SEVENTH FRAMEWORK PROGRAMME

Information & Communication Technologies
Trustworthy ICT

NETWORK OF EXCELLENCE

A European Network of Excellence in Managing Threats and Vulnerabilities in the Future Internet: *Europe for the World*

D4.5: Social, Legal and Regulatory Aspects of Network and Information Security in the Future Internet, Release 2[†]

Abstract: In this deliverable, we report on the social, legal and regulatory aspects of NIS by identifying challenges and providing actionable recommendations for research and policy to mitigate these challenges. By analyzing the societal landscape through key concepts, major actors and emerging technology view points, we tried to identify gaps which led to our recommendations. We also provide an account of SysSec contributions to the EU NIS Platform, Working Group 3 on secure ICT research and innovation.

Contractual Date of Delivery	November 2014
Actual Date of Delivery	January 2015
Deliverable Security Class	Public
Editor	TUBITAK - BILGEM
Contributors	All *SysSec* partners
Quality Assurance	Magnus Almgren, Davide Balzarotti

†

[†] The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement № 257007.

The *SysSec* consortium consists of:

FORTH-ICS	Coordinator	Greece
Politecnico Di Milano	Principal Contractor	Italy
Vrije Universiteit Amsterdam	Principal Contractor	The Netherlands
Institut Eurécom	Principal Contractor	France
IICT-BAS	Principal Contractor	Bulgaria
Technical University of Vienna	Principal Contractor	Austria
Chalmers University	Principal Contractor	Sweden
TUBITAK-BILGEM	Principal Contractor	Turkey

Document Revisions & Quality Assurance

Internal Reviewers

1. Magnus Almgren (Chalmers University)
2. Davide Balzarotti (Institut Eurécom)

Revisions

Version	Date	By	Overview
1.0	26.01.2015	Editor	Deliverable ready for public release after final review by Editor.
0.4	25.01.2015	SysSec Internal Reviewers	SysSec Internal reviewer comments on contents, structure and language addressed.
0.3	19.01.2015	Editor	Draft made available for SysSec Quality Assurance Review after typos corrected and references updated.
0.2	12.01.2015	TUBITAK – BILGEM reviewers	Recommendations restructured, conclusions updated.
0.1	05/01/2015	Editor	First draft.

Table of Contents

Acknowledgements

Our work on SysSec deliverable D4.5, Social, Legal and Regulatory Aspects of Network and Information Security in the Future Internet, Release 2, has been supported by our discussions and exchanges with the participants of the EU Network and Information Security (NIS) Platform Working Group 3 (WG3) on Secure ICT Research and Innovation.

We would like to acknowledge the general contribution of the EU NIS Platform WG3 organization and its participants to our work and thank them for bringing to our attention new aspects of network and information security from the perspectives of individuals, businesses, governments and civil society actors.

OECD Working Party on Security and Privacy in the Digital Economy (WPSPDE) has been a forum for exchange regarding the critical aspects of cyber security and privacy from societal, economic and legal perspectives.

We thank the secretariat of the OECD WPSPDE as well as the government officials from OECD member countries, business leaders, researchers and NGO representatives we had the opportunity to interact with during the meetings of this working party for demonstrating to us how emerging technologies lead to complex and interconnected consequences in the societal, economic and legal domains.

1 Introduction

1.1 Scope

The main scope of this second release [35] of deliverable D4.5 has been twofold:

1. Provide concrete and actionable recommendations and conclusions in the deliverable on research and innovation policy and strategy on the social, legal and regulatory aspects of NIS by determining where challenges exist and opportunities could be unlocked by innovative research.

2. Support the work of the EC NIS Platform WG3 [6] on the social, legal and regulatory aspects of NIS and report on these contributions.

