a significantly longer lifespan than telecommunication networks [ALO12]. In addition, privacy concerns have risen, such as the possibility of creating behavioural profiles of customers if their energy consumption is transmitted over the Smart Grid in small time intervals [LIN14]. In particular, the attack surface is increasing over time in the Smart Grid for two reasons. Firstly, an increased amount of private sensitive customer data is available to service providers, utility-, and third party partners. Secondly, new data interfaces such as new and improved meters, collectors, and other smart devices cause new entry points for attackers [NES14].

Resilience has always been the prime goal for the operators in charge of the generation, transmission and distribution infrastructures. In Europe, these operators have a long track record of success in containing accidents, avoiding black outs, and mitigating the effects of natural disasters. With the Smart Grid, cyber-security is now at the core of their efforts to provide a resilient infrastructure.

The issues linked to cyber-security follow from the very nature of the Smart Grid transition. It should be assumed that all software components could be compromised either because they are exposed to the Internet, or because physical security can be bypassed. It should be assumed that all

components of the Smart Grid, from smart meters, to power plants, or relays could be targets for cyber-attacks, as well as the SCADA systems used to monitor these software components. As mentioned earlier, user's privacy should be enforced, and the mechanisms of trading marketplaces should be resilient.

The fact that any components might be compromised is commonplace on the Internet. The obvious solution is to rely on encryption whenever data is transmitted or stored. The problem then is (i) to secure encryption keys, (ii) to secure encryption and decryption and (iii) to secure the computation that takes place on decrypted data. The existing hardware protection techniques (e.g., trusted execution environments or hardware secure modules) can be used to guarantee confidentiality and integrity (as the sensitive data is protected in hardware that can provide tamper-resistance and tamper-evidence), but they cannot guarantee availability (as the secure hardware is accessed from software which is potentially compromised). Sandboxing techniques can be used to contain the computations on decrypted data. Note that these techniques address the issues linked to cyber-security as well as privacy.

The challenges thus are the following. First, the use of hardware protection techniques must be integrated in the software development processes that shape the Smart Grid. Second, it is crucial to devise denial of service defence methods that do not disrupt the Smart Grid. Third, the Smart Grid architecture and governance must be such that compromised components are detected and isolated in a way that minimizes the impact on the rest of the infrastructure. Finally, disaster recovery testing techniques such as Google's DiRT or Netflix' Chaos Monkey should be adapted to the Smart Grid.

5.7.2 Identification of Technology, Policy and Regulation enablers/inhibitors

5.7.2.1 Enablers

1. Resilience for the generation, transmission and distribution infrastructures

2. Early-warning systems, which contribute to situational awareness for every part of the smart grid infrastructure

3. Accessibility and complexity of legal requirements

4. Means to respond in (almost) real-time to attacks on the smart grid infrastructure

5. Secure SCADA systems (cf. section on ICS control system's security)

5.7.2.2 Inhibitors

1. Fear of effects of possible attacks on the energy/smart grid

2. Privacy concerns regarding customer's sensitive data as such data is available to service providers and third party partners to an increasing extent

3. Increasing attack surface due to new data interfaces, collectors, and related devices

4. Lack of security awareness on provider-side

5. Insecure SCADA systems (cf. section on ICS control system's security)

5.7.3 Gap analysis (tech., policy, regulation, and competences) for achieving the vision

These challenges given rise to a number of research topics, which will be relevant in the years to come:

1. **Exchangeable and evolving security mechanisms** are of utmost importance due to long life spans and the previously described changes during the grid's lifespan. For each security mechanism, we have to evaluate possible future threats and provide the means for updates and replacements.

2. **Evolving privacy requirements** have to be considered due to permanent increase of personal data. Moreover, we have to consider that more types of data can become personal data. In the grid, we now consider energy consumption data and location data as personal information. In the future, the list of data that can be contained and analysed will increase by, e.g., food consumption, cleaning, social activities, professional ambition, health status, and upcoming travels. We have to create methodologies to check if new privacy threats arise and elicit privacy requirements for these, which have to be fulfilled by the grid's stakeholders and technologies. A focus should be on visualizing privacy threats to customers and practitioners to **raise awareness** of these issues in an intuitive way.

3. The availability of energy is the primary goal of the Smart Grid. **Early warning systems** are required that can identify if a service or stakeholder threatens this goal. The protection of this goal has to allow for mechanisms that can disconnect smart devices or stakeholders from the grid, and even isolate entire parts of the grid if security threats arise from them that target the availability of energy.

4. Professionals alone cannot tackle the increasing security and privacy concerns in the grid. We have to provide **easy access to privacy and security best practices for practitioners and customers**. Governments and industry have to collaborate to provide incentives to familiarize all stakeholders with these practices, such as reduced energy prices for well-applied security and privacy techniques. Moreover, the grid providers should rely on the information of customers for suspicious activities in the grid. We have to have an easy-to-use infrastructure for reporting these events and supporting the customers in making correct choices where to place their trust.

5. It is of vital importance for all stakeholders of the grid system to be aware of **changing legal requirements** e.g. for energy consumption, privacy etc. We need mechanisms in the grid to distribute and consider this information when interacting with the grid. The information in legal texts has to be explained in a comprehensible way, and the penalties for violating the laws have to be made explicit in order to deter attackers.

6. The Smart Grid and its environment will **change permanently** due to new and updated devices, communication protocols, and services. It has to be permanently re-evaluated if the security assumptions still hold, in particular, when bootstrapping new devices into the grid. The grid connects households, houses and areas, which makes it difficult to isolate single devices. We need technologies that make it possible to **measure how much a stakeholder trusts** a new device, to monitor and evaluate its behaviour, and automatically isolate the device if it violates trust assumptions.

7. The Smart Grid relies on the **integrity of data** in the grid, e.g., concerning energy consumption, information for steering energy consumption and production, etc. The data is transferred throughout the grid. Integrity mechanisms have to ensure that the data remains unchanged by unauthorized persons or services and the data remains available as long as required. In some cases this information have to be transmitted in real time, e.g., to increase the energy production and release stored energy if the demand suddenly

increases. The issue **how to protect these data over the long lifespan from the increasing attack surface** is a current challenge. Moreover, protocols to aggregate data for privacy reasons or to prioritize data have to be evaluated constantly to ensure the privacy and dependability of the grid. Methodologies and implementations that provide these flexibilities have to be developed.

5.8 Transportation

5.8.1 Issues and Challenges

Before introducing issues and challenges it is worth identifying the context of Transport Critical Infrastructures (T-CI) in the transport domain, i.e. define what is part of a Transport Critical Infrastructure, and what is not:

A Transport Critical Infrastructure is a transport system (for people and freights) whose failure may have a macroscopic effect on critical sectors at National and/or European level.

It is worth noticing that the definition applies differently to the different transport modes (road, rail, air, etc.). As a sample, the malfunctioning of a train on the RailRoute2050[25] backbone could have a relevant effect on the tourism sector at European level, so in this case trains running on the rail backbone are part of the T-CI itself. On the other hand, malfunctioning of all traffic lights on a small town would not impact significantly any critical sector, so that particular traffic light system shouldn't be part of a T-CI.

Moreover, we define each T-CI as subject to a single controlling entity (either alone or composed by a consortium). As a sample, Italian and French highways are two different T-CIs as they are subject to different controlling entities.

For the purpose of this section, T-CIs are analysed from the point of view of the ICT systems governing them. In particular, we foresee that, in the next years, the T-CIs will greatly increase reliance on ICT systems. This is also reflected by the aim of creating a Single European Transport Area, thus easing "the movements of citizens and freight reduce costs and enhance the sustainability of European transport."[26] The major challenge in the creation of a single transport area at the European level is the interoperation of ICT systems governing the existing T-CIs, that cannot be easily replaced. Interoperation does not only refer to technical aspects related to the interconnection of existing systems, but primarily refers to the definition of policies and procedures enabling an extensive collaboration of systems that govern every T-CIs.

In the transport sector, there are significant strategic challenges in which ICT can play a vital role. Among the most important challenges, it is interesting to mention:

1. minimization of CO_2 emission by promoting the use of cleaner means of transport such as electric vehicles,

2. increase of road safety with particular attention on reducing significantly the number of deaths caused by road accidents,

3. creation of the Single European Sky, to address the forecasted 50% increase in air traffic in the next 20 year,

4. increase of the capacity, speed and safety of both passengers and goods rail transport systems,

---

[25] http://www.errac.org/wp-content/uploads/2013/11/D9-SRRA-RAILROUTE2050.pdf
[26] http://ec.europa.eu/transport/themes/strategies/2011_white_paper_en.htm

5. creation of an European cross-border integrated and sustainable transportation network,

6. improvement of the cross-border electronic document interchange and logistics support systems to enhance the efficiency of the freight traffic by sea.

Transportation systems are becoming increasingly complex, incorporating numerous, intricate control systems and sub-systems working in parallel; also, they interoperate in an environment composed by a large number of diverse service providers, across several countries. A wider use of communications and information technology will increase the efficiency and functionality of transportation systems. The increase in complexity, functionality and connectivity comes at the price of an increased vulnerability.

These complex infrastructures will be highly distributed and thus difficult to protect; besides, it is also important to consider that every country has its own networks and every transport operator has its own strategy regarding the protection of its infrastructure.

Vehicles and other means of transport will be connected to communication networks to support infotainment, safety and emergency functionalities. Transport support systems will be more easily accessible by nomadic users – this is a truly indispensable factor in the transport sector.

This new scenario will introduce new threats and risks, and more critical dependencies with risk management, prevention, infrastructures monitoring, collaboration and crisis management, user data privacy. Some challenges in security and resilience will be common factors across the different types of transport:

1. assess and manage risks

    a. compliance with the requested level of security, safety, dependability and privacy, taking into account the whole perimeter of the infrastructure (including physical assets, the cyber layer, processes and services)

    b. increasing threat and risk factors, including cyber, physical, process and human risks

2. prevent attacks

    a. achieve a comprehensive and continuous situational awareness, supported by an information intelligence capability

    b. support the information sharing and the effective and automatic use of exchanged data

    c. tampering of field devices, roadside and infrastructure equipment

    d. security (including confidentiality and availability) of the communication channels used by infrastructures, vehicles and other transport means; equipment's mutual authentication and trust

3. monitoring and protection

    a. Integrated monitoring, including all infrastructures layers (physical, field, network, systems and applications)

4. unauthorized data access, modification or destruction

    a. unauthorized use of services or denial of service (DoS)

5. manage incidents

    a. Incident real-time detection

    b. automated systems self-configuration

6. privacy of users data

    a. privacy in open and big data, distributed networked objects, passengers and vehicles geo-localization information and mobility patterns

7. secure and precise positioning of transport means and goods

    a. dependable and attack resilient positioning systems

5.8.1.1 Sub-topic: Port's Security

Critical Information Infrastructures (CIIs) are a vital element for the functioning of the most critical infrastructures that underpin our economy and society, including for example transport, energy and telecommunication infrastructures. Therefore, for over a decade significant efforts have been allocated in the introduction of risk management and assurance methodologies, which hold the promise to alleviate the vulnerabilities of the CIIs, thereby reducing potential adverse effects in both society and economy [GIA12]. In principle, most of the risk assessment methodologies focus on the identification and classification of threats, the identification of the various vulnerabilities and ultimately the evaluation of the potential impact of threats and vulnerabilities [STE10, HER10]. However, the various methodologies feature several differences in terms of the end-users and stakeholders that they address (e.g., policy makers, decision makers, asset managers, CI operators, solution integrators), but also in terms of the assets that they address and the level of accuracy that can handle.

The limitations of existing risk management methodologies in terms of addressing the cascading effects and the complexity of the ports' supply chain, and more in general, of the Transportation ecosystem, have not been considered by the existing standardization and legislation efforts. In particular: Maritime security standards and legislation (e.g. the International Ships and Port Facilities Security Code (ISPS), the International Safety Management Code, EC Regulation No 725/2004 on enhancing ship and port facility security, and EC Directive 2005/65 on enhancing port security) and risk assessment methodologies (e.g. MSRAM, MARISA) do not address the ports CII cyber security adequately. Specifically, they concentrate on the protection of the physical nature of the ports, thereby ignoring their cyber-nature. Additionally, in the calculation of impacts they ignore the cascading effects from the interdependent threats.

Not surprisingly, the first ENISA (European Union Agency for Network and Information Security) report on cyber maritime security (2011)[27] concludes "the awareness on cyber security needs and challenges in the maritime sector is currently low to non-existent".

During the last couple of years, we have witnessed the emergence of research initiatives that attempt to deal with the cyber risks and vulnerabilities of the port-CII ecosystem, both in terms of the number of stakeholders and in terms of the complexity of the CII assets involved. For example, during the DG-MOVE international 2012 conference, the national project S-PORT[28] was acknowledged as a national research effort on ports' CII cyber risk assessment. S-PORT provided a collaborative environment for the security management of the Port Information and Telecommunication systems [NTO12, NIN12]. Except for this national activity, EU wide activities towards a holistic risk management framework for port security have recently emerged under the CIPS[29] (e.g., CYSM[30], MEDOUSA) and FP7 programmes (SUPPORT, CONTAIN). **Nevertheless, the risk assessment methodologies studied in these projects are limited to the port's CII domain and do not consider or predict cross-sectorial, cross-border threats from the port's supply chain**.

---

[27] http://www.enisa.europa.eu/media/press-releases/first-eu-report-on-maritime-cyber-security

[28] http://s-port.unipi.gr/index.php/

[29] "Prevention, Preparedness and Consequence Management of Terrorism" and other Security-related Risks Programme of the European Union

[30] www.cysm.eu

Overall, there is a clear need for extending and validating existing risk assessment frameworks in terms of their ability to deal with cascading effects risks and vulnerabilities, associated with cross-sectoral, cross-border threats. A starting point for modelling cascading effects lies in the understanding of the inter-dependencies of the various infrastructures [PED06, STE01], which include physical, cyber, geographic and other (logical dependencies). Moreover, techniques for modelling and understanding risks in the scope of Systems-of-Systems (SoS) are needed, along new techniques for modelling composite port assets.

5.8.2 Identification of Technology, Policy and Regulation enablers/inhibitors

5.8.2.1 Enablers

1. Technology: secure and resilient network architectures / increased connectivity, secure ICT supply chain, automatic malware detection, real-time incident detection, robust authentication systems, data anonymization, data fusion, secure wireless communications, supercomputing, secure scalable ICT systems.

2. Policy: info sharing PPPs, incentives to innovation, access to risk capital by cyber start-ups, use of EU structural funds to raise cyber protection of infrastructures, incentives to public sector to improve unified governance of complex infrastructural systems, complexity of transport systems [CYS13b].

3. Regulation: cyber security directive, data protection regulation.

5.8.2.2 Inhibitors

1. Scarce public funding to research and innovation, fragmentation of critical infrastructure protection policies, lack of public incentives to ICT infrastructure upgrade, lack of trust for information sharing, freedom of information legislation.

2. Additional inhibitors are failures of public ICT networks, software vulnerabilities, Global Navigation Satellite Systems (GNSS) spoofing, novel attacks (framing attack [attacker causes malfunctioning of on-board equipment of vehicle], Sybil attack [attacker simulates vehicles, e.g. placing ghost vehicles besides real ones] and various other attacks, such as faking identities) [CYS13b].

5.8.3 Gap analysis (tech., policy, regulation, and competences) for achieving the vision

1. Technology and competences: Despite the proliferation and advancement of risk assessment methodologies, most risk assessment frameworks are sector specific without considering the overall picture addressing the spectrum of threats and their various cascading effects that are associated with security incidents occurring from interacting entities, cross-sectoral, cross border interdependencies and massive interconnectivity. A consequence is the tendency to protect themselves from risks relevant to their domain of responsibility, tailored to their particular needs ignoring threats from their supply chain, undertaking disproportional risk mitigation measures narrowing down the possibilities for cost-effective risk mitigation. This gap is very critical in the case of security associated the transport sector, given that they are characterized by significant interdependencies at multiple levels (infrastructural, national/intra-sectorial), interacting with all actors in the complex transportation eco-system and other CIIs (e.g. energy networks, telecommunication networks), thereby they need to treat internal, external and diffused cyber-threats from the whole set of interrelated sectors.

2. <u>Policy:</u> incentives to innovation, incentives to information sharing, programs for the cyber protection of EU assets (Galileo, Copernicus, SESAR, SIS)

3. <u>Regulation:</u> Cyber security directive

5.9 Smart Buildings in Smart Cities

5.9.1 Issues and Challenges

The term "Smart City" provides an umbrella that integrates various types of infrastructure, including traffic light management, smart factories with industrial control systems (ICS) (covered by an own section), power plants (also covered by an own section), public transportation (covered by an own section as well), and smart buildings.

Smart buildings can be considered a key component of today's infrastructure and today's smart cities as they are also a surrounding element for other infrastructure. For instance, a smart factory can be located inside a smart building, which provides physical access control (PAC) and other functionality for the industrial control system (ICS). Being not always a critical infrastructure, a smart building can be basically everything from a small smart home to an international airport, including all its automated components, such as baggage transfer, air-conditioning, smoke removal systems, or heating.

Addressing side channels and covert communications in smart cities is an essential challenge as the feasibility to observe inhabitants, citizens, or employees working or living in buildings as well as elders in Ambient Assisted Living (AAL) is linked to serious threats (e.g. selling electronic healthcare sensor data at the black market). Data leakage protection of sensor data must thus be achieved, what can be done by securing wireless sensor networks (WSN) and other technology used in smart cities, and especially in smart buildings.

One challenge in this regard is the increasing inter-connectivity of smart systems ("systems of systems" within the Internet of Things, IoT) that leads to additional security threats previously not foreseen by the design of these systems.

In an extended scenario, so-called smart building botnets or cyber physical botnets (CPS botnets) are thinkable and feasible [WEN14], i.e. botnets consisting of a high number of CPS like buildings and utilize their sensors and actuators to perform malicious activities. Some of the thinkable activities performable by such botnets are mass surveillance as well as complex scenarios. For instance, a (regional) oil/gas seller might use a smart building botnet to slightly increase the heating levels in his customer's homes each night in order to force them to order oil/gas sooner as they actually were required to [WEN14]. To achieve a stealthy mass-surveillance (which can be used for data leakage as well), it is expected that "network steganography" can serve as an enabling technology [WEN14].

5.9.2 Identification of Technology, Policy and Regulation enablers/inhibitors

5.9.2.1 Enablers

1. Improved standards for network protocols in building automation systems and other components of smart cities such as BACnet, which comprises the most sophisticated security features among the traditional protocols used in the area. Such features should increase confidentiality, integrity, and authenticity of the transmitted data.

2. Increased functionality which leads to easier monitoring and administration of smart city infrastructure incl. smart buildings.

3. Integration of security features which provide security in a way that does not influence the functionality of legacy hardware components, e.g. traffic normalization [SZL14] or passive monitoring approaches.

5.9.2.2 Inhibitors

1. The popularity of old communication standards like EIB or Modbus is a clear inhibitor for the integration of new security features. These protocols enable various security threats while providing (almost) no security features.

2. Some of the communication protocols used in smart cities are not linked to an open specification and cannot even be analysed by the scientific community without performing reverse engineering.

3. Another problem is that legacy systems are still operated and still integrated into "smart" environments – a task that was performed over decades while it is moreover expected that the integrated systems can be operated over decades. These systems are hardly patchable (e.g. providing no functionality for applying patches and moreover do not possess the computing power to integrate state-of-the-art security features).

4. In buildings, know-how about the building automation equipment is getting lost after a building was sold to another party.

5. Means for patching smart buildings and other infrastructure components within smart buildings.

6. Lack of situational awareness in case of a huge number of simultaneously occurring events in smart cities or parts of it (factories, buildings) [WEN14b].

7. Lack of data leakage protection means for smart city environments

8. Decentralized legacy equipment, e.g. many old traffic light management systems are not accessible on-line and can only be configured in field work.

9. Another inhibitor lies in the lack of awareness for security threats by the operators. Especially for smart buildings, operators are – in many cases – facility managers possessing no knowledge on IT security aspects for their operated environment.

5.9.3 Gap analysis (tech., policy, regulation, and competences) for achieving the vision

Patch-ability and security monitoring of smart city environments must be provided. Therefore, novel update mechanisms must be implemented and concepts must be developed to achieve updatability over decades in the context of limited computing power and limited memory on embedded devices such as control units, sensors and actuators.

Side channel analysis of smart environments was up to now only analysed in very specific and academic contexts (e.g. smart metering and some areas of building automation). Research on these topics must be extended in order to provide privacy by design at the infrastructure level.

Operators as well as integrators lack tools and features to integrate security and to keep security alive. For instance, it is uncommon that historic event data (sensor value changes, actuator state changes etc.) is encrypted and that network data communication is encrypted in these environments.

5.10 Industrial Control Systems for Water, Food/Agriculture, Nuclear, and Chemical Operation

5.10.1 Issues and Challenges

Industrial Control Systems, as used in Water, Food, Nuclear and Chemical operations, form a diverse ecosystem with varying components and protection goal. A shared feature of those – as well as similar system in transport, electricity and manufacturing – is that the security maturity level is largely rather low, and many deployed system have no security whatsoever. In the past, this was argued to be acceptable, as these systems where operated as separate islands with no connection to the outside world. With the increasing use of off-the-shelf components, remote maintenance and system integration, as well as increasing realization that air-gapping rarely works in a practical system deployment, those systems are now increasingly exposed to external attacks, and data gathered from commercial companies and national CERTS show a massively increased number of targeted attacks in this domain.

So far, in the industrial control system domain, great emphasis has been taken on safety issues, while security in many systems plays a minor role. While this does give some starting point – the safety culture already accepts investments on product feature that do not add functionality in this sense, and require strict procedures and documentation. At the same time, safety and security often conflict – a firewall or encryption on a communication layer add security, but also add an additional point of failure from a safety perspective. This – and the need for easy maintenance - is also one of the reasons why many systems lack any meaningful access control, which is one of the primary security controls in IT systems.

Patching is a particularly complicated issue in an ICS system. In addition to some components being hard to reach and not prepared for software updates, patches have to be applicable without interrupting the components operations. More critically, the patched version must not introduce any safety risk, for example by changing the real time behaviour of the system or the way it interacts with other components. The assumptions of those requirements are often poorly documented (if at all; the Ariane V explosion[31] is a nice example how undefined requirements led to a disaster even on formally verified code), and sometimes a bug even becomes a feature that the system relies upon. For this reason, any critical patch will need extensive testing on a twin system before deployment. This testing process can take up several months, in which a now known security vulnerability will prevail.

Many ICS related devices tend to be surprisingly unstable, and they have been developed and tested for only a very well defined interaction with the outside world. As a result, even a simple network scan with NMAP can cause such devices to cease operation. This allows an attacker for easy vandalism (crashing random devices on the network needs very little expertise), and complicates defending the network, as some of the defensive tools and architectures as well as frequent patching can themselves interact badly with the ICS Devices.

As for transport, smart grids and related critical infrastructures, the protection goal in industrial control systems is less to safeguard data from theft, but to keep a process going within safe parameters. This does involve physical components, which often cannot easily be interrupted – shutting down a chemical process can take a long time in which the control system needs to operate, and in some cases (such as the cooling of a nuclear power plant) some safety control processes need to be running indefinitely. This makes handling of detected intrusions much harder – even if an intrusion is correctly identified, it is often unclear how to react on it.

As opposed to normal IT components, ICS components usually have a very long lifetime, sometimes remaining in the field for decades. Thus, any security concept needs to be prepared to integrate legacy systems and architectures, and new systems need to be ready for requirements

---

[31] http://sunnyday.mit.edu/accidents/Ariane5accidentreport.html

for an extensive period, without resulting in excessive pricing. An additional problem from this long lifetime is the availability of the suppliers; few suppliers are willing to commit to provide maintenance and security patches for such a long time, and there is a high probability that some suppliers or their subcontractors may be outlived by their devices. One recent example is Windows XP, which is still widely used in the ICS domain, but which is being phased out by the supplier and will have very limited support in the future. Consequently, a number of ICS systems have been hit by classical botnets, i.e., attack programs that had no intention to sabotage a control system, but scan the internet for outdated systems and turn them into spam-bots.

Another legacy are old protocols and standards, which are hard to update once deployed. Many ICS communication protocols support no security at all, and even include safety/debugging features that are counterproductive from a security point of view. Since even standards developed by experts for IT security (e.g., WEP/WPA/WPA2) needed to cycle through several generations to reach an acceptable security level, moving towards a security set of communication standards is a major task.

Finally, the long deployment of devices makes it hard to maintain an accurate network map; over the years, many organizations have lost the overview on devices – let alone software versions – they deploy, and redrawing such a map on the life system is difficult and potentially dangerous.

Due to their nature, many components in ICS systems are constrained in a number of ways, such as available memory, computation power, or user interfaces (This can be very case specific – while some components are essentially full PCs, others are highly optimized for cost and extremely constraint). This restricts the number of available security controls, and further complicates future-proofness. In addition, constrained memory forces programmers to cut corners, while secure code usually includes additional checks, controls, and error handling routines that eat up memory (lack of proper input validation is a common issue in ICS components). Furthermore, many ICS components have little hardware (such as execute-bits) or operating system support for security, making it even harder to produce secure code. This issue is enlarged by the generally low security maturity in the ICS component domain – ICS security rarely got attention comparable to IT security, and few suppliers had a need to implement security coding competence and policies. This is matched with a low maturity level on the procurement side; just as some suppliers struggle to implement secure devices, so do buyers struggle to clearly define requirements for the procurement process.