1.2 Method

In addition to their project activities, SysSec partners [29] have been active in numerous interdisciplinary and multistakeholder platforms to gain expertise and exposure on the social, legal and regulatory aspects of NIS. They have been bringing their findings into the project and the NIS Platform WG3 activities. Through the interaction of SysSec partners with other experts in the NIS Platform, there have also been ideas and information flowing from the NIS Platform back into the project and this deliverable.

A notable activity in the efforts of the partners to capture the requirements and gaps in the social, legal and regulatory aspects of NIS has been their participation in the OECD Working Party on Security and Privacy in the Digital Economy (WPSPDE) [18] which aims to provide policy and strategy guidance to governments and organizations on Cyber Security and Privacy. This working party brings government officials, business leaders, researchers and NGO representatives together around producing concrete guidelines on the critical aspects of cyber security and privacy. Representatives from the Council of Europe, the European Commission as well as members from different national ministries contribute to this working party with their perspectives derived from social, economic and technology policy making. Deeply rooted in evidence based policy making, OECD and the WPDPDE adopted the target of “better policies for better lives” focusing on economic and social challenges. SysSec partners have been actively contributing to the WPSPDE and have been bringing their findings from WPSPDE back to this deliverable and those of the NIS Platform WG3.

The authors of this deliverable have also been informed by the work of numerous interdisciplinary academic research centers around the world regarding the societal consequences of emerging technologies at local, national and global scale [1], [2], [27], [28], [35].

Merging their expertise with the input and perspectives they have collected from these numerous sources, SysSec partners worked on analyzing this interdisciplinary space at the intersection of technology and societal concepts to capture the emerging challenges and provide recommendations to turn them into research and innovation opportunities to support European cyber security strategies.

We strived to identify research challenges by first studying important societal concepts and then, the main societal actors from the point of view of the challenges and opportunities network and information security and privacy developments bring to them. A challenge is raised when the usual functioning of these concepts and actors could potentially be disrupted by digital security and privacy concerns. Feedback from societal challenges back to the technological domain were also identified. Conflicting interests created by emerging security and privacy phenomena are tried to be determined, such as in the case of surveillance. Then we tried to determine if there are mitigating solutions in conflicting situations. If there are no such immediate solutions, this is identified as a gap and a recommendation is issued to bridge the gap by innovative research. Some of our recommendations also propose policy and strategy options to support research activities.

SysSec participation in the NIS Platform WG3 and its deliverables are detailed in Section 5 of this deliverable. Our contributions and content are not only presented in this current deliverable but are also in the deliverables of the NIS Platform WG3 themselves.

1.3 Structure

The current document starts with an executive summary of its contents and the introduction of its scope, methodology and structure. The document starts its analysis by exploring the impact of NIS on the key concepts and building blocks of society in Section 2. This sets the stage to demonstrate the effects of NIS concepts such as vulnerabilities, threats, risks as well as countermeasures on the society. Possible improvements in the current state of affairs are highlighted. This is followed by a demonstration of the relationship between societal actors and NIS challenges in Section 3. This section introduces the current and expected activities of the major stakeholders in the society to ensure

security. Section 4 gives an account of the NIS impact of new platform specific technologies on society. Throughout these sections references to EU NIS Platform WG3 deliverables build the link between the important concepts introduced and the position of the NIS Platform WG3 on them. A detailed account of the SysSec partner contributions to the EU NIS Platform WG3 activities are then highlighted in Section 5. Throughout the document, under each subsection, concrete and actionable recommendations for research policy and strategy are stated with dedicated sub sections and recommendation numbers. These recommendations are consolidated together in Section 6 once more, followed by the statement of the main conclusions in Section 7.

2 Impact of NIS on Key Societal Concepts

2.1 Trust and Risk

According to the OECD, trust has a vital role in social and economic interactions and institutions. Trust is established by reducing uncertainties which lead to risks. “Trust reflects people's perception of others' reliability” [19]. Economic and social development is affected by trust as it facilitates market exchange, enables better functioning public institutions and increases capacities for collective action [16]. Trusting societies prosper. OECD presents data to support the following statements that:

> “High country trust was strongly associated with high household income levels” and ;
>
> “Higher levels of trust were strongly associated with lower levels of income inequality” [19].

OECD sees security and privacy as the key elements of trust in the digital economy. The relationship between security and trust is complex. While security threats could certainly erode trust and hence economic activity, corresponding security measures might also limit innovation and productivity if they excessively restrict and burden the systems they try to protect. This challenge invites research into how security measures can be developed that are proportionate to the associated risks and that encourage open and innovative systems.

There is a parallel challenge in the privacy domain which is even less researched. How will personal data and privacy be protected while allowing for innovative new products and services that rely on the analysis and processing of such data which are seen as a major area for economic growth and opportunities [22], [23], [24]? In parallel there is also the challenge of surveillance where personal privacy requirements are pitched against the claimed security needs of societies. Reconciling these challenges is essential to building trust in individual and societal levels. This reconciliation is promised to be in a risk-management based approach to security and privacy.

While it is difficult to define what trust is, “loss of trust” is easier to detect. Security and privacy breaches, threats and vulnerabilities erode the trust users have towards digital systems, services and applications. Therefore, establishing a sense of security and privacy is paramount. However, it is now generally accepted that, absolute security or privacy is

not possible in the digital world. Yet, people still require answers when they ask “Is my data, computer and network secure? Is my privacy assured? Am I safe in the digital world?” When the answer is invariably “No!”, erosion of trust is inevitable.

Instead of trying to establish absolutely secure or private systems, services, applications or data, there is a risk based approach to security and privacy. Within the OECD, it is widely recognizes that digital security risks go hand in hand with economic and social activities in an open and interconnected environment [18]. Measures that are proportionate to the associated risks are deployed so that if and when such risks materialize, they can be survived and their adverse effects are minimized to ensure continuity. Moreover, this approach is no longer asset based but rather process and flow based [38], [39]. This is to mean that in the past, individuals and organizations were trying to protect their assets from intrusions, threats and associated risks. However, with the increased distribution of resources with systems like cloud computing and mobile platforms, distributed service oriented architectures (SOA) and the Internet of things, there is a chain of dependencies that is getting longer by the day. As these dependencies grow and assets such as networks and data are distributed, risk management methods protecting these assets no longer protect the vital processes of organizations and individuals.

Borrowing from object oriented methodologies, use cases are generated to identify the key processes and flows of organizations. Risk management processes then focus on these processes and flows so that they can “survive” potential threats, vulnerabilities and risks. Not all processes need to be protected with the same measures. Risk and readiness assessments determine what is critical and what are the options to protect them. And the new question to ask is “What are my security and privacy risks in the digital world and how do I prepare for them?” When such preparedness provides long term survival and incident management, this builds trust. However, this management approach has not yet been adopted by all of the stakeholders and organizations at large, particularly SMEs for which such management methods and tools are still not accessible. There is much to be researched and implemented to make security and privacy risk management main stream, affordable and sustainable.

Organizations have been the general focus of risk management. Public and private organizations that use risk management methodologies also manage part of the risks to their users and customers which are other organizations or individuals. However, for the building of trusting

societies, individuals need to be brought into focus as well. Yet this could be a difficult and costly proposition and difficult to implement in a sustainable manner. Governments, consumer protection organizations, NGO's and crowd-sourced initiatives could provide ways to represent groups of individuals and provide solutions for them. It would be beneficial to research how established risk management mechanisms and approaches could be adapted to risk management procedures and methodologies for individuals.

An integral part of risk management is externalizing some or all of the risk by procuring insurance. Insurance companies are indispensable parts of modern society. In the NIS domain, cyber security insurance is an emerging field but there are obstacles to the creation of a cyber security insurance market [11]. Measuring the potential risks in the NIS domain and estimating the value of compromised digital assets are challenges. Without a viable cyber security insurance market an important component of a functioning risk management eco-system remains unfulfilled.