A separate challenge is the tendency to reuse existing technologies. While in many contexts, this is a wise decision – for example, no one should develop their own block-cipher as an alternative to AES unless there is an extremely good reason as well as available competence – in many cases, IT guidelines are a poor fit for ICS systems.

One of the strengths of ICS systems is the potential for simplicity on the component level – a thermometer needs to only transmit simple data units, and the code base therefore can be kept reasonably small. However, if IT standards are used, the thermometer might end up using a web-server for remote configuration and SOAP as an interoperable communication standard. While this does make the integration into the IT environment easier and allows IT professionals to fully use their expertise, this also dramatically increases the complexity of the device and introduces a large number of new potential vulnerabilities.

Even in a 'normal' IT security setting, performing a proper risk analysis can be a daunting task, and it is difficult to obtain solid numbers. In an industrial control system, this analysis can get even harder. On the probability side, the attacker motivation is quite diverse – while one can get a feeling on the benefit an attacker would get from industrial espionage or a cyber-heist (and thus the effort such an attacker would be willing to spend), the reasons for sabotaging a control system can range from a hacktivist making a point to a nation state actor with practically unlimited budget and patience. On the risk side, it is also not well understood so far what damage an attacker can do – while an act of vandalism is comparatively easy, little work has been done on the difficulty and possibility to perform an attack that causes long term structural damage. This is especially important as the effect of a sabotaged ICS system usually goes beyond the company that got

sabotaged, for example due to a product with wrong properties (in case of a chemical plant), unhealthy food, lack of critical services (such as water supply), or environmental damage.

With ICS systems being increasingly connected, there is also an increasing level of dependencies, many of which are not well defined. A number of control systems, for example, require precise time, which is acquired from the GPS system, which creates a common point of failure over numerous systems. Furthermore, many manufacturers require a remote maintenance possibility, which will massively complicate any security architecture.

ICS systems can reach an enormous level of complexity – the biggest example, the smart grid, covers an entire continent with a system that has literally 100s of millions of components. It is well known that software services of this level of complexity are difficult to execute[32], and therefore execute those in a way that results in a secure system. Digitizing an already complex control system is therefore something that requires a high level of skill in planning and execution, which may not always be available. Furthermore, increasing complexity and reliance on digital components make it harder to revert to a manual backup plan. For the time being, it is still possible in many systems to at least safely shut them down manually, which is a property that is increasingly disappearing.

Besides, the following challenges are listed by the CAPITAL project [CAP14]:

1. Off-the-shelf-software

2. Legacy systems

3. Remote access to data

4. Increasing complexity

5. Delay in fixing vulnerability of ICS

6. Improper input validation

7. Poor code quality

8. Insufficient access control

9. Missing encryption of sensitive data

10. Network security weaknesses

11. Privacy challenges: more detailed information on end-users, increased monitoring of employees (cf. previous section on smart buildings), integration of data, increasing information flows, conflicts between company and consumer interests, trust as an essential ingredient for technology adoption, privacy policies, and influence of end users and privacy policies

5.10.2 Identification of Technology, Policy and Regulation enablers/inhibitors

5.10.2.1 Enablers

1. Technology

   a. Baseline procurement guidelines, clear standards

---

32   http://www.iag.biz/images/resources/iag%20business%20analysis%20benchmark%20-%20full%20report.pdf

b. Security architectures that accommodate a large amount of untrusted devices

c. Increased experience with actual scads attacks

d. Trust in ICS / Management of identity, privacy and trust, Data and Policy Management, and Security and Privacy by Design [CAP14].

2. Policy

a. Information sharing communities, sharing of expertise

b. Compliance frameworks

c. Trainings

3. Regulation

a. Clear liability rules

b. Minimum requirements to create a fair market for security (don't give insecure, but cheap components a competitive edge)

5.10.2.2   Inhibitors

1. Low maturity level

2. Diverse environment

3. Difficulty of proper risk assessment and undefined business cases

5.10.3   Gap analysis (tech., policy, regulation, and competences) for achieving the vision

1. Technology:

a. **Evolvable and fault tolerant architectures.** Given the pace of digitization compared with the current maturity level, it is an illusion to expect an acceptable level of security in the near future; while security by design should be the goal and is the only approach that we can really recommend, in reality security will be designed in an insufficient way. This makes it very important to deploy systems that can evolve and improve over time, and grow the security level over time. Given the long lifetime of the systems deployed now, this needs to be built into the systems deployed now. Furthermore, it is necessary to establish an appropriate monitoring infrastructure to both react on incidents, and to be able to learn from them to harden the system in the future. Finally, systems need to be able to tolerate some level of device corruptions without a catastrophic failure, and to gracefully degrade if the processes cannot be operated properly anymore

b. **Zoning.** Zoning is an important tool to limit the effect of an intrusion, and to manage the complexity of the system (or the system of systems). As the primary thread here is a hazardous failure rather than information leakage, the classical zoning models will need to be improved upon.

c. **Testing Frameworks.** Security testing is not yet a well-defined part of an ICS Security strategy. While individual robustness tests and certifications exist, and some devices undergo penetration tests, there is a lack of a comprehensive approach that makes the tests efficient as well as thorough. Developing such a testing strategy required a solid set of requirements taking into account the devices usage and potential role in a

hazardous scenario, as well as structured testing approach and potentially a system design optimized for testability.

d. **Monitoring and Intrusion Detection.** Given the difficulty of protecting devices, it is of vital importance to be able to detect a potential attack at an early stage. While there is some activity in SCADA monitoring, there is still a technology gap in terms of optimized sensors, combining physical and data sensors, event correlation for ICS systems, and automated reactions in case a countermeasure needs to be deployed faster than a human operator can make a decision. Finally, good monitoring will give input on where the critical attacks occur, and can be used to more efficiently guide the effort on securing the systems on the long run.

e. **Intrusion Mitigation.** In an ICS system that safeguards processes, reacting on a detected intrusion is a difficult problem; even though the operators know their system is compromised, it still needs to keep running to keep the process safe. The solutions here are very process dependent and will look different for each individual scenario. Nevertheless, a common approach to develop a strategy can be built.

f. **Low resource security.** While some ICS devices are rather powerful, many components lack the resources to apply standard security measures. While some work has been done on low-resource security mechanisms for embedded systems, more effort is needed to make this applicable to the ICS domain.

g. **Non-Intrusive Security.** In safety critical systems, additional components are seen as a new potential point of failure, which makes deployment of security mechanisms difficult; furthermore, adding new components to legacy systems, or adding additional code to a 10 year old controller may not be a feasible option. Non-intrusive security is designed to be invisible to the system it secures, and to avoid affecting operations, network designs, timing, or any other critical factors.

h. **Realistic Attack Scenarios.** For IT systems, the security community has a lot of experience with realistic attacks. Penetration testers and white-hat hackers know how to execute successful attacks, and log files from exposed systems give a wealth of information on practical attack vectors. For ICS systems, this experience is lacking – few testers specialize on those systems, and little public data on real attacks exists. Data sharing on real systems as well as strategic use of honeypots can fill this hole, and help tuning the defensive approaches to real attacks.

i. **Malware.** Malware targeting embedded devices, ICS, or vehicles: With the ongoing trend to connect things, whether it is to the Internet or different devices together, and to include IT components in a magnitude of things (e.g. Internet of Things, Connected Car) malware authors will attack different kinds of targets. Thus, we need to research detection and analysis capabilities for malware running on embedded devices, ICS or vehicle components.

2. Policy

a. **Documentation.** Many ICS systems suffer from undefined external dependencies, requirements, assumptions, Interfaces or other features. This should be required for all parts of the production chain, i.e., device manufacturers and their suppliers, integrators, and the system operators.

b. **Simplification.** By using IT technologies in ICS systems, the level of complexity is often increased to critical levels. While it is difficult to encode this in a policy, it should be tried to keep systems and components as simple as possible, rather than using the multipurpose tools developed for IT applications.

c. **Dedicated Standards, Requirements, Best practices, Assurance Scheme.** There is a lack of standards to certify or develop against in the ICS area. While some standards are now starting to be deployed (such as ISA99/IEC 62443), a more solid and broader framework of requirements and standards is needed to help operators buy and vendors to implement proper security guidelines.

d. **Testing.** Many devices in the field fail even the simplest security tests. These tests should be performed before devices are deployed (preferably by the vendors themselves), and all components of a critical system should undergo a thorough testing mandate.

e. **Training/Workforce development.** Security expertise is required on all levels of the value chain, from the embedded system programmer to the system operator. Currently, there are few universities with programs that include control system security, as well as few on-the-job training programs.

f. **Information Sharing Frameworks.** Given the low level of experience in the field, it is important for the participants to learn from each other. For most ICS systems – at least on the operator side – security is not a competitive differentiator, so sharing within the community is a possibility without endangering business goals. One should note, however, that resources need to be provided to enable efficient sharing; incidents and experiences need to be properly processed to generate the sharable information, and time needs to be dedicated to disseminate and make use of the information. Furthermore, an effective sharing program does require building a trusted community, which needs itself needs maintenance through workshops, visits, etc.

3. Regulation

a. **Handling of Critical Infrastructures.** While the risk of the failure of a critical infrastructure is a risk for society, the cost of protecting them are often burdened onto the infrastructure owner, and sometimes strictly regulated (in the case of a natural monopoly). Mandatory security standards and procedures for such infrastructures can create a business case for an acceptable level of security. Developing such standards is a non-trivial task – it needs to take into account the state of the art now to avoid overburdening the operators and vendors, be reasonably cost effective, measurable, and needs to avoid motivating operators to try to elude the standard (according to Anderson [AND10], the high security requirements of the NERC CIP guidelines for power-plants with black start capabilities caused plant owners to remove those capabilities, leaving them with lower requirements and the entire grid more vulnerable.

b. **Enforcement.** While some good security guidelines exist, they are rarely enforced; both European and many national legislations restrict themselves to a non-committing set of recommendations. A stricter framework of enforcement is required to create a business case for security.

5.11 Public Administration and Open Government

5.11.1 Issues and Challenges

Public services are at the core of modern societies, and their availability and trustworthiness is a key enabler for economic growth and social innovation. Innovation in Public Administration is influenced by different drivers, such as the necessity to cut costs and to "do more with less", the rising expectations of citizens with respect to participation and openness of public processes and

data, the pervasive availability of mobile devices which represent an ubiquitous entry point to services, the mass usage of social media, and the obsolescence of old legacy systems versus the growing trend toward cloud-based ICT infrastructures for Governments.

All in all, governments must engage with the wider public and follow the **open government** principles in order to "make the services more user-friendly and effective, improve the quality of decision-making, promote greater trust in public institutions and thus enhance public value" [EC13], but at the same time they have to cope with strong economic constraints, which require the conception of new sustainability strategies and the reuse of best practices and solutions across all governmental levels.

The key role played by ICTs in such transformation is both a fundamental enabler and a source of issues. Indeed, for example, digitalization of public services and mobile government (mGovernment can be seen as the extension of eGovernment to mobile platforms) on the one hand help improving efficiency of the back-office and provide users with better and ubiquitous services, and on the other hand increase the attack surface and causes new security issues and privacy concerns, including distributed denial of service, identity thefts and information leakage.

5.11.2 Identification of Technology, Policy and Regulation enablers/inhibitors

5.11.2.1   Enablers

1. According to [CAP13] future governmental cloud infrastructures are a very appealing target for *malicious hacktivists*, since they represent a "single point of failure", and a successful attack can potentially give access to a high number of agencies. However, since the security countermeasures deployed in data centres are quite high, external attacks that aim at stealing sensitive data or at mounting Distributed Denial of Service are not very likely to be successful. Indeed the security level of future cloud infrastructures is likely to be much higher than the one implemented by each single Public Entity, since they will be operated by personnel highly skilled on cybersecurity, which is not the case in the vast majority of Public Administrations.

2. Citizens will have the means to access and manage (including grant access to any third party), from a single point, their data and to adapt public services to their specific needs and to their specific context. Moreover, since data will be managed in a unique place, it will be possible to solve problems of redundancy and scattering of information across Public Administrations, thus improving accountability of the services.

3. Increasing diffusion of mobile devices that enable m-government (mobile government).

4. Establishment of effective and scalable identity management frameworks.

5.11.2.2   Inhibitors

1. Public Administration is made of many entities, with many people with different capabilities and levels of awareness about security threats, each one running an entry point to the ICT infrastructure. It is thus very difficult to ensure a measurable and reliable enforcement of security policies.

2. Resistance to change by PA employees may be an obstacle to the diffusion of best practices for preventing cyber attacks.

3. There is a lack of methods and tools to specify and manage security and protection of data and information, beyond that of the underpinning ICT infrastructure.

4. New ICT channels such as smart TVs, mobile devices and other smart devices are multiplying the number of entry points for attackers and need different countermeasures with respect to traditional web portals.

5. Current ICT infrastructures, especially in the local PAs, are based on old legacy systems that can be hardly integrated with new security features and that do not support any open specification. Moreover there is a high risk that know-how about security in the systems gets lost when the system provider changes (vendor lock-in often implies unavailability of the necessary documentation to manage security).

6. Operators often are not specifically trained on security threats. Especially for front-office operators, this results in very high risks for data security and privacy protection in their daily-operated environment.

7. The obsolescence of governmental web applications is the cause of widespread vulnerability to XSS or SQL injection. Europe has the highest ratio of countries vulnerable to either XSS or SQL injection. More than 90% of European e-Governments have a vulnerability [NIS14].

5.11.3 Gap analysis (tech., policy, regulation, and competences) for achieving the vision

Achieving the vision of an open government that is centred on citizens and that is able to leverage ICTs to make public services more effective and improve participation, collaboration and transparency, has a very strong impact on security and privacy issues and requires different type of research actions.

As to data protection and ownership, research must be done in order to give users full control on their own data and let them directly care about their accuracy and set individual access control rights, thus preventing data leakage and the multiplicity of a user's identities on different systems.

Threats to resilience of governmental ICT infrastructures and services are reinforced by the lack of interoperability and common security standards. There is the need, at all governmental levels, and with the participation of private entities, individual citizens, and NGOs, to develop and put in place ad-hoc standards, policies and regulations and to share best practices from both the public and the private sector.

PAs manage a very wide spectrum of privacy/security relevant data (from data of public interest which are to be identified, prioritized, aggregated, extracted and opened, to highly sensitive data that require privacy by design approaches to the development of transactional services), each one with specific requirements and specific cyber security threats. This results in the necessity to address data protection and security through in an incremental and proportional way, provided that there is always a trade-off between increased security and usage, and that PAs must optimize their resource investments in this strategic area [AND11].

Finally, end-users education is one of the issues that has to be constantly addressed in the future, beyond purely technical aspects. According to [AND11] "*Human behaviour, whether rational or not, lies at the core of cybersecurity".* Human factors play an important part in most attacks. This is due to the high complexity of the internal systems and overall lack of security expertise –especially considering modern attacks-, and lack of strong understanding about the organisation's "sensitive" data [CAP13].

5.12 Healthcare Sector

5.12.1 Issues and Challenges

The massive trend towards seamless system and data interconnection, mobile services, smart devices and data analytics has already started and will lead to revolutionary changes in health care and nursing.

Healthcare system is evolving during the last years to address the new challenges deriving from the new social and economic conditions Europe is experiencing: citizen aging, more and more increase of chronic disease, overlap between health and social problems, new family models and the request for a drastic rationalization of the healthcare costs.

To meet these challenges, the European countries are drawing the priorities that should drive the development of their Health Systems and that should be based on:

1. Citizens empowerment easing the respect and adoption of healthy lifestyles aimed at a correct prevention of the chronic diseases and, as a consequence, finalized to address the goal of an healthcare systems spending review

2. Reinforce the community care and its integration with the mere hospital care (integrated care) are enablers to put the patient at the centre of the Healthcare system and benefit in this way of a better management, for instance, of chronicity, physical inabilities and new family compositions.

In this scenario, the IT will play a relevant role enabling eHealth for citizens empowerment and eHealth for integrated care. Specifically, to address these two aspects which are strictly related each other, it will be necessary to move toward a complete and deep digitalization of all the healthcare levels which is a precondition to put the citizens / patients in the position to exploit and use all the information – shared also with the healthcare and social institutions – necessary to enable the self-management of cares and preventions. All this will be possible thanks to infrastructures enabling the hosting and sharing of an increasing amount of clinical data following increasing standards of reliability and security.

5.12.2 Identification of Technology, Policy and Regulation enablers/inhibitors

5.12.2.1 Enablers

The new technologies will be a crucial factor to master the challenges of an ageing society, but will also foster higher level health care through e.g. novel patient-centric therapies, improved prevention services and disaster management.

1. **Patient-centric health care**: systematic interaction of domain experts across institutions, e.g. through virtual boards (e.g. for patients with chronic or multiple diseases), use of bio-informatics data analytics for personalized drugs, integration of patients into therapies fostering patient empowerment

2. **Novel and improved health services**: surgery robots, world-wide monitoring of medical treatments for high quality medical treatment, real-time disaster management for optimal distribution of emergency resources, real-time assistance for chronic diseases (e.g. allergy patients), telemedicine services for optimal distribution of expert knowledge, controlled worldwide use of antibiotics to cope with antibiotic resistance of bacteria, worldwide surveillance of epidemics

3. **Prevention and Assistance**: Real-time surveillance of health data through smart devices (e.g. measuring blood pressure, consumed kilocalories, blood glucose, etc.), individual risk profiles, real-time detection of dangerous pathogens, smart assistance for disabled and elderly people (e.g. smart guidance for blind people, smart prostheses and or theses for people with mobility impairment)

Moreover, these additional enablers could be determined:

4. The citizens will be provided with apps which will share a unique bunch of clinical information and they will be tailored for specific target users, for well-defined activities on certain devices and in given usage context;

5. All the information will be managed by a unique and enriched Electronic Health Record which will overcome the current problems related to the scattering of the information and will be the pivot for the coordination between citizens and National Health Systems, clinical and social private providers;

6. The increasing interest of the citizens towards solutions enabling the mobile-health (m-Health);

7. The possibility to put into communication daily and 24/7 citizens with clinical and social staff;

8. Contribute to the definition of standards on the topics related to e-Health and m-Health.

5.12.2.2   Inhibitors

The risks related with such vision are:

1. Legislative and logistical conditions that can cause failure in the federation healthcare systems with the consequence of a partial or null management/ exploitation of the information available;

2. The absence of supporting legislations and guidelines;

3. Lack of co-funding initiatives;

4. Scarce attitude of the clinical and social organizations to invest on e-Health.

The two prevalent inhibitors are costs and quality concerns. Safety, security and privacy are predominant quality aspects of the new technologies. New intricate attacks may arise for the new kinds of IT systems, affecting individuals but also large parts of the population.

5.12.3   Gap analysis (tech., policy, regulation, and competences) for achieving the vision

The combination of interconnected cyber-physical systems with manifold potential vulnerabilities and complex data analytics services requires new generation safety and security measures. For instance, personalized drugs or worldwide antibiotics control cannot be tackled with today´s security technologies. In particular, gaps arise concerning the coordination of security and safety measures in such world-wide scenarios and the need to drive security measures from a business (i.e. cost-driven) point of view. Privacy issues require a high level of transparency, e.g. by fostering trust through high quality security processes and by empowering citizens to set individual access control rights.

A lot of work is expected to be done in order to address the described challenges, to exploit the opportunities and to avoid the potential risks. In particular, it will be necessary to work on eHealth solutions enabling the realization of a fully integrated healthcare system involving Electronic

Medical / Social Record (EMR), Personal Health Record (PHR) and the Electronic Health Records (EHR) able to share the data in a coherent, compliant and reliable way.
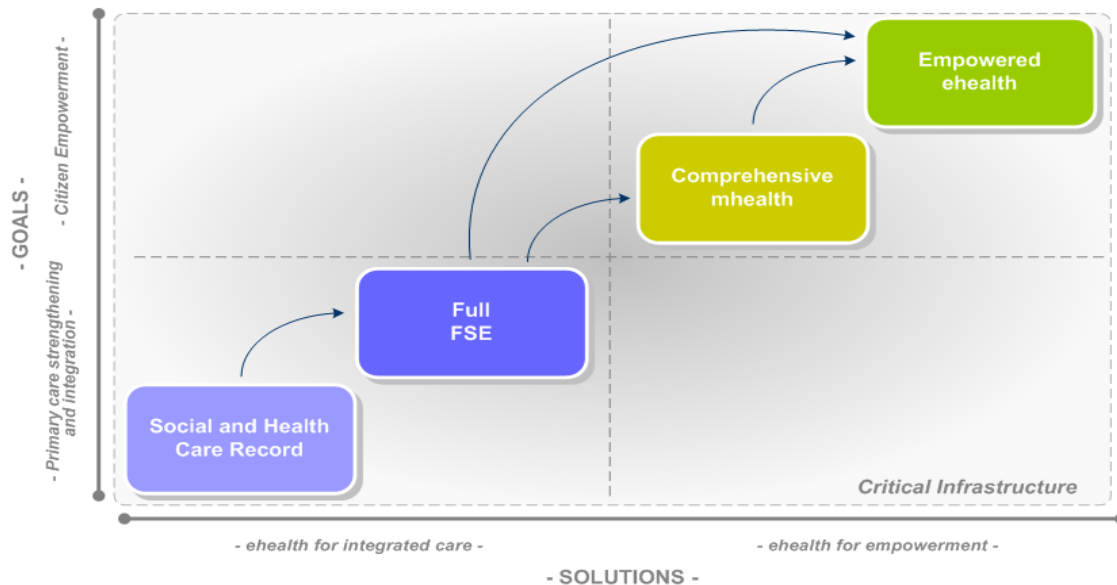
Specifically, it will be necessary to work on solutions for the full digitalization of the community care thanks to Electronic Social Records enabling the citizens to be really at the centre of the system thanks to a full integration between the clinical and social aspects of the care. It will be also necessary to go far beyond the current conception of EHR, a mere static repository of clinical reports in the worst cases neither structured or nor classified, to realize a more dynamic and flexible EHR able to collect all the socio clinical information related to the citizens moving further the current exclusive hospital boundaries. In other words, it will be necessary to create a live repository for the care and assistance pathways, containing all the relevant information for the citizens and the clinical social operators as well as being accessible anywhere, anyhow and anytime. This obviously will enable the creation of comprehensive mobile Health (m-health) solutions enabling the citizens to actively participate to their health management and to share care and treatment pathways (via the EHR) with the medical and social institutions using mobile applications for mostly any task or activity. All this will definitely empower the citizens that thanks to these apps will be able to support, monitor and follow their appropriate lifestyle, pathologies and chronic disease using the information contained the in the integrated healthcare information systems.

To enable all this it will be then necessary to have safe, secure, performing and reliable infrastructures that are distributed and interoperable in a federated approach and such to ensure the storage and management of massive amounts of sensitive data but also able to manage the security and privacy in compliance with the current regulations.

5.13 Automotive / Electrical Vehicles

5.13.1 Issues and Challenges

Intelligent transportation systems (ITS) promises to improve the safety of drivers, e.g. by reducing road accidents, convenience, e.g. with improved cloud and mobile devices connections, and supports new applications, e.g. electric vehicle charging. Therefore the emergence of ITS affects the design of both, the communicating vehicles and the cooperating infrastructures.

Beyond classical features on modern vehicles which include a high number of interconnected embedded control units and advanced multimedia systems, future vehicles will not only have embedded control units (wired and wireless) connections and access to social network, e-mail, in-

car apps, and so on. Exploiting the rising "*vehicle-to-vehicle*" and "*vehicle-to-infrastructure*" paradigms (grow up to 210 million by 2016[33]); future vehicles will also have multiple inter-vehicle connections as well as (wireless) networking with other vehicles and non-vehicle entities such as charging stations and traffic lights. The resulting interconnectivity increases attack surfaces and their damage potential. These technologies offer great benefits, but they also bring new risks for users today, becoming critical for both quality and security performances. Specifically, the future "connected" vehicles will be considered as a mini-network of ubiquitous embedded and external systems that can be hacked, increasing attack surfaces and their damage potential.

Exploiting automotive domain weaknesses that are typically caused by physical accesses, malicious attacks, manipulations and vulnerabilities due to access via infotainment or remote access based exposures, may now enable to attacking the car using the infrastructure or attacking the infrastructure using the car. The damage of such attacks could be catastrophic for car manufacturers, ITS providers and service users, in terms of security and safety.

The fact that vehicles were not originally designed with a set security requirements to fulfil is exacerbating the challenge of providing appropriate countermeasures. The example of the Internet shows how difficult it is to integrate security in a running ecosystem. Most of the vulnerabilities could have been largely avoided by correct construction methodologies.

Due to safety criticality and the vital role of vehicular and transportation systems, in personal, business, government, energy and economic affairs, leaving security as an afterthought is disadvantageous. However, since legacy protocols and hardware take a long time to change, for present and pending vehicle generations, security afterthoughts maybe the only practicable choice.

On one hand, many challenges arise due to the increasing system complexity as well as new functionalities that should jointly work on the existing legacy protocols and technologies; such systems are likely unable to warrant a fully secure and dependable system without afterthoughts. On the other hand, challenges arise due to the escalating number of interconnections among systems from various natures.

The interplay between security and safety issues can only increase if one also considers the future wide adoption of autonomous cars.

From a societal point of view, the customer's expectation in secure and up-to-date software is rising. The consumers, indeed, will benefit from improved security through better prevention from increased malicious attacks and improved comfort.

Another aspect coming along the required collection of data to run ITS applications is the privacy of the users. Current laws/standards in the EU are partly addressing ITS privacy issues (e.g. ETSI TS standards), but privacy of users in community based ITS services are not addressed. An example of such an application is community-based navigation systems. Confidentiality has also to be taken into account to prevent eavesdroppers from accessing the available data. Privacy-preserving intrusion detection and protection against malicious software to envisage on in-vehicle computing devices (e.g., smartphone, tablet, ECU) has to be addressed. Existing solutions for the communication, as well the contained data, i.e. some container formats including the new software, have to be evaluated and their applicability have to be verified, taking into account the security threats of the automotive world, to ensure that the proposed architecture will be up-to-date against current and future threats, and assess the maturity of the security countermeasures.

Following challenges are listed in [KOU13, MUS13]:

1. Model-based automotive security

2. Temporal models and constraints

3. End-to-end secure & reliable integration

---

[33] https://www.abiresearch.com/press/210-million-connected-cars-by-2016

4. Security validation and testing

5. User privacy in community based applications

6. Multiple identity management of the same entity for various services

7. Privacy-preserving intrusion detection and protection

5.13.2 Identification of Technology, Policy and Regulation enablers/inhibitors

The following list of enablers and inhibitors was partly created on the basis of Checkoway et al. [CHE11].

5.13.2.1 Enablers

1. EU Standards

2. Innovative cryptographic primitives to enforce privacy at various levels (e.g. pairing based cryptography)

3. Innovative verification tools and methods to enforce security at various levels (incl. formal methods for mission-critical subsystems)

4. Secure Ad-hoc routing protocols for car2car communication

5. Improved in-car communication security for bus systems (e.g. CAN bus)

6. Growing customer's expectation in secure and up-to-date in-vehicle software

7. A systemic approach driven by automotive requirements

5.13.2.2 Inhibitors

1. National laws restrictions

2. Proprietary protocols and mechanisms

3. Insecure RFID car keys

4. Insecure electronic and connected components, including telematics, heating, air-conditioning, antilock braking system, radio (and included components), engine control system, airbag control system, and others.

5.13.3 Gap analysis (tech., policy, regulation, and competences) for achieving the vision

1. To develop a new set of technologies for overcoming cyber-attacks starting from the results achieved on mechanisms for fighting botnets. These mechanisms still need to be enhanced to become systemic from automotive requirements point of view. Moreover, the security risks linked to the increasing use of mobile devices need to be taken into account as customer's mobile devices connected to the in-vehicle systems are in fact already a reality. This requires enhancing existing software components to integrate them into a reliable and secure in-vehicle system. For example, technology such as OTA (Over the Air Update) that is facing a growing market demand is enabling the upgrade of cars' existing HW with new SW releases. Since this upgrade of safety critical and not-safety, critical vehicle ECUs

(Electronic Control Unit) is Internet based, further research is needed for preventing malicious attacks or manipulations and avoiding any SW related vehicle recall campaigns.

2. Improving RFID communication and improved vehicle anti-theft systems (VATS)

3. Increasing the barriers for surveillance of cars and drivers via data leakage protection (DLP) for vehicles

4. Introducing means for easy-patchability of vehicles or alternative methods to manage software security of already sold vehicles

5. Increasing awareness and competence in the handling of security-related threats at the manufacturer-side as well as for mechanics (e.g. enabling them to easily perform software upgrades on cars)

6. Research for manipulation-safe on-board components and functionality, including speedometer, steering, braking, and acceleration[34]

7. Hack attempt detection (IDS), prevention (IPS), and response (IRS) systems for all electronic components within the car

5.14 Insurance

5.14.1 Issues and Challenges

These paragraphs suggest that insurers, over the next years, will deal with new personal data coming from sensors, increase the usage of cloud solutions and look after an emergent cyber insurance market. The cybersecurity, privacy and trust consequences of the aforementioned technology driven developments are also pointed out. Core insurance processes (i.e. risk pricing, reserving[35] and claims handling) are the focus, while asset management, finance, marketing and sales are not specifically considered. Ordinary cybersecurity management is not considered either.

Insurers have traditionally priced risks based on risk factors. For example, Motor Third Party Liability (MTPL) coverage is traditionally rated according to variables such as age, territory, vehicle type and previous claims history. Health insurance rates may depend on age, gender and medical history. There is a growing consensus [PWC12] that the increasing use of mobile sensors will improve the way certain risks are priced by insurers, making insurance rates closer to the underlying risk drivers. Data coming from so-called black boxes are already being used within MTPL tariffs, which in some countries start to be based on vehicle usage and driving style. "Mobile health" is also expected to make health insurance rates more and more based on lifestyles. The shift towards more risk sensitive prices, driven by increased data availability, means that insurers will collect and analyse a larger amount of data, mainly personal. Previous examples refer specifically to individual risks, even if there is evidence that mobile data may improve commercial insurance pricing as well. The use of new data by insurers brings about challenges, among which people awareness, technology user friendliness, assurance of security and privacy, and discrimination of people based on technology skills and privacy preferences.

In addition, further attention to legal issues is required regarding the use of sensor data by insurers. For example, while age and territory have a clear legal meaning, the validation of data originated from mobile devices could be problematic. Device reliability and data attribution require attention.

---

[34] http://resources.infosecinstitute/car-hacking-safety-without-security/

[35] Reserving is the process of setting aside the amount to fulfil insurance obligations and settle all commitments to policyholders and other beneficiaries arising over the lifetime of the portfolio (source: www.iaisweb.org).

Similar challenges arise from the use of sensors to ascertain events that trigger indemnity payments. Along with the authenticity of collected data, the question lies on the level of cybersecurity needed to make the collected data valid.

Solvency II, the new prudential regime [ED09] that will enter into force in 2016, can also influence the use of technology by European insurers. The new principles according to which reserving and capital modelling should work under Solvency II require higher computational power and larger storage capacity than the previous solvency regime. Because of the aforementioned availability of more data and the need to implement new models, both to analyse the large sets of data itself and to deal with the new prudential regime, the insurance industry might also use non-private cloud solutions more. Challenges stemming from the use of the Cloud include interoperability, data security and privacy, and cross-border data handling.

The previous paragraphs have been drafted assuming that, under the 2013/0027 Proposal Directive, insurers are categorized as users rather than "market operators" (i.e., in short, providers of information society services or operators of critical infrastructures).

Another important topic rapidly gaining attention is insurance of cyber risks. The insurability of the network and information security itself has been debated by institutions and scholars [BIE14]. Measurability is necessary for a risk to be insurable, since rates are built upon loss frequency and cost. However, existing actuarial models cannot rely on historical loss data, since the quantity of historical data is scarce and its homogeneity is compromised by continuous technological advances. The lack of reliable models to estimate the value of loss / stolen data also prevents the reliable evaluation of losses.

Next to the difficulty to acquire data for reliable risk analysis, insurance of cyber risks faces a number of other difficulties. Among them information asymmetry and correlation of risks are, probably, the most important ones. Information asymmetry is impossibility of one party (usually insurer) to get complete knowledge about the other party (usually, insured). Security managers of IT systems are reluctant to share the information about the applied security controls with third parties and even less eager to share the information about occurred breaches. This makes hard for insurer to separate high risk and low risk organisations (averse selection problem) resulting in an inefficient pricing strategy. Partially, new regulations for mandatory disclosure of breaches (e.g., European regulation 2012/0011 "on the protection of individuals with regard to the processing of personal data and on the free movement of such data", which has passed the first reading) may solve such problem. Another problem is that for IT it is not enough to just install certain controls, but it is required to maintain them properly. Being insured, many organisations may start feeling reluctant to invest in proper maintenance of security controls, since the losses in case of a breach will be covered by insurance anyway. This situation leads to another type of information asymmetry problem, called moral hazard. Thus, there is a need for models which will incentivise the insured companies to continue investing in security.

Cyber risks are highly correlated because of the monoculture of used technologies, i.e., the same attack surface, which can be exploited in a similar way (e.g., by worms). Models for computation of correct premiums and coverage must consider this correlation. Moreover, outbreaks of the correlated breaches impose heavy burden on an insurer. In other insurance markets such problem is solved with geographical distribution of insured organisations (e.g., in case of earthquake insurance) or with re-insurance of high losses. Note that in cyber-insurance case, technologies are similar in different geographical regions, and most worms are equally dangerous for US as well as for China or Germany. Re-insurers for cyber risks do not exist yet at all. This leads to the policies with large amount of exclusions and high prices. More accurate models, e.g., which use diversity in technology, may help to solve some of these problems.

5.14.2 Identification of Technology, Policy and Regulation enablers/inhibitors

5.14.2.1 Enablers

1. Individual awareness of the nature of collected data and how it is used

2. User friendly control over third party usage of personal data

3. Assurance of security and privacy

4. Identity management and frameworks to enable the correct attribution of sensor data

5. Assurance of sensor output

6. Interoperability of cloud solutions

7. Cloud data security assurance

8. International standards and cooperation on data security and privacy

9. Cooperation on security data sharing

10. Regulations on mandatory breach reporting

11. Granular risk definitions and availability of loss statistics about information security failures

12. Models to quantify the economic value of personal and business data

5.14.2.2 Inhibitors

1. Divide of people not at ease with technology or concerned with privacy

2. Difficult internal threats mitigation for cloud solutions

3. Evolution and dynamism of technology

4. Intersections among national security, espionage and cybersecurity

5. Limited transparency on security failures causes and losses

6. Correlated risks

7. Information asymmetry

8. Lack of re-insurers

5.14.3 Gap analysis (tech., policy, regulation, and competences) for achieving the vision

5.14.3.1 Technology

1. Methods to verify and validate sensor data related to a person would enable new, data driven, approaches to risk profiling. Verification methods could range from friendly Biometric Fingerprinting Systems to algorithms able to recognize individual styles (e.g. of walking or driving). Similarly, methods to authenticate sensor data related to machines will

be valuable when the Internet of Things becomes a reality. The concept of a "register of things" might even be developed.

2. Joint research by technology specialists and insurance experts would help identify the data needed for cyberinsurance pricing and so facilitate the establishment of a cyberinsurance market. Cyber risk maps for different technology platforms (including Cloud) and insights on IT industry perspectives as these platforms become more interlinked would also be beneficial [TOR14].

5.14.3.2 Policy and Regulation

1. Secure hubs for personal data might help people understand and easily control at once what data they release to different parties, including commercial entities. These hubs, either sector specific or multipurpose, would also allow people to view/amend the data and change permissions.

2. Regulations on mandatory breach disclosure. These regulations should specify the cause of security failure and its effects in order, on the one hand, to more efficiently combat the spread of cyber threats and, on the other one, to help an insurer to assess the cyber risk level of an organisation correctly.

The need to develop frameworks to appraise the value of information has already been clearly raised by ENISA [ENI12] in considering which factors are hindering the development of a cyberinsurance market.

5.15 General Privacy Aspects for all Infrastructure Sectors

5.15.1 Issues and Challenges

Provide a privacy-preserving cyber Infrastructure that people will learn to trust and use for their benefit and according to their expectations.

5.15.2 Identification of Technology, Policy and Regulation enablers/inhibitors

5.15.2.1 Enablers

At the time of this writing at least 2.8 Zettabytes, that is 2.8 trillion of Gigabytes, of data are available on-line[36]. We expect that over the next few years this amount will significantly increase. Driven by the increasing penetration of the Internet and the ubiquitous connectivity of most devices, data collection approaches will result in a corpus of data much larger than ever before. Stored under the umbrella name of "big data", and mined using modern "Data Analytics" approaches, we expect that these data have the ability to contribute to science and prosperity of human kind.

5.15.2.2 Inhibitors

We expect that a number of actors will try to adversely exploit these data in order to serve their own agenda.

---

[36] http://www.technologyreview.com/news/514351/has-big-data-made-anonymity-impossible/

1. **Attackers**, for example, may manage to gain access to such data for financial and political profit.

2. **Governments** may also attempt to acquire these data so as to gain an advantage against their enemies or even to collect intelligence about their citizens.

3. Various **corporations** may also attempt to gain access to the data so as to increase their profit.

5.15.3 Gap analysis (tech., policy, regulation, and competences) for achieving the vision

1. **Big data collection awareness**: One might be tempted to underestimate the impact or even the coming of the big-data era. One might be tempted to believe that such data will never be collected in large scale or that will immediately be deleted if collected. Unfortunately, data are collected and will probably continue to be collected. Given that an increasing percentage of our lives is becoming digital, it becomes difficult *not* to collect data. We need to find a framework to use these data for the benefit of their users.

2. **Provide regulation to protect the end user**: The fact that data are collected does not mean that they should be freely available to anyone who wants them. The collectors should be responsibly operating under a framework that will prohibit them from sharing the data without the control of the end user. Even more, the collectors should operate in a legal framework that will protect them from unreasonable data collection requests. Finally, collectors should even have the legal and financial capacity to challenge requests for the data if they do not seem to fit the end users' expectations.

3. **Transparency and Accountability**: Once data are collected it is not clear how they are used and for which purposes. Regulation should be put in place so as to discover inappropriate use of data and hold these organizations accountable for any such use.

4. **Advance Privacy Enhancing Technologies**. More Research is needed to improve Privacy Enhancing Technologies including anonymity, privacy-preserving web access, etc. More research is also need to store data in a privacy-preserving way.

5. **Promote awareness for Privacy Enhancing Technologies**: People, and especially young people should be encouraged to value and protect their privacy in cyberspace, much like they value and protect their privacy in the physical world.

6 Cross analysis

6.1 Introduction: Purpose and Scope

The SRA methodology as described in section 2.2 is based on the identification of issues/challenges, enablers/inhibitors and research gaps from three different viewpoints, which are represented by Areas of Interest (AoI):

- AoI#1: Citizen Digital Rights and Capabilities (Individual layer): ensuring that, as ICT is used by people, it addressing rights, needs, wants of citizens as individuals – in a sense this looks at the trust problem from the 'demand side'. Citizen's rights and needs and wants (rights and societal norms) have to be met by the organisations as to how they behave online, the risks they are exposed to and how they use and manage digital data.

- AoI#2: Resilient Digital Civilisation (Collective layer): Digital Interconnected Society – ensuring that digital institutions of society are as trusted in their digital forms as they are in physical form, in a way this is the 'supply side'. Organisations operate under a whole series of obligations – regulation, contracts, societal norms, and to manage risks, ensure security, and handle information securely and respecting fundamental rights of the customers/citizens.

- AoI#3: Trustworthy (Hyperconnected) Infrastructures (infrastructure layer): ensuring security and continuity of infrastructures and systems – so that the economy and institutions can operate. Infrastructures and systems need to be secured against threats and failures to ensure the continuity of institutions and services they support.

The AoIs are interdependent, since they look at the same artefacts, technical and non-technical concepts, but respect priorities of different stakeholders, namely individuals, societal entities and groups including businesses, and infrastructure providers operating the foundation of the information society. Figure 1. Explains their relation as well as the priorities that are driving the respective viewpoints.

The purpose of this section is to analyse the different views given by the AoIs with respect to their commonalities, in particular, research priorities that have been identified by all different views, and differences. Such differences do not only include immediate conflicts, where one topic is viewed as priority by one AoI, but as being of less relevance by another AoI – in fact, such conflicts currently have not been observed --, bur also refer to differing priority or relevance ranking, including topics that have been mentioned by one AoI, but not by another. The cross analysis derives key findings from the analysis providing input to the definition of future European research priorities that respect the importance of all three AoIs.

Commonly identified needs indicate high global relevance, importance and impact of a topic which should translate into high priority research activities, while differences are indicating the need for engagement of specific communities.

On top of the findings of the AoIs, additional input streams for the cross analysis include the research landscape document, the business and innovation deliverable, and the feedback received from NIS Platform WG1 and WG2. Since the emphasis is on identification and analysis of future research priorities, focus of the analysis are the "gaps" sections of the respective deliverables as well as the recommendation for research priorities provided by WGs 1 and 2.

The structure of the section is as follows: section 6.2 contains short descriptions of commonly identified research and innovation priorities, section 6.3 reports on observed divergences, while section 6.4 contains additional key observations summarising the findings in order to provide guidance for future research programmes.

6.2 Commonalities

This section highlights the topics that have identified as commonalities among the main AoIs whose further investigation would be beneficial.

6.2.1 Assurance

6.2.1.1 Context

The "quest for assurance" in cyber security is a long-standing issue with many facets and related aspects. It is commonly agreed that, in order to be effective security, privacy and trust considerations should be involved from the very beginning in the design of systems and processes (i.e. security/privacy/trust by design). This entails a whole series of activities, including social and human aspects in the engineering process until the certification that the developed systems and processes address the planned security/privacy/trust properties.

In addition to the usual aim of building a secure system, we often need to prove (and offer evidence) that the system is secure. This is necessary also when considering systems of systems, whose security could depend on the security of subcomponents. This assurance and certification steps are very challenging and emerged in several of the AoIs.

The engineering process of the systems should thus take into account those security/privacy/trust/compliance requirements and should consider as well notions of cost and risk in the development process and well as in the system lifetime.

This process of enabling assurance techniques and processes can be definitely eased by regulators. Indeed, the introduction of regulatory actions could ease the adoption of assurance techniques (having a benefit on the overall security level of the infrastructures, systems and products).

It has been noticed that cost and risk are two relevant factors in building and operating security-sensitive systems. The cost of developing security countermeasure should be related to be assets to be protected (and often in the digital world these are intangible). A strong component of any risk management is the capability to predict the current strength of the system. Thus security and corresponding risk metrics are crucial (as other quantitative aspects of security).

Starting from these considerations, residual risk could be managed with other approaches rather than just security countermeasures. A growing area of interest is cyber insurance. This growing business area needs further research on security metrics, security assessment as well as forensic and related technologies for establishing responsibilities in security incidents and attacks.

Overall we may see two extremes from just focussing on dealing with the problem of developing a secure systems thus aiming at avoiding security breaches till the scenario when the focus is on how to insure the exposure to possible security breaches.

We thus recall here several areas that represents commonalities for assurance[37] (although in different flavours) in the findings of the 3 AoIs.

6.2.1.2 Research topics to be addressed

Translating the above findings of the AoIs and the research challenges identified in the research landscape document into research priorities on a finer level of detail, we suggest to structure along

---

[37] NESSoS D4.3 Part II Engineering Secure Future Internet Services: A Research Manifesto and Agenda from the NESSoS Community: Final Release

the dimensions of security / privacy by design, security / privacy validation, and processes. These dimensions should be complemented by research aiming at understanding their relations -- not only technical, but also psychological and economical. The latter is based on interdisciplinary research.

1. **Security / Privacy by Design.** By "security / privacy by design" we understand all methods, techniques and tools that aim at enforcing security and privacy properties on software and system level and providing guarantees for the validity of these properties. Since the required security and privacy properties depend on the system context and the application domain, understanding these requirements and being able to precisely define them is a prerequisite. Hence, **security requirements engineering**, is part of this discipline. In order to come up with practically feasible techniques, emphasis should be on close integration with existing software requirements engineering approaches (like, for instance, those based on UML, but with a stronger focus on automation and modularisation) and the inclusion of risk considerations. The identified requirements need to be formally traceable to security features and policies throughout all phases of the secure development lifecycle, considering the complete system view (which might include assumptions about the context that need to be enforced upon deployment). Research into **secure engineering principles** supports this approach.

2. **Secure (programming) languages and frameworks** establish some requirements by default via enforcing secure architectures and coding. While there is an existing body of research in the field, there are typically good reasons why developers prefer potentially insecure approaches: performance, interoperability, ease of use, etc. The challenge is to provide secure development and execution environments that are up to the traditional environments with respect to these qualities, and still allow the flexibility and expressiveness developers are used to (e.g., including higher order language constructs).

3. While secure languages and frameworks mainly address the issue of software vulnerabilities, many privacy requirements can be addressed by **secure computing** solutions. Research challenges include advanced schemes that allow to execute operations on the data in an efficient way while maintaining a high level of security (e.g., by processing encrypted data or providing differential privacy) and still being practically feasible in terms of performance, key management etc. Such schemes should be flexible enough to allow for scaling security, functionality and performance, as well as providing proofs of the properties achieved.

4. **Security validation** Security validation comprises all activities that aim at demonstrating the security qualities of (specified, implemented or deployed) software and systems. Hence, it includes formal verification, static code analysis, dynamic code analysis, testing, security runtime monitoring, and more. Since all of them have their particular strengths and weaknesses, emphasis should not only be on their individual advancement (which includes increase of automation, coverage analysis, modularisation, soundness, efficiency), but also on the understanding of their complementarity. For instance, promising results have been achieved by combining static and dynamic code analysis, and further combination and interaction of different techniques is seen as a valuable approach towards managing complexity and increasing the quality of results.

5. **Processes** By processes, we understand all approaches that aim at providing assurance for security and privacy properties by defining those activities throughout software and system development, deployment and operation that aim at achieving a desired level of security and privacy. This includes the secure development lifecycle, certification schemes, maturity models, checklists, guidelines, etc. The major research challenge in

this area is to provide practical feasibility (in terms of managing costs and risk) while understanding the exact nature of the contribution to security and privacy of each activitiy.

6. **Metrics** are key to understand the security status of a system under development or in operation. Hundreds of metrics have been proposed, but they still lack a mapping to the actual risks that relate to a particular measurement. Hence, metrics should be derived from risk models and assessments, taking technical and business context into account and adapting to system and context evolution. This contributes to the **quantification of security and privacy risks**, as an ingredient of balancing the cost of security measures and their potential risk reduction.

7. In the long term, such concepts can lead to a viable business model for a **cyber insurance**. Insurance prices need to be set up. This on the one hand needs to measure the security level of a system assessing the current security level and considering how this evolve with the time as well as the capability to prove cyber incidents responsibilities (that connects this area with forensic etc.). Formalization of liability of system produced and service deployed is also a relevant are where investments should be made.

8. **Certification schemes** – including both product and process certification – have shown to be a meaningful approach to security and privacy assurance, in particular being recognised by users as an assurance means. However, many of the schemes suffer from a trade-off between the expressiveness of the certificate and the effort required to achieve a certificate. Hence, investigations into cost-effective schemes (for both suppliers and consumers of systems and services) can boost the value and proliferation of certification schemes.

9. On top of research into the technological dimension of assurance, **interdisciplinary research** is key to analyse the different approaches towards assurance with respect to their feasibility, their economic viability, their social acceptance, and their contribution to the perceived reduction of risk by the customers and users. So far, research has mainly focused on technology and technological governance (e.g., by providing process models for secure software development). Many of these did not find their way into practice because they are considered as being too cost-intensive (in particular, causing large initial investments) and the actual gain in terms of increased customer trust or risk reduction is unclear. Economics, social sciences, legal sciences, psychology and other disciplines can provide valuable insights into the "human side" of assurance.

6.2.1.3 Catalysts for improving impact of research

- Cover the full spectrum of assurance techniques
- Encourage interdisciplinary research on the human and economic factors of assurance
- Encourage research on the interdependence of assurance techniques
- Focus on integration with state-of-the-art techniques for software development and analysis – no separate approach for security / privacy
- Focus on automation of activities to enforce and/or analyse security and privacy properties
- Encourage research related to the cost factor of assurance

6.2.1.4 Timeline

This table lists the research topics and the corresponding time framework when those can be addressed.

Topic / Timeframe	Short (1-3)	Medium (3-5)	Long (5-8)
Security / Privacy by Design		Schemes for focused problem areas	Generic theories and frameworks
Security Requirements Engineering	Requirements specification and elicitation languages for security, privacy and trust	Tool support	Fully integrated security requirements engineering
Secure Engineering Principles	Security Guidelines, focused tool support	Comprehensive methodology and tools, Security IDE	Theoretical foundations and supporting methods and tools
Secure Languages and Frameworks		Secure Programming languages, type systems	Integrated secure development and operation frameworks
Secure Computing	Individual schemes	generic schemes	significant improvements on efficiency
Security Validation	static and dynamic analysis	integrated analysis	integrated analysis based on formal semantic models
Processes		Comprehensive set of security standards approved and established in practice	
Metrics	Security Process KPIs	Security Quality KPIs	

Quantification of Risk	risk metrics	risk assessment frameworks based on publicly available data	
Cyber Insurance			operational insurance schemes
Practical Certification Schemes	lightweight certification		
Interdisciplinary Research		economic models	socio-economic models

6.2.2 Focus on Data

6.2.2.1 Context

A major characteristic of current and future systems and applications, which has been recognised by all different viewpoints as represented by the AoIs, is the ever-increasing amount of valuable data that needs to be properly managed, stored, and processed. Data can be produced by systems as a consequence, for example, of interconnected devices, machines and objects in the Internet of Things, and by individuals as a consequence, for example, of business, social and private life moving on-line, thus including data resulting from observations (e.g., profiling) and data intentionally provided (e.g., the prosumer role of individuals). As the value of data increases, opportunities based on their exploitation and the demand to access, distribute, share, and process them grows. Highly connected systems and emerging computing infrastructures (including cloud infrastructures) as well as efficient real-time processing of large amounts of data (including Big Data methods and applications) facilitate meeting these demands, leading to a new data-driven society and economy.

The collected data often are of a highly sensitive nature (e.g., medical data, consumer profiles, and location data) and need to be properly protected. With data being stored and processed in the cloud, and being exchanged and shared between many previously unknown and unpredictable parties, this protection cannot stop at a single system's border, but need to be applied to the data over their full lifecycle, independent of what system is processing the data, what access channels are used and what entity is controlling the data. Hence, a system-centric view on security and privacy, including, among others, secure devices and infrastructures (cf. sections below), needs to be complemented with a data-centric view, focusing on data lifecycle aspects.

Providing transparency on where data resides, who has access to them, and for which purposes they are being used, together with mechanisms that allow the data owner to control the usage of their data, have been identified by all AoIs as essential aspects of a data-centric view and a prerequisite of a secure and privacy-preserving digital life. While research has already produced a number of relevant contributions (e.g., sticky policies, privacy policies, and techniques for protecting data at rest), many challenges are still open, including enforcement and usability. These challenges

are not only of a technical nature: for example, lack of awareness of the value of data (and what data are actually produced when engaging in digital life) has been mentioned as an inhibitor.

6.2.2.2 Research topics to be addressed

A variety of challenges need to be addressed to take advantage from the availability of large amounts of data in a secure and privacy compliant way. These challenges should include at least the ones from AoIs and Landscape, and cover issues related to the protection of data as well as the use of data for security.

1. **Data protection techniques.** The size and complexity of collected data in most cases leads to the use of cloud technology and to their storage at external cloud-based repositories using cloud-based services, which offer flexibility and efficiency for accessing data. While appealing with respect to the availability of a universal access to data and scalable resources on demand, and to the reduction in hardware, software, and power costs, the outsourced storage may produce the side effect of exposing sensitive information to privacy breaches. The security and privacy requirements then create the need for scalable and well-performing techniques allowing the secure storage and management of data at external cloud providers, protecting their confidentiality from the cloud providers themselves. However, protecting data means ensuring not only confidentiality but also integrity and availability. Integrity and availability of data in storage means providing users and data owners with techniques that allow them to verify that data have not been improperly modified or tampered with, and that their management at the provider side complies with possible availability constraints specified by the data owner. The variety of data formats (i.e., structured, unstructured, and semi-structured) makes the definition and enforcement of such techniques a challenging issue.

2. **Provenance of data.** The impact of data in our daily lives is growing. For instance, it is possible to collect medical data from individuals via smartphones or medical "self-tracking" devices. The collection, analysis, and use of these data allow people to take preventive actions or to take healthy choices. In this and other scenarios, it is important to establish a given level of trust on the data. Tracking data provenance can then be useful for: *i)* verifying whether data come from trusted sources and have been generated and used appropriately; and *ii)* evaluating the quality of the data. The definition of a formal model and mechanisms supporting the collection and persistence of information about the creation, access, and transfer of data is therefore of paramount importance.

3. **Secure data processing.** Distributed frameworks (e.g., MapReduce) are often used for processing large amounts of data. In these frameworks, cloud providers processing data might not be trusted or trustworthy. There is therefore the need of solutions providing guarantees on the correct and proper working of the cloud providers. This requires the design of efficient and scalable techniques able to verify the integrity of data computations (in terms of correctness, completeness, and freshness of the computation results), also when the processing of the data is real-time, and to ensure that data are distributed, accessed and elaborated only by authorized parties.

4. **Operations on encrypted data.** The confidentiality of data externally stored and managed is often ensured by an encryption layer, which prevents exposure of sensitive information even to the provider storing the data. Encryption makes however data access and retrieval a difficult task. The problem of supporting efficient fine-grained data retrieval has recently received the attention of the research community and led to the development of solutions based on specific encryption schemas or on the use of indexes (metadata) that support query functionality. With respect to the use of specific encryption schemas, any function can be, in theory, executed over encrypted data using (expensive) fully homomorphic encryption constructions. In practice, however, efficient encryption schemas need to be adopted. An interesting problem is then how to select the encryption schemas that

maximize query performance while protecting data according to possible security requirements imposed over them (e.g., data should be encrypted in a way that the frequency of values is protected). With respect to the use of indexes, we note that indexes should be clearly related to the data behind them (to support precise and effective query execution) and, at the same time, should not leak information on such data to observers, including the storing provider. Also, there may exist the need of combining indexes with other protection techniques (e.g., access control restrictions) and such combinations should not introduce privacy breaches. The design of inference-free indexes that can be combined with other protection techniques without causing privacy violations are all aspects that still require further investigation.

5. **Query privacy.** In several scenarios neither the data nor the requesting user have particular privacy requirements but what is to be preserved is the privacy of the query itself (e.g., a query that aims at retrieving information about the treatments for a given illness discloses the fact that the user submitting the query is interested in this illness). It is therefore important to design efficient and practical solutions (possibly exploiting the presence of multiple providers for increasing the protection offered) that enable users to query data while ensuring the access confidentiality (i.e., protecting the data the users are looking for) to the provider holding the data. Effective protection of query confidentiality requires not only protecting confidentiality of individual queries, but also protecting confidentiality of access patterns.

6. **Data-centric policies.** When data are stored and managed by external cloud providers, they can be subject to possible migrations from one provider to another one to balance the system load or to perform distributed computations. This migration introduces many challenges with respect to the proper protection of data confidentiality. In fact, each provider can use different security mechanisms and may be subject to different security requirements (e.g., providers operating in different countries may be subject to different law regulations). When therefore data are migrated from a provider to another it is important to guarantee that the protection requirements characterizing the data are still satisfied. The fully distributed cloud architecture introduces however a lack of traceability on the data and makes the correct enforcement of such requirements complicated. To this purpose, we need to define: *i)* a model and language for easily expressing the requirements on the data usage and for regulating information flows among different servers/cloud domains; and *ii)* data-centric policies (i.e., policies attached to the data) that aim at facilitating the enforcement procedure by allowing the access of the security policies anywhere in the cloud.

7. **User empowerment.** For users or organizations there is great convenience in relying on a cloud infrastructure for storing, accessing, or sharing their data, due to the greater availability, robustness, and flexibility, associated with significantly lower costs than those deriving by locally managing the data. Unfortunately, such convenience of resources and services comes at the price of losing control over the data. Although cloud providers implement some data protection features, possibly demanded by legislation and regulations, such protection typically consists in the application of basic security functionality and does not provide the data owner with effective control over her data. This situation has a strong impact on the adoption and acceptability of cloud services. In fact, users and organizations placing data in the cloud need to put complete trust that the providers will correctly manage the outsourced information. There is therefore the need to re-empower users with full control over their data, enabling them to wrap the data with a protection layer that offers protection against misuse by the cloud provider.

8. **Privacy-aware Big Data analytics.** We are in the era of Big Data where the analysis, processing, and sharing of massive quantities of heterogeneous data can bring many benefits in several application domains. For instance, in the health care domain the data accumulating in health records can be at the basis of predictive models that can lower the overall cost and significantly improve the quality of care, or can be used to develop personalized medicine. The application of Big Data analytics, however, can increase the

risks of inferences that can put the privacy of users at risk. We then need to develop techniques addressing issues related to data linkage, the knowledge of external information, and the exploitation of analysis results.

9. **Economic value of personal and business data.** The large amount of data collected, processed, and shared range from personal data (e.g., user-generated content, social data, location data, and medical data) to business data. The economic value of these large collections of data is increasing rapidly as technological innovations are introduced. In this context, both users and organizations should be able to estimate the economy-wide benefits achievable through the analysis of such large amounts of data to find the right balance between the required information and the desired insight.

10. **Highly scalable data processing for situation awareness. To Be Written**

6.2.2.3 Catalysts for improving impact of research

- Focus on solutions compatible with current technologies
- Decouple the use of cloud data management services from the assumption of trust on data management
- Consider different threat scenarios and develop solutions applicable in such scenarios
- Provide owner with full control over their data

6.2.2.4 Timeline

This table lists the research topics and the corresponding time framework when those can be addressed.

Topic / Timeframe	Short (1-3)	Medium (3-5)	Long (5-8)
Data protection (confidentiality)	Efficient techniques for the secure data storage and management		
Data protection (integrity and availability)	Model expressing integrity and availability constraints	Techniques enforcing integrity and availability constraints and verifying compliance	
Provenance of data	Model and mechanisms supporting the life-cycle of provenance information		

Secure data processing	Efficient probabilistic techniques for assessing the integrity of query results	Access control model regulating access and distribution of data and computations	
Operations on encrypted data	Design of inference-free indexes supporting efficient and fine-grained access to encrypted data	Physical design of encrypted data according to operations to be supported and possible requirements on the needed protection	
Query privacy	Practical solutions exploiting multiple providers for protecting access and pattern privacy		
Data-centric policies	Requirements on data usage and data flows	Static data-centric policies	Adaptable data-centric policies
User empowerment		Self-protecting solutions	
Privacy-aware Big Data analytics		Inference-free data analytics techniques	
Economic value of personal and business data		Model and metrics for evaluating the economic gain obtained from the analysis of large collections of data	
Highly scalable data processing for situation awareness			

6.2.3 Secure execution

6.2.3.1 Context

All three AoIs and their ICT based instruments for gaining trust depend on a secure execution environment for the respective software. Such secure execution environments not only includes the execution platforms themselves plus the operative systems, but also the mechanisms (e.g. security supporting services, control and intrusion prevention systems) that ensure an adequate level of security in the execution of all processes. Moreover, it is also essential to approach this topic from a holistic point of view, where multiple execution environments interact with each other due to the delegation and distribution of tasks. If these execution environments cannot be secured, then major problems will arise.

For example, individuals (as addressed in AoI 1) cannot really control the data flows out of their domain, e.g. their mobile phones, if the mobile phone device platform can be manipulated by other parties. The same holds for anybody and any institution that works towards a resilient digital civilisation as described in AoI 2: institutions in a civilisation need to provide reliable and stable behaviour, e.g. when documenting facts (such as a crime scene or the ownership of real estate), making decisions (on any kind of applications) and archiving the respective records for accountability. Any loss of integrity in these processes is an opportunity for manipulation and possibly corruption. If it is easy to manipulate an institution's information processing, the institution's integrity and reputation are at risk. With more and more information being processed outside of secured premises (e.g. by a police patrol using a laptop or smaller device) the need for secure execution environments and corresponding devices is rising. Last but not least many of the trustworthy (hyperconnected) infrastructures discussed in AoI 3 depend on secure execution environments. This holds for institutions in the public administration as well as for other critical infrastructures such as the health care sector, smart grids, and industrial control systems for water, food/agriculture, nuclear, and chemical operation. Secure execution environments are then even a critical factor for public safety.

6.2.3.2 Research topics to be addressed

1. **Secure execution platforms**. In order to provide a secure execution environment, the platforms themselves (e.g. cloud servers, mobile devices) must guarantee the secure execution of all operating systems and services. However, this is not a trivial task. In current paradigms, like cloud computing, the attack surface has expanded, and new risks and threats have appeared. We need to overcome challenges such as malware exploiting and bypassing virtualized environments. Therefore, novel methods for virtualization and compartmentalization need to be investigated. Moreover, personal devices (mobile phones, tablets, etc) will become key players. Thus, the platforms where the mobile devices will be running should be trustworthy. For example, such devices might be based on a secure core that could help the trustworthy engineering process and can also be used for monitoring trustworthiness at runtime.

2. **Operating systems security**. Each application is only as secure as the OS it runs on. As a result, the isolation of applications and the minimization of the attack surface becomes a necessity. The benefits from component-oriented design (i.e. reusability, adaptability) can be brought to operating systems by defining standards to which operating systems

components must adhere. This requires integrating the minimum TCB (Trusted Computing Base) mindset with this software engineering approach, such as only running a small subset of components in privileged CPU modes and running legacy OS components in virtualized environments.

From an implementation standpoint, it is also necessary to find a balance between low-level close-to-the-hardware languages and safe languages that do not suffer well-known vulnerabilities such as buffer overflows. Also, it is important to extend the secure boot and remote attestation techniques to component-based OSs that can be updated at runtime. New patching strategies must cover the upcoming scenarios of highly dynamic, resource-constrained embedded devices such as sensors and control units. Finally, as a transversal concern, it is important to keep HCI (human-computer interface) security and usability in mind.

3. A secure execution environment requires of several **security-supporting services**, such as data protection and secure communication protocols. There are, however, several issues that need further research in this particular topic. For example, the uprising of cloud services calls for enhanced cryptographic techniques that enable encrypted processing, attribute-based cryptography and policy-based decryption techniques, since they are the only way to ensure that data remains opaque in transit, at rest, and during processing and accessible only to those with legitimate access. It is also of paramount importance to address information leaking, side channels and covert communications together with off-the-record properties to encrypted channels, such as forward secrecy and plausible deniability. Another issue is the implementation, in personal devices, of secure elements on top of the operating system. The goal of these secure elements is to protect devices and allow them to protect themselves. For example, devices such as assurance tokens and wallets could verify their respective controllers by an extra communication channel, which demands a portfolio of communication and redundancy mechanisms. Also, secure elements on mobile devices could allow the holder to influence the type of identification information to be displayed.

4. Even if the environment is properly secured, it is not realistic to assume that no successful attacks will ever take place. All the amalgam of interconnected, dynamic systems will not only affect the situational awareness of all entities, but also will open new avenues of attacks, such as cloud-based and IoT-based targeted malware. Just as a body needs an immune system, it is essential to provide **control and intrusion prevention systems** to effectively monitor the state of the environment and react against all kind of (potential) threats - from punctual to severe and continued. The challenge is to create such systems taking into consideration various factors such as the massive amount of event sources, the interaction with related subsystems (e.g. trust management systems, autonomous response systems), and the development of intelligent, adaptable, and interoperable detection and mitigation mechanisms, among others. All of this while aiming to maintain several properties such as scalability, autonomy, usability, fault tolerance, and responsiveness.

5. **Secure Integration**. As multiple systems and paradigms will interact with each other in a distributed and dynamic environment, it is crucial to achieve a full secure integration of all of them. On this topic, several areas need further research. Not only do we need to allow novel technologies to cooperate with each other (using strategies such as compatible protocols or intelligent gateways), but also we need to consider the migration of legacy systems, whose components and protocols are not usually up to the security and privacy risks. Other issues, such as the security and privacy implications of scaling (up & down) storage systems, need further investigation.

The integration with untrusted services and devices must also be carefully considered. Of special interest will be the case of the BYOD (Bring your own device) paradigm. Another important area is the interaction with mobile applications (Apps). They must guarantee privacy and integrity of the information they handle in order to protect the data of their users. Hence, their integrity and compliance need to be protected.

6.2.3.3 Catalysts for improving impact of research

- Cover the full spectrum of threat prevention, detection and response solutions.
- Aim to provide a holistic point of view in the monitorization of the different systems.
- Follow state-of-the-art techniques in the security engineering field for the design and implementation of operating systems and its components.
- Encourage the application of formal verification techniques to security-supporting services and protocols.
- Stress the need of realistic simulation scenarios that mimic real-life assumptions and contexts.
- Full understanding of the differences among all the technologies, platforms or services that need to be integrated
- Aim to provide fully secure environment platforms where personal devices play a key role and are not a menace to the data security of their users.

6.2.3.4 Timeline

This table lists the research topics and the corresponding time framework when those can be addressed.

Topic / Timeframe	Short (1-3)	Medium (3-5)	Long (5-8)
Secure Execution Platforms	Protection mechanisms for existing virtualization ecosystems.	Novel approaches for secure HW/SW virtualization.	Development of trustworthy mobile platforms.
Operating Systems Security	Secure component-based OS approach.	HCI security. Low-level, safe languages. Secure boot, remote attestation.	Dynamic, resource-constrained patching.
Security-supporting Services	Effective protection of IPv6 and other communication protocols.	Feasible crypto for cloud. Effective protection against side channels and data leakage.	Secure core and self-protective devices.

Control and Intrusion Prevention Systems	Effective monitoring and threat prevention on specific systems.	Integration of diverse control and intrusion prevention systems, interaction with other subsystems, intelligent threat analysis.	Intelligent, holistic, autonomous defence systems against insiders and Advanced Persistent Threats.
Secure integration	Identification of major hurdles. Definition of integration best practices.	Integration of several ecosystems, including apps and BYOD.	Full interoperability and management of dynamicity in distributed environments.

6.2.4 Establish privacy enhancing technologies and digital identities

6.2.4.1 Context

In an increasingly connected society, where large amounts of information are collected, stored, processed, and shared, Privacy Enhancing Technologies and technologies that ease and secure the management of Digital Identities are of utmost importance.

Privacy

The three AoIs acknowledge that the ability to guarantee privacy in ICT services is a cornerstone for advancing the state of the art in technology and policy. For instance, Ao1 recognizes that unless privacy is guaranteed in human interactions (among citizens, institutions and businesses), we are in danger of witnessing a "chilling effect" on citizens' participation in democratic processes, due to their actions being potentially observed. Hence, it highlights the need to embed the protection of fundamental rights (such as privacy) in the design, implementation and deployment of systems.

Similar concerns are mentioned in Ao2, where a constant concern of surveillance and loss of personal data is considered an obstacle that may jeopardize the future of the Digital civilization. This concern grows when it comes to new architectures and services based on shared platforms and infrastructures that increase the impact of privacy-related incidents on individuals and organizations.

Finally, privacy is also important at infrastructure level (Ao3). In order to keep ICT infrastructure safe and reliable, it is necessary that it operates preserving confidentiality and in a privacy-preserving manner so that it is capable of resisting (and preventing) cyber attacks.

Digital Identity management

Strongly related to the protection of privacy is the necessity of managing digital identities. This must be done in such a way that digital identities do not become an asset to breach users' privacy and enhance organizations' surveillance capabilities, but an opportunity for citizens and businesses to broaden their use of services taking advantage of the digital advances. This necessity is amplified by the appearance of new policy initiatives that target wider adoption of electronic identity cards, such as NSTIC in USA or eIDAS regulation, and with new requirements stemming from the revision of the data protection.

6.2.4.2 Research topics to be addressed

Three strands of topics are envisioned:

Privacy Enhancing Technologies:

1. **Development of privacy-preserving cryptographic protocols**: more research is needed in order to: i) keep meta-data private with a minimum amount of overhead; ii) build scalable solutions that can handle large databases; iii) protect anonymous and private interactions from abuse (detection of misbehaviour, revocation, or penalization without revealing private information); and iv) design efficient protocols that can be incorporated in resource-constrained devices.

2. **Private communication networks:** research is needed to improve current designs, for instance: establishing long-term or transient IDs without anchoring them into real-world identities; ensuring that adversaries cannot take over a network or distributed system by creating a large number of identities (what is called 'Sybil attacks'); improving the robustness of private channels towards censorship, enabling unobservable access to the service; and making such systems secure towards attacks that exploit persistent communication patterns, visible attributes of the user device, or end-to-end correlation of traffic.

3. **Privacy Enhancing Technologies for organizations and infrastructure**: research is needed to extend PETs designed for private users to the privacy needs in large institutions, private company assets, and national infrastructure services, to protect themselves against invasions by foreign state-level adversaries. This includes adapting generic protocols and tools to new data-intensive business models such as smart meters, electric vehicle charging, pay as you drive taxation or insurance, general sensing and the Internet of Things (IoT). An area of intense recent interest is genomic privacy, which requires adapting techniques from privacy-preserving computations and big-data to specific problems in a high-value domain.

4. **Privacy Engineering practices.** a key open challenge is how to integrate PETs, established and custom, into an overall process of secure software development to ensure they meaningfully contribute to the protection of users. Moreover, PETs compose in complex ways, and hence a key research challenge involves the design of PETs that are easier to compose and integrate into designs. Furthermore, research is needed to provide systems designers and analysts with tools to assess the level of privacy protection provided by their systems. This includes formal definitions for privacy requirements, privacy metrics, and methods to assess privacy risks and test for compliance.

5. **Usability of PETs**: research is needed in order to improve the usability of PETs, making them accessible to designers, engineers and general public. This line of research should look into friendly and intuitive user interfaces, as well as friendly interfaces for engineers to include PETs into ICT system implementations. Major research challenges remain open with respect to the interactions between end users and the system. In particular, better and more usable privacy controls that provide contextual feedback to users and raise their level of understanding and awareness on how the system functions.

6. **Data sanitization and anonymization**: research is needed to enable the extraction of aggregated statistics from datasets without compromising the privacy of individual users who might have provided their data. Differential privacy techniques have been proposed to address this issue, but many challenges remain, such as the development of such techniques for linked data, or the joint computation of such aggregated results by multiple entities that hold parts of a distributed dataset.

7. **Mobile privacy-preserving applications**: The widespread adoption of mobile devices has raised concerns with respect to location privacy. Designing mechanisms and location-based services that effectively prevent the unwanted disclosure of location data remains an open challenge. More research is also needed to anonymously access services and the web from mobile devices.

Privacy-aware Security Technologies

1. **Surveillance monitoring tools**: in order to limit the impact of surveillance technologies in digital civilization, research is needed into systems that measure the amount of surveillance, such as web browsing tracking, which may be performed by states or private actors, on the Internet as well as at services.

2. **Privacy-preserving monitoring tools**: research is needed to develop and integrate PETs in the surveillance infrastructure in order to mitigate the invasiveness of such surveillance.

Identity management

1. **Partial identities**: research is needed to build technologies that allow users to separate their identities for different aspects of life. This must be done at both the application and physical levels. Furthermore, research is needed to deal with authentication in services that do not require a persistent identity. Protocols that allow the authentication and authorization of users based on attributes (e.g., attribute-based credentials) need to be fully developed and combined with electronic identities to provide a flexible framework.

2. **Scalable and interoperable of Identity Management solutions:** research is needed in order to build identity management solutions that are scalable to large populations, and also that can be used not only by individuals, but also by entities and machines (e.g., Internet of Everything). Such solutions should also be interoperable, identity promoting trust on, and among, identity providers (e.g., by having control about the level of security achievable by each provider).

6.2.4.3 Catalysts for improving impact of research

- Encourage usability research related to PETs and electronic identity management
- Encourage open software implementations of PETs that can be broadly reviewed (to increase trust in its guarantes) and integrated in services.
- Increase awareness in society and industry about privacy issues to foster PETs adoption and deployment
- Foster the creation and development of a Privacy Engineering discipline
- Automation of design and analysis methods to assess privacy properties

6.2.4.4 Timeline

This table lists the research topics and the corresponding time framework when those can be addressed.

Topic / Timeframe	Short (1-3)	Medium (3-5)	Long (5-8)
Development of privacy-preserving cryptographic protocols	Efficient solutions for focused problem areas	Efficient solutions for focused problem areas with	Efficient and scalable solutions for generic scenarios

	with limited abuse protection.	comprehensive abuse protection.	
Private communication networks	Censorship-resistant access to the communication network	Protection from inferences in long term usage against powerful network adversaries	Fully de-centralized efficient sybil-resistant private communication networks for heterogeneous traffic
PETs for organizations and infrastructure	Privacy requirements for large organizations and infrastructure	Adaptation of protocols to the identified scenarios	Off-the-shelf PETs for organizations and infrastructure
Privacy Engineering practices	Standardization of privacy metrics	Privacy design patterns and composability rules	Comprehensive privacy engineering methodologies and assessment frameworks
Usability of PETs		Improved intuitive user interfaces	Efficient and packetized implementations for developers
Data sanitization and anonymization	Assessment of current algorithms	Distributed data-sanitization techniques	Comprehensive data sanitization frameworks
Mobile privacy-preserving applications	Assessment of existing data leakage	Application-specific privacy-preserving mechanisms	Generic comprehensive privacy-preserving mechanisms
Surveillance monitoring tools	Identification of surveillance targets and practices to be monitored	Single-user surveillance monitoring tools	Privacy-preserving collaborative surveillance monitoring
Privacy-preserving monitoring tools	Integration of PETs in specific monitoring use cases	Integration of PETs in generic monitoring tools	Improved understanding of remaining risks and potential mitigation strategies

Partial identities	Efficient protocols for unconstrained devices	Interoperable protocols for constrained devices	Efficient protocols for constrained devices (e.g., smart cards)
Scalable and interoperable of Identity Management solutions	Machine-compatible identity management solutions	Scalable privacy-preserving identity management solutions	Fully interoperable scalable identity management solutions

6.2.5 Increasing trust

6.2.5.1 Context

While technology oriented communities often see security as a basis for trust, social-science oriented communities see trust as a something that is needed, when no security can be assured. This difference in the understanding of basic terminology leads to frequent misunderstandings on the role of trust and security. This Gap reported by AoI 1 seems to be shared with other AoIs as evidenced through text, and call for more research on terms on terms like "trust" and "trustworthiness" and their meaning and relation in different disciplines (e.g. to create mutual understanding and deliver a unified trust model shared and agreed and from which to deliver the solutions needed to effectively and efficiently manage Trust and Trustworthiness). Despite some research has been initiated here by Project such as OPTET, additional and multi-disciplinary research needs to be conducted to cover this and other gaps as reported by the 3 AoIs.

Indeed individuals need to be empowered to develop trust into digital services and/or apps for them to make informed decision. This calls for methodologies and tools to not only focus on Security and Privacy by design but also Trustworthiness by design. This calls also for proper lifecycles to be covered from development to management (monitoring) going through important steps such as certification, distribution and deployment. This part has been also highlighted in other focus areas.

When it comes to AoI 2 focusing on Digital Interconnected society, Trust management has also been advocated in many places since seen as key to fully embrace the Digital Society. As such researches on models for fostering Trust at the collective layer have been called for together with trust assurance, trust accountability and trust metrics. Among others what is expected here by AoI 2 is to enable Trusted (Cloud) Services to be developed in any layer (IaaS, PaaS, SaaS) in order to reduce the consequences of the vulnerabilities at each layer; Trust models for the digital civilizations (Trust areas for the "cyber world"); Security engineering embedding properties as security, privacy and trust, compliance in the very early phases of system and services design to increase trustworthiness of systems.

Looking at AoI3 concentrating on trustworthy (hyperconnected) infrastructures (and especially critical infrastructures due to their importance for the European Cyberspace and the European Economy) research and development on trust and trustworthiness management the way needed is seen as a gap to be covered to achieve the Vision. If AoI3 share a number of research actions with other AoIs it also puts additional emphasize or even bring some new ones. Indeed AoI3 calls as others for measurable indicators of trustworthiness but here in the combination of safety and security means for infrastructure. At such it puts additional emphasize on research needed on security architecture for Trust and Trustworthiness measurement and management (calling for not

only reactive measures but also and most importantly proactive measures). As other AoIs, AoI 3 calls also for users to be provided with access to information that allows the confirmation of the trustworthiness of the infrastructure and its services (even if partly) but also calls for increase trust in information sharing and some more freedom of information legislation.

Overall trust issues have been also advocated from several research communities as Trust in the Digital Life Initiative (TDL)[38] and ERCIM Security and Trust Management [ERC14].

6.2.5.2 Research topics to be addressed

We envisage the following research areas to be further investigated:

1. **Computational trust models.** There is the need to define sound and robust computational trust models able to cope with the heterogeneity of modern ICT infrastructures, ranging from IoT to cloud services. The computational trust models should be robust enough to resist to attacks as defame and collusion. New aggregation and filtering approaches should be identified. Overall an unified trust and reputation models/principles should be also investigated.

2. **Dynamic trust assessment.** The initial approaches to trust focus on relatively static or intrinsic trust parameters that could be updated from time to time, in conjunction with other events, such as rebooting of a platform or a first connection with the base after powering up or installation. As the infrastructure requirements changed, so did trust requirements associated with it. As a result, in many areas, such as Trusted Computing, dynamic trust analysis became a necessary feature. This also demands for appropriate trust metrics that could take into account, context, time, structure of services/devices etc.

3. **Privacy aware trust negotiation.** Trust negotiation in complex systems is still an active area of research involving negotiation algorithms and privacy preserving techniques. The mixture of anonymous credential mechanisms could help in this matter.

4. **Trust and big data.** Big data heavily interplay with trust. On the one hand, we need to trust on the collected data, i.e. who are the providers, who manipulated etc., on the other hand data helps to define proper trust and reputation systems, often based on recorded evidence by several parties. In particular, we need to develop and monitor techniques for trusted information sharing (including several incentives schemas).

6.2.5.3 Catalysts for improving impact of research

- Investigate the epistemology and semantics of trust and provide clarification of meaning and domains of application, fundamental definitional questions
- Investigate the notion of trust for on-line word and the influence in security
- Encourage research on unified trust models, also in basic trust principles
- Promote sociological studies on the interaction between human and software devices/services/agents in the cyber physical systems.
- Encourage research of integrated trust metrics also for hardware and software artefacts that could be easily integrated in the SDLC

---

[38] http://www.trustindigitallife.eu/

6.2.5.4 Timeline

This table lists the research topics and the corresponding time framework when those can be addressed.

Topic / Timeframe	Short (1-3)	Medium (3-5)	Long (5-8)
Computational models of trust	Methods to define, compute, and aggregated trust in complex domains		Unified computational trust models able to cope with several scenarios
Dynamic trust assessment	Trust metrics for context, time and other relevant features	Dynamic trust assessment also for resources constrained devices	
Privacy aware trust negotiation	Negotiation protocol that enable privacy	Efficient methods also for resource limited constraints	
Trust and big data			

6.2.6 Managing and assessing risks

6.2.6.1 Context

There is a common understanding across the AoIs that the new developments in ICT technology and its applications are increasing the complexity of system and provide a challenge for managing this complexity and the related cyber risks.

On the other hand, the state of play today, as contributed by NIS WG1 "Risk Management" to NIS WG3, indicates that however several approaches and frameworks to risk management exists, the lack of awareness of decision makers, the lack of interoperability and standardized metrics, the costs-benefit ratio (especially for SMEs), the lack of statistical information for predictive approaches, the existing frameworks' outdated status, their static assessment model, as well as the perception of weakness and coverage not sufficient for the complex business and cybersecurity risks of today, it is becoming a real and important disincentive and barrier for adoption either by larger or smaller organizations.

The complexity has been increased during recent years as threats also evolve along the time. Their very nature as well as their motivations, techniques and tactics are becoming polymorphic and more sophisticated day after day, making them unpredictable for any risk analyst. Vulnerabilities in technology are found at a rate that renders current cybersecurity solutions and strategies rapidly obsolete. In addition, there are threats, such as APT, state-sponsored attacks or governmental

surveillance programmes, for which no effective solution exists, leaving our organisations and society dramatically exposed.

This ever changing and unpredictable nature of the threats and the technology on which the organisation depends makes expert judgment for risk assessment incomplete and inaccurate. As a consequence, this assessment should be continuously reviewed and verified against the updated state of the system under observation.

The system under observation has to be expanded, especially in the supply chain model, where organisations need to incorporate the risk level of their suppliers into their global picture. The security paradigm has changed, although traditional security approaches are based on the existence of a perimeter that needs to be protected, this paradigm does not hold anymore. We need to operate in a world where a perimeter is not there or has already been breached.

Another important factor it is the ability to decide and execute effective courses of action in timely fashion in order to mitigate and remediate the impact of attacks, when occurring on real time.

Historically, technical security controls (anti-malware, firewalls, IDS/IPS, etc.) have focused on prevention of compromise. However, it is now widely recognised that no matter how good your preventive controls are, they can only reduce the number of and severity of security breaches and not eliminate them. The emphasis has now shifted to augmenting preventive controls with detection and remediation measures. Clearly, the time taken for detection, diagnosis, remediation planning, and action is critical in limiting the impact of an attack. In the future, we can expect the sophistication and speed of execution of attacks to increase, and the difficulty of formulating a timely response to become correspondingly more challenging. A capability for autonomous response will become essential, because there will simply not be enough time to have a man in the loop. However, an inappropriate response may be more damaging than the original attack, so that the controls need not only to be speedy, but also trustworthy. This implies that they must understand the limits of their authority and the consequences of their actions. To be trusted as well as trustworthy, they must be able to explain and justify their actions in retrospect. Of course, the attackers will attempt to evade the defences, so that the defensive technology must be able to adapt dynamically to the attackers' tactics. Despite the automation, people must remain in ultimate control, being able to set and modify policies that govern the actions of the autonomous agents. Establishing effective means of man-machine co-operation will be a research challenge in itself.

Current frameworks and methodologies, in the way they were conceived, cannot provide a solution for all these problems. We need novel / modern, simpler, disruptive, dynamic, multi-stakeholder, interoperable (based on formal sustainable models), standardized, predictive, reactive and holistic approaches capable of estimating and reducing the risk in real-time, feeding from real-time operational information and threat intelligence sources, and automating the risk assessment and management activities (especially detection and remediation ones) for a new perimeter paradigm as never before.

At the same time the cyber risk surface increased at all levels, especially in Critical Infrastructure Protection, where the solution is too complex and significant to be left to an ad hoc collection of volunteers. On the other hand this opens to EU the opportunity to address this by an executive and collaborative approach between member states in order to keep a permanent and standardized protection of EU essential services.

That is to say, EU needs and has the opportunity to harnessing barriers to become enablers and opportunities.

6.2.6.2 Research topics to be addressed

Translating the above findings into research priorities on a finer level of detail, especially those coming from NIS WG1 ("Risk management"), as well as those coming from each of the AoIs and

the research landscape document, we suggest to structure along the dimensions of the following research priorities:

1. **Methods to reduce and manage systems complexity.** The limitations of existing risk management methodologies in terms of addressing the cascading effects from the interdependent threats, the change of the security perimeter paradigm, the increasing complexity and nature of threats and the need to manage a multi-stakeholder supply chain inside a global risk management picture between other different facts, justify the need of more research in reducing complexity, improving accuracy of impact calculations at the same time the availability of simpler tools, simpler interfaces supporting these processes allow cost-effective solutions in order to avoid more barriers to adoption.

2. **Dynamic risk assessment and management.** In order to achieve a comprehensive and continuous situational awareness, we need novel, disruptive approaches capable of estimating the risk in real-time, feeding from real-time operational information and threat intelligence sources, and automating the risk assessment and management activities as much as possible. Dynamic risk management should take care about systems evolution for a sustainable assurance. Dynamic discovering, the way the system inference new topologies as well as the usage of new advanced multi-dimensional sensors of different nature (such as environmental sensors) as inputs to the risk analysis could improve the accuracy and efficiency of the management process. For a broader impact, information sharing and the effective and automatic use of exchanged data tampering of field devices, roadside and infrastructure equipments along the value chain, should be considered.

3. **Formal interoperable models to enable comparisons and compatibility between multi-disciplinary environments.** Interoperability and standardisation of the way the risks are calculated. Without this, comparing and interpreting results of two different approaches is not possible, undermining the objective evaluation of the performance and effectiveness of new solutions. This is especially relevant in the supply chain model, where organisations need to incorporate the risk level of their suppliers (including physical, human, the cyber layer, processes and services) into their global picture. There is a need to progress toward comparability of risk assessment results, whatever method is used. As we go to ever large scale interconnected systems, and the development of new risk management models and systems for cyber societies is necessary wide activities towards a holistic risk management framework.

4. **Statistical and predictive risk analysis.** Considering that statistical risk methods do not work well with intentioned threats, new methods should be researched. Furthermore acknowledging that most common risk assessments models depend on past information to picture the current risk scenario, additional data models that helps to predict probabilities and impacts of threats in the EU could be extremely useful for example as a tool for remedial actions, investment priorization or even for a risk externalization. For Cyber Insurance (as explained under Assurance section), the capability to predict the current strength of the system is considered to be a strong component of any calculation. Thus security and corresponding risk metrics (as explained below) are crucial (as other quantitative aspects of security). The way this data can be shared effectively and re-used at scale it is a key factor to provide organisational and shared benefit in EU.

5. **Autonomous detection and remediation by a man-machine effective cooperation.** A capability for autonomous response will become essential to fight against cyber attacks, because there will simply not be enough time to have a man in the loop. However, an inappropriate response may be more damaging than the original attack, so that the controls need not only to be speedy, but also trustworthy. This implies that they must understand the limits of their authority and the consequences of their actions. To be trusted as well as trustworthy, they must be able to explain and justify their actions in retrospect. Of course, the attackers will attempt to evade the defences, so that the defensive technology must be able to adapt dynamically to the attackers' tactics not only as an active defense but also to know more about the attacker while in the attack. Despite the automation, people must

remain in ultimate control, being able to set and modify policies that govern the actions of the autonomous agents. Establishing effective means of man-machine co-operation will be a research challenge in itself.

6. **Integrated risk metrics and indicators.** In order to evaluate to what extent current metrics can be incorporated (and enhanced) into new solutions, there is a need to have a better comprehension of the metrics currently being used in traditional frameworks and methodologies. They are usually said to be based on the 'experience' of the designer, but this doesn't mean anything if the method is not justified based on solid criteria. Calculation methods should at least be auditable. Current metrics tend to focus on individual organisations and not take into account supply chains or dependencies across sectors and borders. It is also easy to focus on those things that are easy to measure and possibly ignore the real indicators of success or failure. The increasing scale and connectivity of cyber security issues means that organisations can no longer live in their own silos (and measures things that only affect them) and new approaches to identifying and setting realistic metrics should be considered. i.e. that the security mechanisms are appropriate for the protection of the assets. This requires security mechanisms that fit the purpose and are able to allow security managers to trade-off between cost and risk. New security metrics frameworks able to be easily computed should be envisaged. These security metrics could be merged with risk analysis methods to decide the appropriate security controls to be put in place or even facilitate the risk externalization (i.e. Cyber Insurance).

7. **Visual decision making governance frameworks.** The increasing complexity force simpler interfaces for an effective man-machine governance framework. We lack of a coherent framework that puts all these pieces together and helps to identify gaps that need to be filled with further research. For example, with the aforementioned solutions it is not possible to effectively translate the risk level into business impact, moving the analysis from the operational/technical layer to the business layer. This achievement would significantly support and ease the decision-making process for risk owners. New techniques are also needed to enable more consistent and appropriate security decision making as well as allowing aggregation and composition of different pieces (Software and Hardware) without losing the control of risks either including all the value chain sensors or other factors like legal and economics.

8. **Legal risk assessment and management.** For a holistic and complete approach, legal risks should be integrated in the organizations decision making process. It may enable the evaluation and comparison of alternative regulatory and non-regulatory responses to complex and interdependant risks and selecting among them. This process requires knowledge of the legal, economic and social factors, as well as knowledge of the business world in which legal teams operate. Risk-preventive, reactive and mitigation services, including process identification, empirical analysis, quantitative evaluation, cost analysis and dynamic support. The system's basic concept is to solve enterprise legal risk problems by means of management, and the basic principle is to describe the enterprise legal risks in the language of economics although its value should be added to the enterprise risk decision making. Research should provide medium and long-term, holistic and dynamic legal risk management solutions compatible and interoperable with other technical and business risks. At the same time, legal and contractual obligations could also facilitate the adoption of risks management practices by "hard to reach" organizations as an enabler as noted by NIS WG1.

9. **Incentives for adoption of risk management best practices and reducing barriers (especially for SMEs).** As noted by NIS WG1, there is a strong belief, backed by feedback, that SMEs are not applying even basic cyber risk management methods or best practices. A research is needed to establish how to communicate with 'hard to reach' organisations and to incentivise the adoption of best practices due to the fact that still most damaged cyber attacks against this kind of organizations are considered basic (social engineering, phising, default passwords, patching) however all the efforts being done in awareness raising. Of specific interest is further research into the use and take-up of risk management

94

methods and practices by SMEs. Barriers already identified by NIS WG1 include the lack of awareness, the complexity of risk assessments, the imbalance between resources devoted to analysis and the benefits for the organization (usually seen as one-off static exercise rather than part of on-going activity within a governance framework that is maintained). In additon to this, the executive and decision makers perception is all about cost and expense rather than preventing financial and material loss. Usually in smaller organizations, the lack of expertise, training, dedicated staff are also barriers. There is a need to look and research about potential incentives for take-up and maintenance, both within an organisation and across supply chains.

6.2.6.3 Catalysts for improving impact of research

- Cover the full spectrum of the value chain, interdependencies and domains.
- Encourage research to incentivise effective adoption of risk management practices by "*hard to reach*" and other SMEs organizations.
- Focus on automation under an effective man-machine cooperation against risks.
- Encourage research on formal models, languages and ontologies to compare and interoperate between different frameworks and disciplines.
- Encourage research on statistical and predictive analysis based on new models for intentioned threats.
- Encourage research of integrated risk metrics, indicators and the cost factor of risk management.

6.2.6.4 Timeline

This table lists the research topics and the corresponding time framework when those can be addressed.

Topic / Timeframe	Short (1-3)	Medium (3-5)	Long (5-8)
Methods to reduce and manage systems complexity		Methods and process for managing risk interdependencies	Simpler tools and interfaces available to support these processes
Dynamic risk assessment and management	Automation of risk analysis	Advanced real time multi-dimensional sensing capabilities	Significant improvements on real time risk estimation
Formal interoperable models		Comprehensive set of formal interoperable semantic models based on ontologies.	Comprehensive set of guidelines and interoperable standards approved and established in practice

Statistical and predictive risk analysis		Theoretical foundations and supporting methods and tools for intentioned threats prediction	Statistical methods to estimate the current strength of the system against current and predictive risks
Autonomous detection and remediation by a man-machine effective cooperation		Effective means of man-machine co-operation	Pseudo-autonomous real-time reasoning systems for detection and remediation
Integrated risk metrics and indicators		Auditable calculation methods for risk metrics	Integrated KPI
Visual decision making governance frameworks		New techniques for appropriate risk decision making	Integrated visual decision frameworks to support this new techniques
Legal risk assessment and management		Legal risk semantic formal models	Comprehensive legal risk guidelines and interoperable standards approved and established in practice
Incentives for adoption of risk management best practices and reducing barriers	Research into the use and take-up of risk management methods and practices by SMEs		Lightweight certification and other effective models

6.2.7 User–centricity

6.2.7.1 Context

All AoIs share the view that the more a user engages in digital life, by moving activities on-line and relying on ICT services and connected infrastructures, the more involved in interaction with these

services and infrastructures she will become. If privacy protection demands users to be in control of their data and systems and services to provide transparency about their data processing, users need to be able to express their preferences and to assess the risk that relates to the decisions they make related to their data. When users interact with critical infrastructures, e.g., citizens requesting open government services, employees operating control systems or individuals enjoying the convenience of home automation solutions and the additional safety coming with automated healthcare support, these interactions need to be designed in a way that users can be aware of security and privacy implications, that they can adapt their interactions intuitively according to their security preferences and risk profiles, and that they are protected from unintentionally introducing security weaknesses or excessively disclosing data. Users need to be empowered to manage their digital identities by defining their policies and preferences in an intuitive way.

All these examples amplify the need for designing and operating ICT systems and services with the user and her abilities and preferences in mind. In particular, usability, user acceptance and awareness need to be integral parts of security solutions. While many security and privacy relevant aspects of systems and services can be technically accessed, configured and maintained already today, such configuration and maintenance should not be manageable by technology experts only. With the increased penetration of ICT, everyone must be able to do so. How this can be achieved while at the same time technology gets more complex, remains a challenge. Meeting this challenge is a prerequisite to avoid a digital divide.

6.2.7.2 Research topics to be addressed

This should include at least the ones from AoIs and Landscape, in particular:

User centric design	focus on user centric technologies (individuals)
	Engineering technologies for users
	reduce digital divide
	technologies to reduce user misbehaviour

Usability of security mechanisms	usability of security mechanisms
	usability of authentication
	visualization techniques
	Usable secure public key algorithms that cannot be compromised by quantum computing

6.2.7.3 Catalysts for improving impact of research

6.2.7.4 Timeline

This table lists the research topics and the corresponding time framework when those can be addressed.

Topic / Timeframe	Short (1-3)	Medium (3-5)	Long (5-8)

6.2.8 Standardisation and interoperability

As a common enabler identified by the three AoIs, the standardisation process should evolve into a more coherent, proactive, transparent, inclusive (open to all stakeholders) process, as well as it should be driven by (European) research more than ever.

As an example, the near future of Critical Infrastructures may need processes and resources more adaptive, decentralized, transparently collaborative and efficiently controlled. The more pervasive usage of ICT to comply with such requisites, the more interoperable and hyperconnected it must be. ICT infrastructures are as critical as the critical services they may support.

Due to the dynamic nature of cybersecurity and its threats, new products and services may need to be deployed continuously at the same time they should co-exist with other legacy systems still under depreciation, so interoperability is a major challenge inside such a fragmented market.

The exponential explosion trend and availability of new ICT products as well as the diversity of components, applications and services, created, integrated and deployed from anywhere in the world, may need an extra effort of standardisation if we want any end-user to trust cross-boundary interoperable and privacy guaranteed communications as an example. First, better political and

regulatory support is needed for a cross-border effective approach, and secondly, an industrial transparency of hardware and software components and functionalities used may happen.

There is a business opportunity for the European Industry to be the reference in privacy and security-by design to end users. The key for success is the standardisation, the transparency and a stronger coordination and cohesion of stakeholders groups. It can drive a faster adoption of R&I results by the Industry as well as a proactive approach by policy makers which enable a more effective industrial policy avoiding societal mistakes before they happen. Reactive approach as of today involve regulatory and political actions to fix mistakes which already impact end users and European industry investments. The key is to avoid mistakes before they happen and to drive a better industrial strategy.

Inhibition examples today include contactless technology partially implemented (RFID vs. NFC) managed by different standardisation bodies, cross-border different regulation approaches, lack of a basic security classification and interoperable levels between different devices, lack of assessment and effective feedback ecosystem, lack of transparency over different functionalities, lack of an agile approach (evolving pre-standards created by a consensus of a community).

6.2.9 Education and awareness

 As a main challenge, our future needs a reinvention of our education. It is not a matter of standard recycling but a real multidisciplinary, coordinated and coherent approach. The ICT has changed our lives and the way we understand the problems and how to address them effectively.

We must teach the teachers in cybersecurity as never before. School teachers must learn before teaching kids, law professors must learn before teaching law students and engineering teachers must learn before teaching security and privacy by design practice.

Awareness raising initiatives are more important than ever, by using new training models like MOOC (massive open online courses) we can expand the impact, but understanding the issue is far from effectively addressing it. It is not enough for top level management to simply understand the problem, at least they should react. The more proactive European top managers we may have, the more business opportunities for European Industries.

The cybersecurity often seen as a cost driver, may produce new business cases and innovation paths. The situation is changing continuously and it is clear that cybersecurity skills is more and more a requisite by employers in a multi-faceted approach (i.e law). There are more jobs than qualified candidates today however the European unemployment rate is still high. There is an opportunity of careers re-orientation which may need special efforts for recycling.

Medium-long term trends indicate that the cybersecurity employment rate will also evolve, so the more coordinated and coherent approach by all member states the better European situation for resilience and competitiveness. The bad news is that the main reason is the likelihood and impact of cybersecurity attacks. As an example, future cities will depend on Critical Infrastructures and will compete for cybersecurity talent motivating skilled people to stay or being moved to that city.

Today the educational programs are so fragmented, lead by specific mainly international companies for their own purposes, the knowledge is not shared as it should be and none of them address a dynamic up to date light weight process (aligned with the cybersecurity dynamic nature).

There are lots of new disciplines and skills training opportunities as enablers, some examples are cybersecurity insurance, awareness in values (particularly among the youngest), user empowerment and control of personal big data, digital legal education (i.e, rights to be forgotten versus free of speech, anonymity versus trust and security, crowdsourcing versus legacy manufacturing), cybersecurity risks and practices, security engineering, agile security management and so on.

6.3 Divergences

This section highlights on those topics which have been seen prioritised differently across the AoIs. While there are no strong apparent conflicts (as in one AoI saying a topic should be prioritised while another AoI suggesting to de-prioritising it), some topics receive different attention from the respective AoIs.

6.3.1 Do societal and technical viewpoints lead to different priorities of security and privacy?

Section 3 of this report which discusses individuals digital rights and capabilities aims to position the individual at the very centre of influence over information and communications technologies in a connected digital society, giving individual citizens not just a right to privacy online, but encompassing fairness, democracy, freedom of expression, consumer rights, and even the right to opt out of the digital world if they so wish.

At the same time, innovative digital networked services require global digital infrastructures, consume personal information and process it to provide services that businesses provide, consumer's want and public administrations need. Section 4 of this report looks at this from the perspective of those institutions, exploring the enablers and gaps in technology and how it is managed that are necessary to enable civil society to operate. These include technologies to increase security, enhance privacy, control information, and provide governance and assurance and will enable digital institutions to comply with cultural norms and the laws of the countries in which they operate.

Yet it is clear that there is still divergence between these perspectives, that of the individual and the institutions. Developing new technologies is not sufficient to ensure that cultural norms with respect to privacy are followed. Social networks enhance freedom of expression and democracy. Advanced technologies prevent censorship. The internet is global and spans many states and cultures, even when they are in conflict. Technology fuelled innovation proceeds at furious pace and norms adapt and respond to it (followed, eventually and not always consistently, by regulation).

Ensuring that individuals are at the centre of a networked digital society is more complex than technology, business or regulation can deal with separately when there are differences between states, diversity in perspective between different cultures. Multidisciplinary research is vital to develop clearer understanding, and research into technical and non-technical ways to improve facilitates effective governance of digital infrastructures, services and institutions is necessary.

6.3.2 Security and privacy: subject to market conditions or a societal goal?

NIS innovation can contribute to the European economy in three main ways:

1. By reducing the number and severity of security breaches and their consequent negative financial impact;

2. By reducing the actual and perceived security risk associated with introducing new and improved technologies and practices;

3. Through revenues and employment provided by enterprises offering NIS technology, products and services.

In regulated market economies such as the EU and its member states, competition is seen as the main driver for innovation. Authorities try to steer the market by means of rules and incentives in order to protect the weak and align the profit motive with collective societal goals.

Clearly, individuals, enterprises and society in general will benefit from a more secure, resilient and trustworthy ICT infrastructure. However, much of this infrastructure is privately owned and enhancing security will require sizeable investment. This can only be justified if the outlay can be recovered and a fair return generated within a reasonable time. Unfortunately, it is often the case that customers/users expect security, but are unwilling to pay a premium for it. Regulation, either imposed from above, or through industry standards and best practices, may have a role to play in stimulating innovation by requiring improvements or preventing providers with good NIS being undercut in a race to the bottom. It also holds dangers, however. e.g. imposing an excessive cost burden, or stifling innovation by implicitly requiring particular technologies or approaches. It may also result EU consumers using services provided from less regulated jurisdictions.

It is common now, that ICT service providers seek return on investment by monetising information gathered in the course of providing the services. Clearly, this is a potential threat to privacy, and legislation is one route by which authorities seek to define and enforce individuals' rights. Another approach is to develop products and services that empower individuals by giving them control of their personal information. This is easier said than done, but is already the focus of much R&D, and represents a significant innovation opportunity. Should effective tools be developed and become widespread, service providers would still need to make money and users would have to pay one way or another or else lose access to services. The choice may be between paying a fee for services that do not exploit personal information, or negotiating controlled disclosure of personal inform in return for a free or subsidised service.

In addition to regulation, authorities can offer incentives to encourage invention and speedily bring it to market. They can also seek to lower barriers to innovation e.g. through access to investment capital and leading by example by pioneering procurement of novel technologies. Perhaps the greatest step forward would be to change attitudes so that NIS was valued by consumers, businesses and public sector bodies when making purchasing decisions in the same way that safety is valued when buying a car.

6.3.3 New developments may change the priorities

Many of the challenges that are identified by the different AoIs are related to recent developments in ICT infrastructures, systems and services, including cloud computing, big data, Internet of Things, infrastructure/platform/software as a service, content delivery by everyone ("prosumer"), and more. Many of these developments were not visible or predictable five to ten years ago, but have been disrupting technology, business and society since then.

What will be comparable developments that are going to disrupt over the coming five to ten years? While there is no precise answer to this question (likely, the developments mentioned above would not have all been prioritized when asking this question ten years ago, while many of the technologies were already in research stage), the observation indicates the need to observe early, upcoming and new technologies with respect to their security and privacy impact, and to provide responses to the protection of security and privacy needs of citizens, organisations and infrastructure providers. Examples of such technologies include wearable computing, augmented reality, quantum computing, etc.

Since such new developments may change the priorities for research because they impose new challenges or put additional emphasis on particular challenges, it is important to invest in their observation and the preparation of adequate responses to new challenges.

6.3.4 Migration of legacy systems

Many of the critical infrastructures discussed in Section 5, in particular, those that are now going to be connected to the digital world via the Internet of Things, are the result of long-term evolution and investments, with components having an expected lifetime of many years, sometimes decades (e.g., in transportation systems or the power grid). The operators of these infrastructures on one hand need to secure the huge investments made, while on the other hand preparing to protect

them against new threats resulting from increased connectivity, for which the legacy systems have not been designed.

While the individual's viewpoint in AoI1 suggests accepting the fact that these legacy infrastructures cannot be secured for their new usage scenarios, and promotes the provision of secure devices and the establishment of secure computing schemes, which allow users to protect their data on top of untrusted and potentially insecure infrastructures, the infrastructure viewpoint as expressed by AoI3 suggests to investigate into the migration of legacy systems, components and protocols towards solutions that are up to the security and privacy risks. The suggested direction is not to recommend replacement of legacy components (which seems to be infeasible taking business needs, investments made and pragmatic considerations into account), but build frameworks and environments around the existing infrastructures that allow their proper protection. Hence, the design of connected and virtualized infrastructures need to acknowledge the existence of legacy components and aim at their integration. AoI3 sees an important role of standardization in the approach to meet the above challenges.

This is seen as a major challenge for the infrastructures, in particular those which are undergoing a major transformation through increased connectivity. On the application and service side, cloud deployment models and virtualization are easing the migration task, since, for instance, upgrading, patching and replacement can be centralized under the control of the cloud provider.

6.3.5 Terminology

During the discussion and the creation of this document, emerged that the many people involved have sometimes different understanding of several concepts, due to the fact that generic terms, as trust, inherently gets different meaning in each different community (and WG3 has a multidisciplinary nature). Still the need for a commonly agreed terminology is something that naturally emerged and should be further elaborated through several means. At the EU/US levels, several efforts have been done to provide common bodies of knowledge (CBKs) in the area of cyber security, risk management and trust management. Those however still are view as islands with limited attempts to try to provide a wider coherent view. As mentioned, the typical example that emerged is the different meanings of trust and the interpretation of trustworthiness in the ambit of cyber security. This demands an answer at the scientific and technological community level (hopefully trying to harmonize the EU/US answers to these issues). The same issue was discussed in the education and training deliverable.

6.3.6 Surveillance

By "Surveillance" we refer to both monitoring of digital infrastructures, networks and services by law enforcement agencies, and also the use of digital surveillance technologies (predominantly visual/cctv but potentially expanding to other sensing technologies) for surveillance by those same agencies.

Access by law enforcement agencies to information stored or passing through digital infrastructures and services (a.k.a. "surveillance") provides powerful capabilities for law enforcement agencies whose aim is to protect society from crime, cyber-crime, and terrorism. At the same time the pace of technology innovation, emergence of innovative and often global digital services, and the evolution of connected digital societies has run ahead of global consensus on access to digital information by law enforcement agencies. For example:

1. Many cloud and social network services have global presence and operate from global infrastructures which means that agencies from states where services are operated, pass through, and delivered may have access to digital information.

2. Technologies developed with the aim of increasing privacy for individuals (e.g. anonymous routing), or of increasing information security against illegal activities (e.g. enhanced

encryptions, transport layer security) also have the effect of rendering information opaque to law enforcement agencies.

3. Technologies that facilitate legitimate access by law enforcement agencies (e.g. deep packet inspection) also facilitate wholesale access to information by agencies where legitimacy of access may be questioned or disputed.

4. Arrangements made by law enforcement agencies for access to infrastructures of global cloud services ("backdoors") may not be visible to their users

The use of CCTV cameras for surveillance by public and private organisations continues to increase dramatically with the UK being reported as having one camera for every 11 citizens in 2013[39]. Combined with images uploaded to social networks (which may also be used for surveillance), this represents a formidable resource for those seeking to track individuals and to monitor their activities, or to monitor collective behaviours which may be for business purposes as well as for law enforcement and for public and private security needs. As the scale of surveillance grows there is a need for research into what we can call "**Privacy Aware Surveillance"** technologies and governance of surveillance that respond to concerns over the scale of surveillance activities and their impact on individual privacy.

These are just a few of the divergences that are emerging as we move towards ever greater dependency on networked digital technologies - a full discussion of the issues surrounding surveillance is beyond the scope of this report. Nevertheless, it is clear that research with the aim of developing better understanding of the role, impact and governance of surveillance in networked digital societies as well as technological approaches that support effective governance and control of surveillance activities. This could include technologies that might limit access to information not required for specific surveillance goals (e.g. attribute based encryption, policy based data management), technologies that enable auditable surveillance that enables strong accountability for organisations carrying out surveillance.

6.3.7 Specific topics

In some of the AoIs, specific topics have been mentioned which are mainly highlighted by their respective viewpoint. Such topics are typically focused, by pointing to a specific technology or application domain, and provide their own respective challenges.

The specific topics include at least:

1. Privacy-preserving digital currency

2. Fraud detection

3. Cybercrime protection, cyber forensics

4. Electronic voting

6.4 Key Observations

This section summarises a few key observations that were made during the execution of the cross analysis. It is not meant as a summary of the cross analysis, but as adding findings and observations that were striking during the analysis, and that might add further insight to the discussion and help in setting up future research activities.

---

[39] http://www.telegraph.co.uk/technology/10172298/One-surveillance-camera-for-every-11-people-in-Britain-says-CCTV-survey.html

It is noteworthy that for all identified challenges initial existing contributions could be identified. In terms of technology research, some of these contributions could even be seen as relatively mature (e.g., in the areas of digital identities or privacy enhancing technologies), and identified inhibitors are mostly relating to business and societal aspects. As a result, the cross analysis cannot report on the existence of blank areas or totally open fields, where no contributions can be spotted yet. This might be largely due to the future predictions being dominated by developments that can already be seen on horizon or are even becoming real business opportunities (e.g., Big Data or the Internet of Things). Still the recent history has told that technology and market disruptions can dominate the developments within a very short time span (less than 5 years), so that research activities, while mainly following an evolutionary approach, need to include fundamental and ground-breaking research as well[40].

While the AoIs stressed a common emphasis on assurance, at the same time many ways to provide assurance were mentioned. They are not introduced as alternate options or respective replacements of each other, but rather indicate a need for investigation into the relation between and complementarity of the different means and their factual as well as perceived contribution to the trustworthiness of ICT systems and services (from both a consumer and provider viewpoint).

All AoIs put a strong emphasis on non-technical aspects of security and privacy, in particular, requiring a stronger role of organisations in the uptake of security and privacy enhancing technologies and of regulations to emphasise on European tradition and values. The debate on whether trustworthiness of ICT should be subject to market conditions and developments or seen as a societal responsibility needs to be conducted. This observation is understood as recommendation to continue and intensify multi-disciplinary research (technology, economy, society, and jurisdiction) in the field. Important aspects driving the related business aspects, including adoption, innovations, and market, need to be considered.

Since information and communication technology and business have faced major disruptions just recently, in many cases without considering security and privacy from the very beginning, it is not surprising that the majority of challenges and, hence, research priorities are driven by responses to those disruptions. Still, it seems to be worthwhile to look into future potential disruptions, taking into account that the speed of technology developments is not expected to decrease.

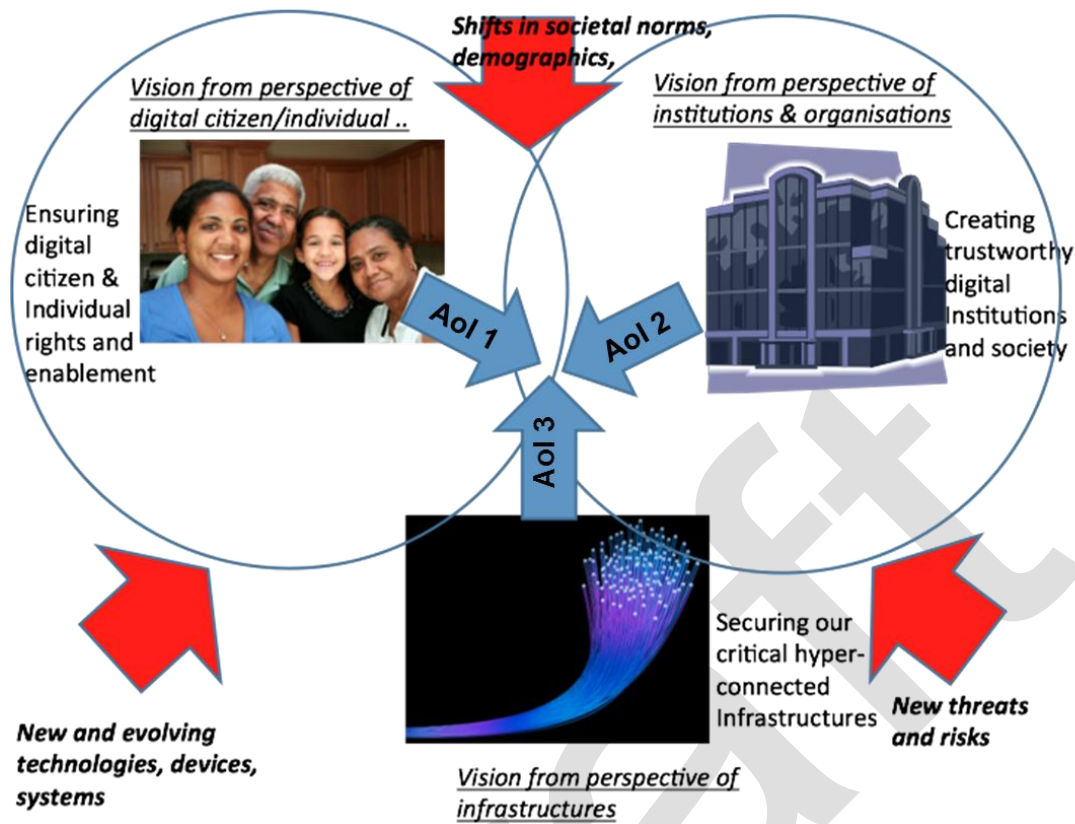[40] Therefore a provision for open research similar to the FET scheme is needed.

Figure 1. Areas of Interest coverage areas

7 Summary of the main findings

This Section collects some of the main findings of the SRA plus of other two deliverable documents produced by NIS WG3, i.e.: Business cases and innovation paths and Snapshot of Education & Training landscape for workforce development. Overall the main findings with the corresponding opportunities to be exploited are split in 4 main areas: research, policy, business and education.

7.1 Research

TBD

7.2 Policy

NISP WG3 constituents identified that policies in the NIS and privacy domains should;

- act as enablers to support research and innovation, and,
- set the targets that researchers and industry should aim for.

Guided by these two principles, the following sub-sections highlight the proposed areas of focus (key aspects) for NIS policy making (see also a thorough analysis done in [SYS15]). In addition to the focus area, each sub-section presents actionable recommendations to meet the challenges in the area as well as potential performance indicators for these recommendations.

7.2.1 Key Aspect: National and international cyber security and privacy cooperation and governance

Achieving and maintaining cyber security targets is a challenge that cannot be met alone by a single organization or country, due to the heavy interdependencies in the ICT and cyber security sectors. Organizations depend on each other for their most critical processes and countries depend on each other for the end-to-end functioning of the Internet and its services worldwide. In such an interconnected environment it is important to identify the chain of dependencies accurately, to distribute responsibilities fairly and to maintain accountability. However, when policy makers, and governments in general, have limited jurisdictions at local, national and international level, it becomes difficult to create policies, laws, incentives and enforcement mechanisms to cover the complete, end-to-end chain of dependencies worldwide.

Under these circumstances, it becomes difficult to cooperate for and coordinate cyber security efforts nationally and internationally to the detriment of users and societies. Lack of coordination and cooperation in handling cyber security threats, incidents and responses leads to sub-standard results and associated risks to materialize.

Information sharing is an integral part of cooperation. However, there are many challenges in this field. The stakeholders are reluctant to share information among themselves as this might bring liabilities to them in current legal frameworks. Incident reporting and breach notifications are hot topics in the area. Mandatory reporting and incentive driven approaches are yet to be proven effective. Sharing vulnerability and threat information is currently inadequate. Once an information sharing framework and governance mechanism are established, this would lead to better research results in this field as well since currently, research projects cannot find sufficient data to work on.

International standards are an indispensable element of interoperability which is a cornerstone of cooperation and collaboration. Without standards for operations, tools and technologies, it becomes very difficult to cooperate. Yet, lack of strong, applicable standards in cyber security and privacy is consistently emphasized.

It is for all policy makers worldwide to be aware of this challenge and to build a worldwide cyber security cooperation and coordination environment using breakthrough mechanisms.

7.2.1.1 Recommendations/Opportunities:

1. Creation of an international cyber security and privacy executive organization or watchdog: Similar in nature to international organizations monitoring the global economy, health or the proliferation of prohibited substances, an organization could be created with appropriate powers and responsibilities to coordinate international cyber security efforts. We are in a transition phase. While there is currently a need for a cyber security watchdog to coordinate international cooperation in this domain, this watchdog could become obsolete once cyber security is successfully integrated in all national and international processes by design and principle.

2. Creating national, European or international cyber security and privacy certification schemes, compliance frameworks and associated accreditation and audit organizations.

3. Enacting laws and regulations that clearly assign responsibilities and provide accountability criteria without increasing the complexity of legal requirements which are coordinated across jurisdictions to provide end-to-end coverage in the cyber security and privacy chain of dependencies.

4. Supporting the creation and use of effective metrics for vulnerabilities, threats, incidents, mitigation functions and their financial implications.

5. Creation of a best practice exchange for cyber security and privacy practitioners.

6. Financial and cooperative incentives for incident and breach notifications.

7.2.1.2 Performance indicators

1. National and international cyber security and privacy exercises: One of the methods to see the capabilities and readiness of organizations and nations in the face of cyber security incidents and threats is to carry out exercises with the participation of all stakeholders. These exercises bring out the deficiencies in coordination and cooperation as much as in

technical competencies. A key aspect is continuity. Once these exercises are carried out periodically, one can observe the progress made.

2. Cyber security and privacy stress tests: Much like in the financial sector, major organizations, nations and international agencies might be the focus of cyber security and privacy readiness stress tests. Continuous application of the tests would be necessary for progress monitoring.

3. Cyber security and privacy surveys: Periodic surveys carried out among all stakeholders and users would help keep the pulse on the perception of key players in the global cyber security effort.

4. Number of national and international cyber security standards, certification schemes and frameworks and their adoption statistics.

5. Cyber security and privacy metrics: Once established, cyber security and privacy metrics will help monitor the state of national and global cyber security efforts.

7.2.2 Key Aspect: Balancing cyber security and privacy requirements

Societal and governmental requirements for security and personal needs of privacy are often seen as counter forces. These divergences often emerge as individual/fundamental rights and freedoms versus security law enforcement as well as anonymity versus trust and security. Surveillance in particular is a hot topic, especially when its purposes and methods are not well-understood.

From a digital identity management perspective cyber security requirements demand traceability while privacy advocates often press hard for anonymity. There is a need for both in different contexts and identity management mechanisms would need to cover both – yet this is an elusive target if left to technology alone. It is for policy makers to build a societal consensus on the issue with potential compromises since the physical world does not exactly match the digital world when it comes to anonymity.

Another challenge in the field is between control and protection of personal data and the use of direct and derived data (correlation) for emerging new services and products. Control over personal data is difficult when data provenance is hard to determine. Regulations are often inconclusive in the area and the responsibility falls to individuals to protect their rights in this uncertain domain, often with great opposition from industry players. A holistic approach to regulate this space would be beneficial.

Building a balance between security and privacy is essential for building a more trusting society and a well functioning and inclusive economy.

7.2.2.1 Recommendations/Opportunities:

The following measures could help construct the balance between privacy and security:

1. non-intrusive security,

2. oversight: regulate surveillance activities,

3. transparency and accountability,

4. user centric data protection regulations,

5. effective digital identity management that can accommodate anonymity when needed,

6. users' control and protection of personal data that can prevent data correlation.

7.2.2.2 Performance indicators

1. Reduced complaints by individuals regarding the violation of their personal rights and freedoms, and data breaches,

2. National data protection agency reports and analyses,

3. Law enforcement agency disclosure requests to Internet companies dropping (since there are effective identity management schemes in place).

7.2.3 Mitigating the concentration of strategic cyber security resources and technologies outside Europe

Creating a vibrant European NIS market is a key target and challenge emphasized in most NIS related policy discussions. With governments, organizations large and small and individuals depending on tools and technologies sourced from outside Europe, it is extremely difficult to enact and implement policies that reflect European strategies and priorities. While this external dependency is present in most Internet technology domains, its implications are far more concerning in the cyber security and privacy domains as reflected in the recent revelations about surveillance operations.

While the primary focus of mitigation strategies would be to increase the number of European companies, technology and tools in this domain in the long to medium term, in the short term, analyzing, testing and accrediting externally supplied products and technologies according to European standards and criteria should also be part of the strategy. What is critical is that externally supplied products and services should be able to demonstrate their trustworthiness according to transparent criteria. Today, most products and services are presented as black box components which need to be trusted as is. Using open-source tools provide a level of relief in this respect.

7.2.3.1 Recommendations/Opportunities:

1. Create inventory of firms and technology capabilities and monitor continuously the match with R&I priorities (strategic + tactical levels), identifying the gaps.

2. Provide financial support: especially to SME's in this domain.

3. Use public procurement as a tool to support emerging tools and services.

4. Support R&I → products and services transition programs.

5. Industry participation in and funding of R&I and PPPs: if industry funds all or part of research and innovation projects, their results could be more willingly adopted by these companies.

6. Encourage the use of open source tools and technologies that are hardened according to security and privacy criteria.

7. As stated in the first subsection above: Creating national, European or international cyber security and privacy certification schemes, compliance frameworks and associated accreditation and audit organizations.

7.2.3.2 Performance indicators

1. The number and breadth of European cyber security and privacy companies increase and the gaps between these and the European R&I priorities in this area close.

2. The number of products and services that submit to security and privacy certification and accreditation increase.

3. The amount of private R&I funding for projects increase.

4. The transition from R&I to products accelerates.

5. Usage of open source security and privacy tools increase.

7.2.4 Key Aspect: Critical infrastructure protection

While user empowerment and a user centric approach constitutes one pillar of an effective cyber security strategy, another one is critical infrastructure protection. While technical research challenges in the general cyber security domain may be similar to those in the critical infrastructure sector, there are many specific challenges in the critical infrastructure sector from a policy perspective.

From a cyber security perspective, critical infrastructure sector may be a small market as compared to the general ICT market sector. Within this sector the industrial control system component (SCADA) constitutes an even smaller yet a most critical part. Therefore it is potentially under served by security companies and researchers which demands incentives to bring it up to par with the rest of the ICT security sector. Critical infrastructure operators often find themselves dependent on proprietary, expensive and often obsolete technology.

Upgrading critical ICT infrastructures in general and SCADA systems in particular is a risky process due to the critical impact of potential failures. Therefore, upgrades are not performed very often or systematically in this sector which creates serious vulnerabilities. Tight regulations may be needed to formalize the management of ICTs in the critical sectors.

Another challenge for policy makers is on designating critical infrastructures. By different norms, varying number of domains fall into this category and there doesn't seem to be a global consensus on this topic. Without these definitions, nations often fail to identify their critical infrastructures and do not provide special care for them.

7.2.4.1 Recommendations/Opportunities:

1. Create incentives and financial instruments to make it more attractive for companies and researchers to work on critical infrastructure security requirements.

2. Regulate the ICT and SCADA dimension of critical infrastructure operations from a cyber security and resilience perspective.

3. Propose critical infrastructure criteria and obtain wide consensus on these criteria.

7.2.4.2 Performance indicators

4. Increase in the number of alternatives for critical infrastructure SCADA components as well as the market size for the security of these components.

5. Existence and wide adoption of regulations for critical infrastructure sector ICT and SCADA systems.

6. Existence of international consensus on critical infrastructure definitions and norms.

7.2.5 Providing facilities for NIS research experimentation

NIS (network and information security) arena is then different from other arenas and other market segments. Indeed, it is asymmetric, that is, it is an adversarial game in which just a small flaw and a small investment is enough for a cyber-attacker to succeed, while, at the same time, big investments by organizations are taking place to prevent, detect and response to those attacks in an ever increasing complexity and escalating scenario, where sometimes those investments are completely ineffective if a small flaw with great impact associated is exploited.

Several studies, research and literature are available about the specificity of **cybersecurity research & innovation ecosystem**, timescales and asymmetry, and all of them provide with recommendations in terms of:

- **Experimental** cybersecurity research is needed to **shift the asymmetric** cyberspace context to one of greater **planning**, **preparedness**, and **higher assurance** fielded solutions.
- **Emphasis on** isolated and niche equipment and related software solutions **alone** will **fall far** short of achieving the **transformational shift** in research, **community**, and supporting **experimentation** required to address cybersecurity in the **ever escalating** cyber environment.
- **Strong**, **coupled**, and **synergistic** advances in **fundamental methodological** development, fostering and leveraging **communities of researchers**, and advancing capabilities of the **infrastructure supporting that research**, will move the field beyond today's state of the art.
- Support for **cross domain and multidisciplinary experimentation** is recommended that includes computer science, engineering, math/modeling, human behavior, sociology, and economics. The views, perceptions and behaviors of the different fields cannot be ignored because it could be decisive to obtain optimal results.
- **Portability of experiments**, packaged for sharing and re-use in cross-discipline experiments – provides also effectiveness.

A shared, vetted community experimentation capability at EU, as a Cybersecurity **Testbed** can reduce the risk of error, ultimately improving the quality of research and thus innovation of resulting European products.

European cybersecurity **Testbeds** and their **federation** could collect and provide results in a short, medium and long term for all the stakeholders, even if they have different levels of maturity in the

field or if they represent a different part of the value chain. The real value for every actor involved consists in how they apply the obtained results.

Inside cybersecurity arena, research and innovation are usually processes not well synchronized to provide useful business innovative & short term time to market results from research. Testbeds will help to speed up the process and have a better R&I processes synchronization.

Another advantage by using a cooperative approach, it is to get multidisciplinary research environments at all different levels and the possibility to test solutions with different networks, realistic or simulated attacks, new cost-effective approaches and make solutions taking into account more specifications as a result of that common approach.

7.2.5.1 Recommendations/Opportunities:

- **Cybersecurity Testbed and its instantiations:**

  Holistic approach is required to frame the future of Cybersecurity Testbeds to first come up with a product Vision encompassing all the features that a Cybersecurity experimental facility (or Testbed) should offer and second enable those features to happen through research and technology advancement. Once developed the Cybersecurity test bed can be assembled and made available for any of the targeted stakeholders (including experimenters, researchers, trainers…) to create its own instance and perform its work in a controlled manner also report on it. Overall it is important to learn from any of the stakeholders to further advance the Cybersecurity Testbed product to get it complete and up to the task also benefitting from each of the disciplines at stake. It is also important to learn from domain specific instances once created.

- **Cybersecurity Testbed governance and community building:**

  Goverance of Cybersecurity Testbed should be carefully defined to be open to any of the stakeholders (e.g. users, researchers, …) interested to use it and/or ready to contribute to it. Also entry barrier should be lowered through dedicated actions (e.g. Training material and sessions). Usages of Cybersecurity Testbed and its instances should also be tracked and reported since source of further improvement. Cybersecurity Testbed governance should also target interested and/or interesting communities to make it sustainable in the mid-term.

7.2.5.2 Performance indicators

How to measure the success of the exploitation of the previous opportunities

- Number of adopters (starting first with early adopters)
- Level of completion of Cybersecurity Testbed product vision (focus on service offering and especially very innovative services enabling the new usages)
- Number of Testbed instances deployed (total and by research priority)
- Cybersecurity Testbed services/features offering (focus on usefulness and usability of the tools/processes/services)
- Training facilities offered

- Number of Cybersecurity experiments conducted on the Testeds (also their ranking and stressing the ones specifically enabled)
- Capacity to attract communities or create community to make Cybersecurity Testbed sustainable
- Number of tools/processes/services contributed within vs outside of the Cybersecurity Testbed community.

7.3 Business/innovation

7.3.1 Key aspect: A systems approach to security

NIS solutions must be recognised as complex human-technical systems consisting of many dissimilar elements that must work together harmoniously; consequently, they require a holistic approach. NIS is not a technology itself, but a mind-set and a collection of principles that must be applied in a technical and organisational/social context. The pace of innovation in technology and in the business practices, leisure activities and societal institutions that exploit it, means that NIS must re-invent itself continuously. It is straightforward to list current technical and process innovations that are problematic conventional security approaches (Cloud, Internet of Things, Mobility, etc.) and we can be sure that the years between now and 2025 will bring further challenges. While the specific innovations are difficult to anticipate, it is probable that the trends of increasing technological diversity, ubiquity, interconnectivity, complexity, shared usage and interdependence will result in a global, common, ICT infrastructure that is critical to society and the world economy, and which is likely to remain vulnerable to attack.

Currently, technical security measures are largely used independently, with people providing the matrix that integrates the components. In the future, the pace of response required means that the technical systems will need to co-operate directly. A recent market report says the following:

> *The time for selling a host of disconnected security products and hoping for the best has long gone. Enterprise organizations need integrated security solutions that work, providing the security monitoring and management information to identify new threats and improve performance levels. Where new technology deployments are the answer, they need to be targeted at the specific vulnerabilities of the organization and when delivered they need to be maintainable in line with its operational capacity for risk. The delivery of security services needs to be seen as a partnership between vendors and their clients where the value-add comes from the practical advice and help a security specialist is able to offer, both on a regular basis and when specific problems occur. '2015 Trends to Watch: Security'*

In a mature market for NIS, a customer (either an end-customer or an intermediary in the value chain) seeking an element to play a particular role in a system should be able to choose among several comparable alternative products and services from different providers. While these may differ in price, implementation technology and effectiveness, they should essentially be substitutable one for another. Similarly, products and services from different providers that play complementary roles within a system should be compatible and interoperate with each other. If this is not the case, the scope for innovation is limited.

The need for integration has implications for the dynamics of innovation as it is more difficult for a radically different approach to penetrate the market due to the need for a new product or service to be compatible with the existing elements with which it must interact.

7.3.1.1 Recommendations

There is need for research on the analysis, design and operation of dynamic systems and the understanding and prediction of their properties. This is needed to allow the reliable construction of solutions that satisfy the requirements of demand-side stakeholders in the face of the prevailing threat. In general, such solutions will combine people, processes and technology, so the science will need to encompass an understanding of (benign and malicious) human behaviour and how to influence it, as well how to combine human and technical elements harmoniously and synergistically. Although people will remain an important part of the solutions, the shrinking window for timely response to attacks make an increasing degree of autonomous operation of technical controls essential. People will set policies enacted by autonomous controls, monitor their operational effectiveness and adapt them as required.

To minimise the need for re-implementation, security innovations should minimise dependence on implementation context. This could mean, for example, definition of an abstract pattern that can be applied in many contexts or implementation as generic capabilities or services that can easily be coupled to an application platform via a thin integration layer.

Stimulating and fostering the emergence of an understanding of sets of abstract product/service roles that can be combined in various ways to satisfy NIS requirements, is an important aspect of an SRA. The NIS research and innovation portfolio should include projects that are aimed at defining and maintaining reference architectures, frameworks and interface standards, and encourage and co-ordinate the creation of ecosystems of compatible and interoperable products and services across a cluster of research and innovation projects. It is important that these architectures, frameworks and standards are defined in such a way as to promote competitive innovation, and should themselves be designed for evolution.

One approach to establishing such frameworks that appears promising is based on defining and analysing a representative selection of demanding use case scenarios. In each case, demand-side stakeholders of different types are identified: e.g. process owners, process participants, and regulators (concerned with wider organisational or societal issues), and their security objectives and concerns in that scenario described. A collection of future security services that would meet their requirements is then hypothesised. The future service concepts resulting from the scenarios are then correlated and generalised to produce a number of sets of compatible security capabilities. One proposal is that this approach be adopted by an existing Horizon 2020 Co-ordination and Support Action (CSA), or provide the basis for a new one.

A related idea is to fund the establishment of experimental testbeds / innovation incubators with access to real data and simulated threat and application scenarios. These would be shared resources accessible to a wide range of stakeholders and would support research, innovation and validation. Cross-project experimental prototyping would be strongly encouraged, or even strictly required. The testbed environments themselves could act as prototypes for innovation-friendly operational platforms.

7.3.2 Key aspect: Mismatch of research and innovation timescales

Research and innovation are distinct, but related, processes that must combine harmoniously if significant positive impact on society is to be realised. Research is concerned with generating new knowledge; utilising this knowledge to achieve beneficial changes is the role of Innovation. Progress in research typically requires in-depth study over 2-5 years, whereas innovation is about satisfying requirements and responding to opportunities, which may be short-lived. This can be a problem in rapidly evolving fields such as NIS.

NIS involves an arms race in which tools and tactics used by attack and defence are co-evolving. This makes the future threat environment highly dynamic and extremely difficult to predict. Furthermore, the number, diversity, organisation, persistence and sophistication of threat agents

facing the defender is continually growing, with some having a high degree of expertise, organisation, motivation, persistence and financial and political backing. Even amateur threat agents have easy access to powerful, automated attack tools. Currently, threat agents have the upper hand, so our aim must be not only to maintain the status quo regarding security risk exposure, but to gain the initiative from them. Thus, we are faced with two issues:

1. It is difficult to anticipate future requirements in order to formulate stable goals for traditional research project;

2. There are urgent requirements that are not being satisfied and business opportunities lost

In consequence, future NIS solutions will need be continuously evolvable in order to establish and maintain a lead over the threat without leaving windows of vulnerability.

7.3.2.1 Recommendations

1. Most research projects solve problems of the future and the first results are available in 3-4 years, whereas customer needs and expectations, especially in cyber security, are close to immediate. This problem deserves special support and treatment, maybe through the open calls managed by individual projects or dedicated platform.

2. We need to develop an 'agile R&I' process model that both accelerates research results into practical use, and uses market intelligence to adapt the direction of research market/threat environment evolves.

3. The NIS research and innovation portfolio should include projects that are aimed at providing an innovation-friendly platform, i.e. a technological environment in which a range of novel applications, products and services can be brought to market or deployed rapidly.

7.3.3 Key aspect: Innovation models

Innovation models have evolved from insular, linear, and reactive models of innovation towards the more contemporary models that are fluid and adaptable processes that aim to raise development efficiency and speed to market through inter-organisational cooperation and strategic alliances. A review of R&I process models in use in WG3 member organisations and reported in academic papers in order indicates that most espouse variants of Open Innovation, whereby the R&I value chain is enacted by an open ecosystem of small and large enterprises, individual inventors, research institutes and universities. Large enterprises are experimenting with a variety of schemes to stimulate and benefit from entrepreneurial activities outside their organisations. Similarly, national and EU research programmes are trying out new instruments designed to encourage participation by small companies and to grow this sector of the market. Information gathering and analysis is still in progress, but it appears that while the general philosophy of Open Innovation is shared, there is considerable variation in how it is interpreted and applied, and a consensus on best practice has yet to emerge.

7.3.3.1 Recommendations

1. NIS R&I projects should include market studies for their technologies and consider lifecycle costs to ensure market-viability of their technology.

2. Business cases for disruptively innovative products need to take into account the difficulty of displacing incumbent solutions arising from dependency networks, regulations (which can either promote or inhibit innovation) and other potentially inhibitory factors.

3. Research is needed to look at market dynamics aspects of innovation in NIS.

7.3.4 Key aspect: Serving society

NIS must serve the needs of European society as reflected in public opinion, government policy, and legal and regulatory frameworks, and must do so in a transparent and accountable way. However, the wishes of society are a dynamic equilibrium of sometimes-conflicting drivers, with the balance point affected by many factors including events, such as terrorist attacks, leaks of personal data, and revelations about government surveillance programmes. This results in a fragmented and unstable legal/regulatory/oversight environment.

7.3.4.1 Recommendations

1. There is a need for harmonisation of regulatory environments in the different legal jurisdictions around the globe. Care must be taken that obligations are not overly prescriptive as this may prevent innovation and result in regulations becoming outdated as technology and business practices advance.

2. Private sector businesses have an important role to play in responding to societal challenges, but the need for companies to recover costs, make a fair return of investment, and maintain a competitive advantage must be recognised and taken into account. Businesses may also be faced with conflicts of interest between disclosing information to comply with legal obligations and serving the interests of their customers and shareholders.

3. There is a need for federation of NIS systems to support co-operation among enterprises, law enforcement agencies, and national and European authorities. At any compositional level, it should be possible to define meaningful risk metrics that can be calculated operationally to allow continuous monitoring, and also policy-based means of influencing system behaviour in a predictable way. Such mechanisms to assert rights and enforce transparency and accountability should be available to all legitimate stakeholders in the system.

7.4 Education and training

7.4.1 Key aspect: Multi-disciplinary focus

For the purposes of this work, we have accepted a broad definition of cybersecurity that comprises a wide range of relevant topics, from cryptography, computer, information and network security to privacy, security economics, or legal, regulatory, and policy frameworks.

Although there is general agreement about multi-disciplinary nature of cybersecurity, it remains difficult to reflect the need for multi-disciplinarity in teaching and training environments, because of the diverse skill sets required for truly integrated programs. While a number of multi-disciplinary programs and centres are in place, acquiring in-depth skills in multiple subjects rather than lighter supplemental skills around the area of specialization remains rare. As a result, professionals with understanding of technology as well as law, policy, psychology, or economics are uncommon. Yet, professionals with multi-disciplinary skills continue to be at the top of the lists of skills gaps, according to reports and surveys.

Multi-disciplinary research that is necessary to feed multi-disciplinary programs also continues to be fragmented. Although efforts had been made to support multi-disciplinary approaches to cybersecurity, funding mechanisms, availability of publications and conferences that support multi-disciplinary work are insufficient.

Ultimately, fragmentation of knowledge in cybersecurity impacts all aspects of society, from the technology environment to legal and policy frameworks.

7.4.1.1 Recommendations

1. Support multi-disciplinary curricula and training, with clear goals for professional preparation, to ensure future workforce is capable to address complex cybersecurity problems.

2. Continue to build infrastructure to encourage multi-disciplinary skill development in cybersecurity including curricula and programs in higher education, funding for multi-disciplinary research, and establishment of for a for multi-disciplinary work.

3. Evaluate collaboration mechanisms to enable universities in the EU to provide multidisciplinary degrees when a certain specialization is not available at the degree institution.

4. Evaluate and extend mechanisms for "custom degrees" in cybersecurity (designed y students), especially graduate level degrees for professionals already engaged in one aspect of cybersecurity.

5. Establish infrastructure to enable specialists in various areas in cybersecurity to add multidisciplinary knowledge through additional educational modules (e.g., for a computer scientist specializing in security to add a three month module on legal frameworks or economics of security).

6. Establish prizes for successful multi-disciplinary work in cybersecurity.

7.4.2 Key aspect: Responsiveness to changes in technology and societal environment

With increasing diversity and dynamic nature of the computing environment, a static approach to teaching cybersecurity skills is no longer effective. Today, most environments are dynamic, with entities (e.g., devices and users) joining and leaving domains. Most processes are cross-domain operating in ecosystems with multiple security models and different vulnerabilities.

Figure 1. Cross-domain processes
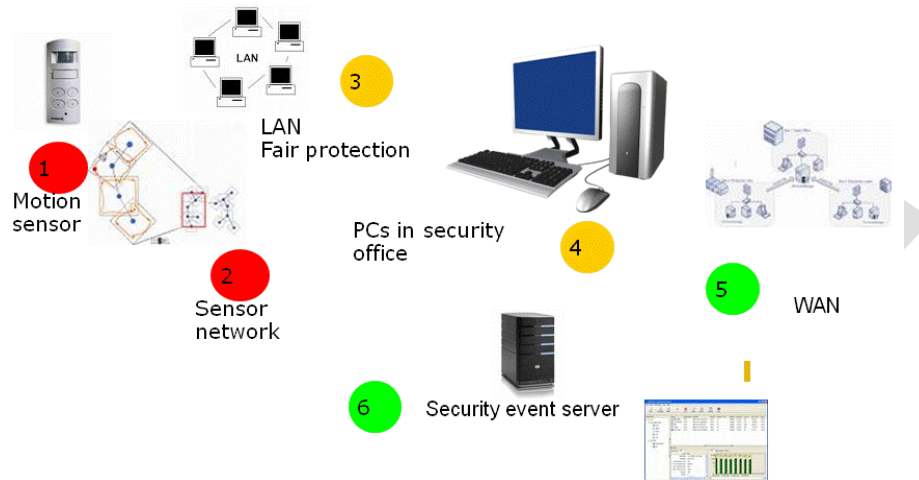
The issues of security composition in complex environments or security and privacy challenges arising at the intersection of several domains remains unresolved, and effects of this complexity on security remain unknown. Preparation and training of cybersecurity professionals continues to focus on one domain, further affecting technologists' understanding of inter-dependencies that need to be considered.

Approaches used for teaching technical and societal aspects of cybersecurity continue to focus on the development of fundamental skills and knowledge in key areas, similarly to teaching fundamental sciences or law. It remains crucial to acquire fundamental skills, and the importance of this aspect of education and training will never decrease. No continued education is possible before solid fundamental skills are acquired. However, the dynamic nature of the technology environment, as well as reactive components and positioning of cybersecurity make it imperative to create additional mechanisms to acquire and continue to develop new skills and knowledge as the environment evolves.

The emergence of the new mechanisms to address the quick evolution of technology and usage models will permit us to prepare professionals with deep fundamental knowledge and the ability to solve the new problems as they emerge. Better knowledge of the connections and dependencies in the ecosystem will make it easier to select solutions that are more effective.

A more responsive approach to evolving technology environment in cybersecurity curricula and training is needed to help ensure quicker alignment of approaches to teaching cybersecurity across the EU, rapid awareness of emerging global issues or new solutions, and greater competitiveness of the EU members.
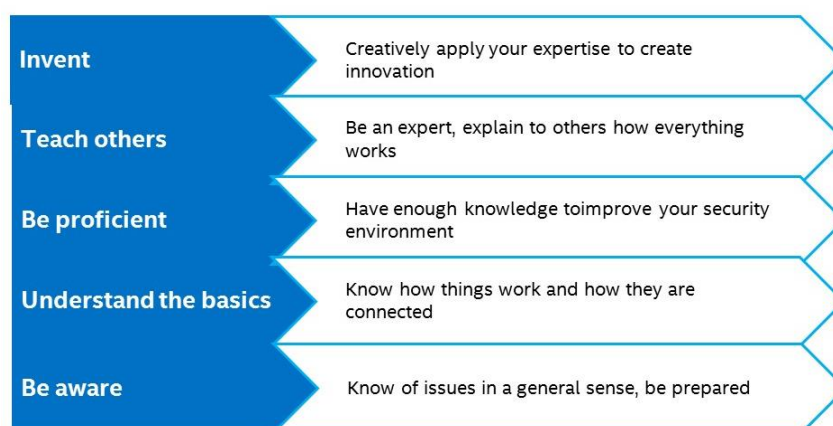
7.4.2.1 Recommendations

1. Establish a task force with an advisory focus to provide recommendations to increase agility, responsiveness, and multi-disciplinarity in cybersecurity and privacy education.

2. Institute an annual survey of employers in cybersecurity to publish lists for skills in highest demand for the next 1-2 years.

3. Devise mechanisms to develop and deploy community built sharable curriculum and training modules in cybersecurity in order to make curricula and training more agile and responsive to real life security threats and changes in the technology environment.

4. Establish ways for professionals to update their knowledge of latest technologies online.

5. Support international collaboration and awareness campaigns, to ensure all EU countries are aligned on levels of proficiency and aware of globally significant issues in cybersecurity

7.4.3 Key aspect: End-to-end skill development

With the digital world becoming integral part of everyday life from an early age, awareness of cybersecurity and privacy issues and elementary skill development should become more organic. Acquiring fundamental skills earlier and organically, as part of regular education, will not only help develop the competence of consumers to take important decisions, but also the preparation of experts and innovators in cybersecurity and privacy. We can illustrate the levels of proficiency as a stack, starting with passive awareness and moving toward innovation at the highest level (see Figure 2 below). Ensuring that more people move from the lowest to the higher levels of proficiency will positively affect the technology environment; development of secure devices, networks, and applications; effective remediation following cybersecurity attacks, and, ultimately, innovation. Focusing on higher education and expert training only is likely to have reduced impact through the loss of opportunity for talent development early in the skill development cycle.

Figure 2. Levels of proficiency in cybersecurity

Invent	Creatively apply your expertise to create innovation
Teach others	Be an expert, explain to others how everything works
Be proficient	Have enough knowledge toimprove your security environment
Understand the basics	Know how things work and how they are connected
Be aware	Know of issues in a general sense, be prepared

7.4.3.1 Recommendations

1. Support research to define curriculum & training requirements including coordination actions for these activities with end-to-end coverage (from minimal proficiency to dedicated curriculum).

2. Invest in development of communities of practice operating mostly through online interactions.

3. Establish a task force with an advisory focus to address strategic requirements of end-to-end cybersecurity and privacy education in order to develop consistent analysis of the dependences among different levels of education and establish concrete measures to encourage continued acquisition of skills in cybersecurity.

4. Support research to develop new mechanisms to provide greater visibility of cybersecurity and privacy vulnerabilities when using common devices, systems, applications, and processes.

5. Support programs focusing on interaction of people with different levels of proficiency.

6. Encourage earlier start for cybersecurity awareness and acquisition of basic skills, to coincide with independent use of connected devices. The earlier start will lead to greater proficiency in security and privacy skills by all consumers and will facilitate the introduction to more advanced and responsive curricula and greater understanding of cybersecurity requirement by computer scientists

7. Encourage entrepreneurship in cybersecurity defining a path from skills acquisition to innovation.

7.4.4 Key aspect: Alignment of curricula and training with demand for skills

Most reports on cybersecurity skills agree that the shortage of cybersecurity professionals is becoming more acute and highlight the sharpest shortages occurring either with regard to the latest skills or at the top of the profession where experience or multi-disciplinary knowledge are essential. The shortage continues to be felt in government, while industry and academia developed some avenues to deal with shortage of skills at the high end of the profession through additional education and, in industry, internal promotion. The skills shortage is connected to the fact that cybersecurity profession is not yet well defined, negatively affecting the effectiveness of cybersecurity education and training.

The complexity of the technology environment and regulatory frameworks as well as quick evolution of technology and cybersecurity threats creates a great diversity of needs among potential employers that remains hard to address.

Greater collaboration of stakeholders in cybersecurity – governments, academia, and industry—is necessary to align perceptions of the needs for skills and vehicles to combine theoretical and practical training. While many industry members and other communities have established programs to support and encourage the design of adequate curricula in cybersecurity, these efforts remain fragmented and receive minimal support from funding agencies in Europe and elsewhere.

Similarly, apprenticeship and internship programs continue to develop as needs for employees with cybersecurity skills is growing, but very few innovative mechanisms to support short-term skill development programs have been established.

Finally, awareness of skills in high demand remains delayed and imperfect, putting additional pressures on students, educators, job seekers, and employers and negatively affecting competitiveness of the EU countries.

7.4.4.1 Recommendations

1. Support development and enhancement of collaboration mechanisms with industry and government and internationally, in order to ensure consistent coverage of cybersecurity proficiency in all EU countries

2. Encourage new flexible models for short terms internships and training in operational environments to develop purpose-based acquisition of top-priority skills.

3. Support emergence of fora for interaction with practitioners across Europe.

4. Establish mechanisms to increase awareness of skills in high demand to increase competitiveness of job seekers.

5. Establish high quality mechanisms for on demand acquisition of high priority skills, open across the EU, including the countries where such mechanisms may not be readily available.

7.4.5 Key aspect: Using appropriate methodologies for teaching cybersecurity at all levels, from awareness to focused expertise

Although online learning is used in teaching cybersecurity skills, the majority of the educational approaches remain traditional. This is not surprising or incorrect, since cybersecurity shares fundamental premises with computers science, mathematics, or law, depending on the aspects of study. However, traditional approaches still prevail in teaching elements of cybersecurity that are either completely practical, very process dependent, or time dependent. Among examples of such topics, we can mention translation of philosophies (e.g., for Privacy or Security by Design) into concrete product or technology development requirements; remedies against latest cyberattacks, or learning how to configure a firewall.

Focused approaches to teaching cybersecurity were proposed and are used in some settings. Many of them are "challenge-based" and preparing students to take the correct decisions in response to structured challenges. MOOC, competitions, apprenticeships, user interfaces and many other methods could be used in this environment.

We need a thorough examination of how to position teaching of cybersecurity with regard to university curricula and practical applications.

7.4.5.1 Recommendations

1. Initiate a study of teaching methodologies for cybersecurity and provide a set of recommendations on this topic.

2. Study "casual" learning of cybersecurity as part of other activities and publish recommendations with regard to processes, interfaces, and metrics for this method of learning.

3. Organize and promote regular cybersecurity competitions at all levels.

7.4.6 Key aspect: Bring all Member States to the agreed upon baseline with regard to cybersecurity indicators

Some eSkills report[41] undertaken for EU Member States as well as other indicators (e.g., Cyberpower Index[42]) provide evidence of differences between the EU countries in various aspects of cybersecurity, Preliminary submissions to ENISA course database also point to potentially uneven development in teaching cybersecurity.

It is important to ensure that all EU countries have access to cybersecurity learning and materials.

---

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

[42] Cyber Power Index. http://www.boozallen.com/content/dam/boozallen/media/file/Cyber_Power_Index_Findings_and_Me thodology.pdf

7.4.6.1 Recommendations

1. Task ENISA with creating a report comparing access to cybersecurity education and practical training among EU Member States.

2. Explore methodological and class delivery options to increase access to cybersecurity courses and programs across the EU.

3. Explore feasibility of a practical training internship allowing interested and motivated students from EU countries with lower numbers of cybersecurity courses and opportunities to receive practical training via dedicated programs in other Member States.

8 Conclusion

TBD

9 References

[RAN13] K. Rannenberg: Where Security Research Should Go in the Next Decade. In: Willem Jonker, Milan Petković: Secure Data Management; Vision Papers on Occasion of the 10th VLDB Workshop, SDM 2013, pp 28-32, Trento, Italy, August 30, 2013; Springer LNCS 8425, ISBN: 978-3-319-06811-4

[GER83] German Constitutional Court: Volkszählungsurteil: Urteil v. 15. Dezember 1983, Az. 1 BvR 209, 269, 362, 420, 440, 484/83; www.servat.unibe.ch/dfr/bv065001.html and Mitglieder des Bundesverfassungsgerichts (Hrsg.): Entscheidungen des Bundesverfassungsgerichts. 65, Mohr, Tübingen, S. 1–71, ISSN 0433-7646; unofficial English translation on https://freiheitsfoo.de/census-act/

[EC00] Official Journal of the European Communities. Charter of Fundamental Rights of the European Union. C 364/1, 18.12.2000

[EP14] European Parliament and of the Council. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC; http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

[TIM14] The Irish Times article. *Global data set for explosion as 'internet of things' takes off.* April 9, 2014.

[NIS14] NIS Platform Working group 3. State-of-the-art of secure ICT landscape (final, version 1), July 2014.

[SYS13] SysSec. The Red Book: A Roadmap for Systems Security Research. 2013. Available via http://www.red-book.eu/

[SMI10] D. Smith, K Simpson, "Safety Critical Systems Handbook: A Straightforward Guide to Functional Safety, IEC 61508 (2010 Edition) and Related Standards, Including Process IEC 61511 and Machinery IEC 62061 and ISO 13849" (3rd Edition ISBN 978-0-08-096781-3, Hardcover, 288 Pages).

[MAT13] R. Mattioli, T. Haeberlen. Understanding the importance of the Internet Infrastructure in Europe – Guidelines for enhancing the Resilience of eCommunication Network, TLP Amber, December 2013.

[EC05] European Commission. Green Paper on a European Programme for Critical Infrastructure ProtectionCOM 576, 2005.

[CYS13] CYSPA Consortium: CYSPA Project Deliverable D2.3 - Trends and threats impact contribution, 2013.

[ERC14] ERCIM ERCIM White Paper on Cyber-Security and Privacy Research (http://www.ercim.eu/images/stories/pub/white-paper-STM.pdf).

[CAP14] CAPITAL project. CAPITAL Deliverable D2.1 Emerging Areas of Information Technology, 2014 (draft version).

[ALO12] F. Aloula, A. Al-Alia, R. Al-Dalkya, M. Al-Mardinia, and W. El Hajj. SmartGridSecurity: Threats, Vulnerabilities and Solutions. In International Journal of Smart Grid and Clean Energy, vol. 1(1), pp. 1-6, 2012.

[LIN14] H. Lin, and Y. Fang. Privacy-aware profiling and statistical data extraction for smart sustainable energy systems. In IEEE Transactions on Smart Grid, vol. 4(1), pp. 332–340, 2014

[NES14] NESSOS project. NESSoS Deliverable D11.4 - Pilot applications, evaluating NESSoS solutions, 2014.

[GIA12] G. Giannopoulos, R. Filippini, M. Schimmer. Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art. Joint Research Center Publication, JRC 70046, EUR 25286 EN, ISBN 978-92-79-23839-0, ISSN 1831-9424, doi: 10.2788/22260, Luxembourg: Publications Office of the European Union, 2012.

[STE10] J. P. G. Sterbenz, D. Hutchison, E. K. Etinkaya, A. Jabbar, J. P. Rohrer, M. Schoeler et al., Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines, Computer Networks, Vol 54, pp. 1245-1265, 2010.

[HER10] I.A. Herrera, R.Woltjer, Comparing a multi linear (STEP) and systemic (FRAM) method for accident analysis, Reliability Engineering and System Safety 95, pp. 1269-1275, 2010.

[NTO12] T. Ntouskas, N. Polemi. Collaborative Security Management Services for Port Information Systems. DCNET/ICE-B/OPTICS, pp. 305-308, 2012.

[NIN12] Nineta Polemi, Theodoros Ntouskas. Open Issues and Proposals in the IT Security Management of Commercial Ports: The S-PORT National Case. pp. 567-572, 2012.

[PED06] P. Pederson, D. Dudenhoeffer, S. Hartley, M. Permann. Critical Infrastructure Interdependency Modeling. A Survey of U.S. and International Research, INL, INL/EXT-06-11464, 2006.

[STE01] S. M. Rinaldi, J. P. Peerenboom, T. K. Kelly. Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies, IEEE Control Systems Magazine, pp. 11-25, December 2001.

[CYS13b] CYSPA Deliverable D.2.1.1: Impact Report Transport Sector, 2013.

[WEN14] S. Wendzel, V. Zwanger, et al. Envisioning Smart Building Botnets. In Proceedings of SICHERHEIT, Vienna, GI, 2014.

[SZL14] S. Szlósarczyk, S. Wendzel, et al. Towards Supressing Attacks on and Improving Resilience of Building Automation Systems – An Approach Exemplified Using BACnet. In Proceedings of the SICHERHEIT, Vienna, GI, 2014.

[WEN14b] S. Wendzel, C. Herdin, R. Wirth, et al. Mosaic-chart based Visualization in Building Automation Systems. In Proceedings of the 9th Security Research Conference on Future Security, Berlin, 2014.

[AND10] R. Anderson, S. Fuloria: Security Economics and Critical National Infrastructure. In Economics of Information Security and Privacy, Springer, pp. 55-66, July, 2010.

[EC13] DG CONNECT (European Commission). A vision for public services, 2013.

[AND11] K. J . Andreasson. Cybersecurity Public Sector Threats and Responses, , pp. 1–26, CRC Press, 2011.

[CAP13] CAPITAL project. CAPITAL D2.3 – List of current and future cyber security threats, 2013

[KOU13] F. Koushanfar, A. Sadeghi, H. Seudié. EDA for Secure and Dependable Cybercars: Challenges and Opportunities. In Proceedings of the DAC 2012. San Francisco. 2012.

[MUS13] A. Mustafa et al. Smart Electric Vehicle Charging: Security Analysis. Innovative Smart Grid Technologies (ISGT), IEEE. 2013

[CHE11] S. Checkoway, D. McCoy, B. Kantor et al. Comprehensive Experimental Analyses of Automotive Attack Surfaces, 2011.

[PWC12] PwC. "Insurance 2020: Turning change into opportunity", 2012.

[ED09] European Directive 2009/138/EC.

[BIE14] C. Biener, M. Eling, and J. Wirfs. Insurability of Cyber Risk: An Empirical Analysis. The Geneva Papers on Risk and Insurance - Issues and Practice, 2014.

[TOR14] Toregas, C., Zahn, N. (2014), "Insurance for Cyber Attacks: The Issue of Setting Premiums in Context", The Cyber Security Policy and Research Institute (CSPRI), Report GW-CSPRI-2014-1, 2014.

[ENI12] ENISA. "Incentives and barriers of the cyber insurance market in Europe", 2012.

[NES11] NESSoS project. D4.3 Part II Engineering Secure Future Internet Services: A Research Manifesto and Agenda from the NESSoS Community: Final Release, 2011.

[SYS15] The SysSec Consortium. SysSec D4.5, Release 2: Social, Legal and Regulatory Aspects of Network and Information Security in the Future Internet, Release 2, January 2015.

10 Contributors

Strategic Research Agenda - Editors:

Pascal Bisson, Thales

Fabio Martinelli, CNR

Raúl Riesco Granadino, INCIBE

Area of Interest (AoI) - Leaders:

AoI#1: Citizen Digital Rights and Capabilities (individual layer)

Gisela Meister, GI-DE

Kai Rannenberg, Goethe University

AoI#2: Resilient Digital Civilisation (I) (collective layer)

Jim Clarke, TSSG

Nick Wainwright, HP

AoI#3: Trustworthy (Hyperconnected) Infrastructures (infrastructure layer)

Piero Corte, Engineering

Steffen Wendzel, Fraunhofer FKIE

AoIs Cross analysis leaders:

Herve' Debar, Telecom SUD PARIS

Volkmar Lotz, SAP

Aljosa Pasic, ATOS

Neeraj Suri, TU Dortmund

AoI1 – Contributors:

- Gisela Meister G&D

- Kai Rannenberg, Goethe University Frankfurt

- Pascal Bisson, Thales

- Dick Brandt, Ministry of Economic Affairs (NL)

- Fernando Carvaja, INDRA

- George Christou, University of Warwick (PaIS)

- James Clarke, Waterford Institute of Technology

- Herve Debar, Télécom SudParis (TSP)

- Marko Hölbl, University of Maribor

- Nigel Jefferies, Huawei

- Sokratis Katsikas, University of Piraeus

- Mari Kert, European Organisation for Security (EOS)

- Klaus Keus, BSI DE

- Antonio Kung, TRIALOG

- Wouter Leibbrandt, NXP

- Emil C Lupu, Imperial College

- Evangelos Markatos. FORTH

- Manel Medina, UPC- Universitat Politècnica de Catalunya

- Elisa Molino, IBM

- Joachim Posegga University of Passau

- Ali Rezaki, Scientific and Technological Research Council of Turkey (TUBITAK)

- Nikola Schmidt, Technological Platform - Energy Security of the Czech Republic

- Ulrich Seldeslachts, LSEC

- Hervé Seudié, Bosch

- Janne Uusilehto, Nokia

- Nick Wainwright HP

- Andrew Churchill CBRNE

AoI2 – Contributors:

- James Clarke, Waterford Institute of Technology - TSSG

- Nick Wainwright, HP Labs

- Pascal Bisson, Thales

- Dick Brandt, Ministry of Economic Affairs (NL)

- Charles Brookson, ETSI

- Fernando Carvajal, INDRA

- George Christou, University of Warwick

- Zeta Dooly, Waterford Institute of Technology - TSSG

- Raúl Riesco Granadino, INTECO

- Maritta Heisel, Universität Duisburg-Essen

- Marko Hölbl, University of Maribor

- Nigel Jeffries, Huawei

- Sokratis Katsikas, University of Piraeus

- Mari Kert, European Organisation for Security (EOS)

- Klaus Keus, BSI DE

- Antonio Kung, TRIALOG

- Volkmar Lotz, SAP

- Emil C Lupu, Imperial College London

- Evangelos Markatos, Foundation for Research and Technology (FORTH)

- Fabio Martinelli, CNR

- Manel Medina, ENISA

- Gisela Meister, Gieseck & Devrient (G&D) GmBH

- Elisa Molino, IBM

- Joachim Posegga, University of Passau

- Kai Rannenberg, Goethe University Frankfurt

- Ali Rezaki, Scientific and Technological Research Council of Turkey (TUBITAK)

- Michel Riguidel, l'École Nationale Supérieure des Télécommunications (Telecom ParisTech)

- Erkuden Rios, TECNALIA

- Amardeo Sarma, NEC

- Nikola Schmidt, Technological Platform - Energy Security of the Czech Republic

- Ulrich Seldeslachts, Leaders in Security (LSEC)

- Hervé Seudié, Bosch

- Carmela Troncoso, GRADIANT

- Janne Uusilehto, Nokia

AoI3 – Contributors:

- Piero Corte, Engineering Ingegneria Informatica spa
- Steffen Wendzel, Fraunhofer FKIE
- Paul Kearney, British Telecom
- Evangelos Markatos, ICS Forth
- Seudie Herve, Bosch
- Hervé Debar, Télécom SudParis
- Nigel Jefferies, Huawei
- Ruth Breu, UIBK, Austria
- Charles Brookson, ETSI/Zeata
- Erkuden Rios Velasco, TECNALIA
- Vashek (Vaclav) Matyas, Masaryk University
- Mari Kert, European Organisation for Security (EOS)
- Paolo Venturoni, Finmeccanica
- Leonardo Fiocchetti, Selex
- Mika Lauhde, SSH
- Maritta Heisel, University of Duisburg-Essen
- Philippe Bonnet, IT University Copenhagen
- Kristian Beckers, University of Duisburg-Essen
- Matteo Melideo, Engineering Ingegneria Informatica spa
- Natalia Pianesi, Engineering Ingegneria Informatica spa
- Elmar Gerhards-Padilla, Fraunhofer FKIE
- Klaus Kursawe, ENCS
- Enza Giangreco, Engineering Ingegneria Informatica spa
- Davide Storelli, Engineering Ingegneria Informatica spa
- Marco Alessi, Engineering Ingegneria Informatica spa
- Carmen Occhipinti, Engineering Ingegneria Informatica spa
- Gabriele Giunta, Engineering Ingegneria Informatica spa

- Riccardo Zanetti, Engineering Ingegneria Informatica spa

- Florent Kirchner, CEA (France)

- Giovani Dimeo, Selex

- Nineta Polemi, University of Pireaus

- Paolo Roccetti, CYSPA project

- Thomas Schabetsberger, ITH icoserve technology for healthcare GmbH

- Stefano Nanni, UnipolSai Assicurazioni

X-Analysis and Final Section – Contributors:

- Pascal Bisson, Thales,

- Sabrina de Capitani di Vimercate, University of Milan,

- Herve Debar, Telecom SUD PARIS

- Zeta Dooly, TSSG

- Carmen Fernandez, University of Malaga

- Maritta Heisel, University of Duisburg-Essen

- Paul Kearney, BT

- Javier Lopez, University of Malaga

- Volkmar Lotz, SAP

- Evangelos Markatos, FORTH

- Fabio Martinelli, CNR

- Svetla Nikova, KU Leuven

- Aljosa Pasic, ATOS

- Ali Rezaki, TUBITAK

- Raul Riesco Granadino, INCIBE,

- Pierangela Samarati, University of Milan

- Neeraj Suri, TU Dortmund

- Carmenal Troncoso, Gradiant

- Claire Vishek, INTEL

The following EU project communities also contributed:

- CAPITAL
- ECRYPT II
- FIRE
- IPACSO
- NESSOS
- PRIPARE
- SECCORD
- SYSSEC
- (TBC)

11 Appendix

11.1   Glossary for AoI1

- **Contactless**

  Contactless technology is pertaining to the achievement of signal exchange with, and supply of power to, the card without the use of galvanic elements (i.e. the absence of an ohmic path from the external interfacing equipment to the integrated circuit(s) contained within the card (see ISO/IEC 14443-1:2008)

- **Mobile Application**

  A mobile application is a computer program designed to operate in a mobile terminal, see ISO/IEC 29179:2012(en),

- **Near field communication (NFC)**

  NFC is a short-range high frequency wireless communication technology that enables the exchange of data between devices over about a 10 cm distance.

  NFC is to enhance the existing proximity card standard (RFID) that combines the interface of a smartcard and a reader into a single device. It allows users to seamlessly share content between digital devices, pay bills wirelessly or even use their cellphone as an electronic traveling ticket on existing contactless infrastructure already in use for public transportation.

  The significant advantage of NFC over Bluetooth is the shorter set-up time. Instead of performing manual configurations to identify Bluetooth devices, the connection between two NFC devices is established at once (under a 1/10 second).

  Due to its shorter range, NFC provides a higher degree of security than Bluetooth and makes NFC suitable for crowded areas where correlating a signal with its transmitting physical device (and by extension, its user) might otherwise prove impossible.

  NFC can also work when one of the devices is not powered by a battery (e.g. on a phone that may be turned off, a contactless smart credit card, etc.) (Source Wiki).

- **Radio Frequency Identification (RFID)**

  RFID is a wireless non-contact system that uses radio-frequency electromagnetic fields to transfer data from a tag attached to an object, for the purposes of automatic identification and tracking(see ISO/TS 16791:2014(en), 3.1.29).

- **Scalability**

  Scalability is the ability of a system, network, or process to handle a growing amount of work in a capable manner or its ability to be enlarged to accommodate that growth. For example, it can refer to the capability of a system to increase its total output under an increased load when resources (typically hardware) are added (Wiki)

- **Scaling up/ Vertical Scaling of Systems**

To scale vertically (or scale up) means to add resources to a single node in a system, typically involving the addition of CPUs or memory to a single computer. Such vertical scaling of existing systems also enables them to use virtualization technology more effectively, as it provides more resources for the hosted set of operating system and application modules to share. Taking advantage of such resources can also be called "scaling up". (Source Wiki)

- **Security level**

A security level is a measure of the level of protection against unauthorized entry, see ISO 6707-1:2014.

Thereby Authorization is a mechanism to ensure that the entity or person accessing information, functions or services has the authority to do so, see ISO/IEC 14762:2009.

- **Storage System (remote)**

A remote-storage system is a system in which the storage device is separate from the collector and is located at some distance from it, see ISO 9488:1999.

- **Trusted Execution environment (TEE)**

A Trusted Execution Environment (TEE) is a standard technology according to GlobalPlatform (www.globalplatform.org), which brings a new execution context for applications on a mobile device processor. This new context runs beside the classical operating system, so called Rich Execution Environment (REE) such as Android and may share the same hardware resources.

The two execution environments are strictly isolated. A TEE platform can execute trusted services, which may employ an exclusive access to the peripherals and resources available, including memory, computational units and controllers for the display or touch screen.

The TEE therefore ensures the protection against software attacks compromising the operating system (RichOS, e.g. iOS, Android). No matter what happens inside the RichOS, all secrets and trusted services that are managed by the TEE are kept safe from software intrusions. Many actors may benefit from this, ranging from end-users, to manufacturers and including mobile operators.

To provide such isolation, the TEE platform requires a specific hard-ware mechanism capable of managing the frontier between both execution contexts.

The concept of the TEE benefits from its deep integration within mobile processor as it can use the powerful resources typically embedded in modern systems. In addition to high performance, it can take advantage of the multiple controllers to bring trust closer to the end user, see Eurosmart White Paper Security and Privacy in the Digital World Solutions from the Smart Security Industry.

- **User-friendly**

User friendly means pertaining to ease and convenience of use by humans, see ISO/IEC 2382-1:1993, Information technology.

User friendly means pertaining to a computer system, device, program, or document designed with ease of use as a primary objective, see ISO/IEC/IEEE 24765:2010.

11.2 Additional material from AoI2

11.2.1 Results of the 29th April, 2014 WG3 workshop and follow up activities.

AoI2 held a working session during the WG 3 workshop in April 2014 and decided to take the approach as depicted in Figure 2.

Figure 2. Approach taken by AoI2 in gathering data

One way to consider the future barriers (and gaps) to secure and trustworthy institutions is to project forward the technology enablers of the digital future to 2025 and consider the risks, threats and vulnerabilities and determine the barriers that are introduced at the same time that prevent the institutions of society being secure or trusted.

At the session for AoI2 held on April 29th, the agreed approach was to focus on the threats and risks landscape by identifying the new ICT technologies and attempting to forecast the 2025 threat landscape and the risks for sectors and users, linking to economic or societal potential damage and then we would be in a better position to find new ways to address these threats/risks in terms of technologies, policies, approaches, systemic, value chain, etc. etc.

In the on-line survey at http://questionpro.com/t/AKUe8ZRGN9, we suggested a range of examples that were brainstormed at the previous session for categories such as: New ICT Technologies (e.g. IoT, Big data analytics, ...), New application of ICT (e.g. Digital currency, Collaborative working, ….) and for each of these and/or new ones the respondent could suggest, the survey walks the respondent through providing the following questions:

- What are the new threats for 2025 arising from new technology adoption for each of the topics (in terms of Systems, Infrastructures, and Institutions)?

- What are the risks and impacts of those threats (in terms of sectors, stakeholders, incl. users, and linkages to economic or societal potential damage)?

- What are the potential barriers and hence solutions to address them all?

On this basis, AoI2 carried out a survey following the methodology as shown in figure 3.

AoI2 Methodology (as agreed at 29 April '14 AoI2 session)
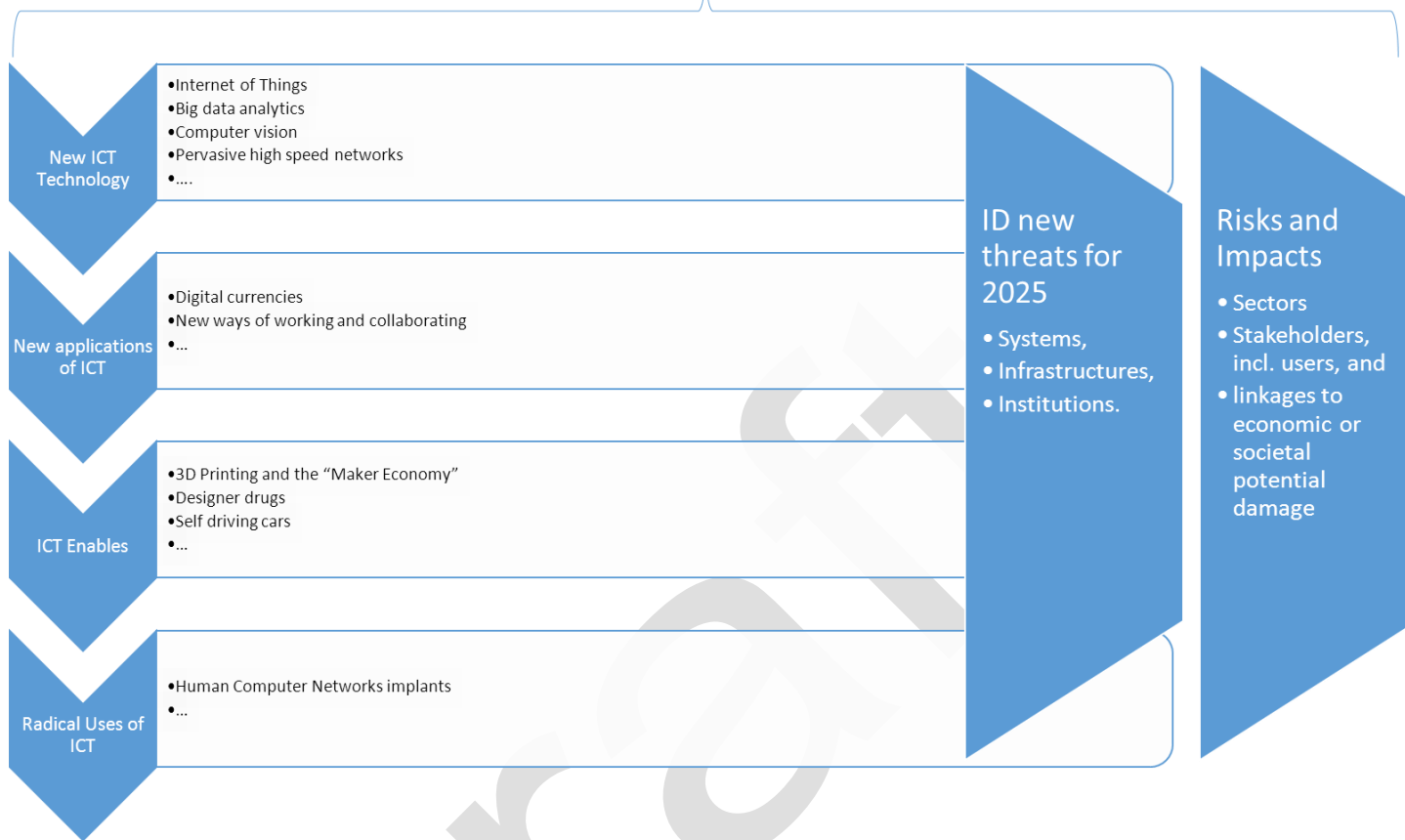
1. Gather this data via survey at http://questionpro.com/t/AKUe8ZRGN9

New ICT Technology
- Internet of Things
- Big data analytics
- Computer vision
- Pervasive high speed networks
- ....

New applications of ICT
- Digital currencies
- New ways of working and collaborating
- ...

ICT Enables
- 3D Printing and the "Maker Economy"
- Designer drugs
- Self driving cars
- ...

Radical Uses of ICT
- Human Computer Networks implants
- ...

ID new threats for 2025
- Systems,
- Infrastructures,
- Institutions.

Risks and Impacts
- Sectors
- Stakeholders, incl. users, and
- linkages to economic or societal potential damage

Figure 3. Methodology of the survey carried out by AoI 2.

Table 1 shows an analysis of the results of the survey.

Table 1. Results of the AoI2 survey carried out at http://questionpro.com/t/AKUe8ZRGN9

ICT Technologies 2025	Enables <Gov | Biz | Civil Soc> to [goal]	Risks	Threats & Vulnerabilities	Provided <trust / privacy/security barriers> are addressed
Big data analytics	Provides valuable marketing information; Lessons learned from past consumers selections; Reduce wastage (from analysing past purchasing data)	private data disclosure (loss of privacy), mass-surveillance (big-brother), data disclosure; Information/Data loss;	privacy threats, mass-surveillance, secure storage and analysis of data, poverty	Transparency about who has your data and what it is being used for; Ensuring citizens privacy rights can be guaranteed.

Internet 2.0 / Internet of Things / RFID technology everywhere	New applications to improve quality of life; New ways of working e.g. collecting of information in agriculture settings via 'Things'; Sensor technologies and new businesses; impact of ICT on vital manners of everyday life;	confidentiality threats; data and private data disclosure; unauthorized access; breakdown of critical infrastructures; complete surveillance of citizens	privacy and security of communication of data between things and servers; unauthorized access; impact of ICT on vital manners of everyday life; Espionage/ secret services collecting all possible data; attackers attacking critical infrastructures; complete dependence on new technologies; Organized Crime tapping into and using data for nefarious purposes; Information misuse; Information error generation maliciously or non-maliciously.	Secure end to end communications; No data leakage; Strong but low power cryptography; Minimum disclosure of data and information; Transparency about who has your data and what it is being used for; Ensuring citizens privacy rights can be guaranteed
Portability of every device	Ease of use when changing devices; Quicker application developments and channel to markets;	physical threats; data and personal data leakage; Information Loss; Privacy Loss	physical threats; data leakage; data confidentiality; Espionage; Organized Crime; Information misuse	Strong identification of device owners e.g. through biometrics;
Immune computing?? *Not sure what they meant by this and no specific data provided for it.*	No data provided in survey	No data provided in survey	No data provided in survey	No data provided in survey
Digital currencies	Paperless currency; Less costs associated with printing; Less wastage of old bills and coins;	Theft; abuse; anonymity risk;	Theft of money; abuse of transfers or someone else's money; no anonymity assured;	Prevention of money laundering; Minimum level of information known; New forms of fraud monitoring and forensics.

	Secure monitoring of currency provenance (source of);		Money laundering; Other criminal activities still to be discovered with digital currencies;	
Body-sensors	New applications to improve quality of life including health; Preventive health monitoring and life-saving measures;	Privacy risks; real-life physical risks; data leakage	Personal data disclosure or leakage; tampering sensors to report wrong data; data disclosure; Blackmail with sensor data.	Transparency about who has your data and what it is being used for; Ensuring citizens privacy rights can be guaranteed; Strong but low power crypto.
ICT Applications 2025	**Enables <Gov | Biz | Civil Soc> to [goal]**	**Risks**	**Threats & Vulnerabilities**	**Provided <trust / privacy/security barriers> are addressed**
ICT supported medicine	New applications to improve quality of life including health; Preventive health monitoring and life-saving measures;	health risks; data leakage; privacy risks	improper operations of medicine equipment; personal data disclosure; data injection or tampering	Transparency about who has your data and what it is being used for; Ensuring citizens privacy rights can be guaranteed; Strong but low power crypto.
People will be connected to the Internet all the times and everywhere. This will deeply influence not only professional, but also private life.	New applications to improve quality of life; Improve security and location awareness, if desired; New and different ways of working (no more 9 to 5)	loss of privacy; breakdown of critical infrastructures; complete surveillance of citizens	Secret services collecting all possible data; attackers attacking critical infrastructures; complete dependence on new technologies.	Transparency about who has your data and what it is being used for; Ensuring citizens privacy rights can be guaranteed;
Citizen Empowerment: Electronic Vote	New forms of carrying out citizens duties without being a burden;	Duplication, forgery and Fake	Identity Theft; Third party (or Gov. offices) independ-ence	Strong identification needed e.g. biometrics; Secure data channels to protect your data and it cannot get tampered with. Strong fraud prevention.

ICT Enablers 2025	Enables <Gov | Biz | Civil Soc> to [goal]	Risks	Threats & Vulnerabilities	Provided <trust / privacy/security barriers> are addressed
3D Printing and the "Maker Economy"	New business models based on the Maker economy; Prosumerism on a grand scale;	Everybody can print their own weapons;	The bad guys printing bad things	Detection of bad things and who is making them.
Self-driving cars	Improved quality of life; More effective use of time during car travelling; Improved traffic routing systems;	Privacy risks; traffic risks; burglary risks	data leakage and disclosure; car tampering; car hacking; car location tracking.	Transparency about who has your data and what it is being used for; Ensuring citizens privacy rights (including their location) can be guaranteed if they wish so;
Critical (&Information) Infrastructure Protection	Secure and dependable ICT being used for Critical Infrastructure Protection Systems	Not dependable ie. lack of Availability; lack of Continuity; lack Resilience	Sabotage; Cyber -war; Little standardization and audit	Security and Dependability of CIP.
Pervasive monitoring of cities and public areas	Provide strong security to citizens; Gathering of evidence for prosecutions; Prevention of criminality	Loss of privacy; Big brother watching at all times; Location monitoring;		Controlling data use - who can use what for what purpose; Ensuring citizens privacy rights can be guaranteed; Correct balancing between security and privacy;
Track everything all the time	Manage the environment; Providing security; Gathering of evidence for prosecutions; Prevention of criminality			Controlling data use - who can use what for what purpose Ensuring citizens privacy rights can be guaranteed; Correct balancing between security and privacy;

ICT Radical Uses 2025	Enables <Gov | Biz | Civil Soc> to [goal]	Risks	Threats & Vulnerabilities	Provided <trust / privacy/security barriers> are addressed
Human implants	New applications to improve quality of life including health; Preventive health monitoring and life-saving measures;	health risks; physical risks; privacy risks; Trespassing ethical thresholds; long time to see side effects; Society radicalization;	influence on physical condition(s); personal data disclosure; improper medical treatment; Radicalism; Unknown side effects; potential for blackmail;	If implants are collecting data, Transparency about who has your data and what it is being used for; Ensuring citizens privacy rights can be guaranteed; Strong but low power crypto;

Draft