Another building block of trust is an incident-free relationship where requirements and expectations are met for all parties over and over again. Yet, incident reporting is a common problem in both security and privacy breaches. As companies and organizations fear damage to their reputations and potential financial losses, such incidents are not always reported. Governments are trying to enact regulations and incentives to encourage incident reporting but this is not wide-spread. As this leads to a sense of doubt about the reliability of the systems and honesty of service providers, trustworthiness is eroded. However, strong laws and tight regulations also run the risk of stifling innovation and open platforms. Therefore, a compromise needs to be found. Innovative incentives to increase adoption of incident reporting, anonymizing some elements of sensitive incident data are potential research topics.

2.1.1 Recommendations

R.2.1.1: Support research into how security and privacy risk management methodologies can be made widely affordable and sustainable by creating tools and services, particularly for SMEs.

R.2.1.2: Support research into how current organizational security and privacy risk management procedures can be applied to individuals.

R.2.1.3: Support research into increasing and streamlining incident reporting that will use a balanced approach between incentives for voluntary reporting and tight regulation that will create an environment

which is neither ineffective for reporting nor stifling for innovation and competitiveness.

R.2.1.4: Support research into how a viable cyber insurance market can be created that includes effective measurement of NIS risks and accurate estimates of the value of digital assets.

2.2 Rule of Law

The principle of the rule of law ensures that society functions according to the laws and regulations enacted by the state and the society itself, that there will be no arbitrariness in the application of laws and that all individuals and organizations will be treated equally before the law. This is a principle that is upheld to the highest degree by the Council of Europe, which is the principal human rights organization in Europe [3], [4]. Laws establish the relationship of individuals and organizations with each other and their environment as well as the relationship between the state and the individuals, organizations and the environment.

Laws regulate the potentially conflicting interests of individuals, organizations, the state and the environment in a way that is determined by the legislature of the nations or supra-national institutions such as the European Union. When individual or societal relationships, assets or processes change, laws need to adapt to these changes. Technology is a major reason why such relationships and processes evolve and change. The invention of the wheel, that of the steam engine or the communication technologies have altered the relationships and the functioning of societies. Laws take time to catch up with these changes and during rapid transition periods, there are opportunities for criminals and fraudsters to abuse the laws and the societal systems. The rapid rise of information and communication technologies and the associated cyber security and privacy shortcomings have provided many so called “grey areas” where what is legal or illegal became difficult to determine. Take the case of ownership of digital assets or forensics challenges? As laws did not adequately regulate the domain of activities, irregularities and arbitrariness arose.

Another key enabler for criminal and fraudulent activities is lack of traceability and observability in virtual systems. The concept of a legal entity, or identity is fundamental in the application of laws. If the identity of individuals or organizations cannot be determined, then their activities cannot be scrutinized. However, on the other hand, there is the well established concepts of anonymity and right to privacy in society.

Constant tracing and surveillance would erode these concepts. The following section on transparency is also related to these concepts.

Laws and regulations assign rights and responsibilities among societal actors. When a newly created or changed technological or economic system or domain is not adequately regulated by laws then societal actors become reluctant to assume responsibility. The case of cloud computing is a good example in this field. The cloud computing business model has disrupted many ownership models in government institutions and companies. The ownership of data, its storage or processing location or transmission paths have been concerns for the owners of the data and service providers. These questions have not been well answered in existing laws and regulations. Therefore, users have been reluctant to adopt cloud computing due to security and privacy concerns. Many attempts by technologists to remedy this situation have been inadequate. Not only did this stifle innovation and uptake in cloud computing, but also caused losses for early adopters of this business model who were mistreated by some service providers.

Another example comes from the early days of cell phone adoption. When laws did not regulate this domain adequately, many cases were reported in the press when individuals were traced by the location information provided by the cell towers and service providers, grossly violating their right to privacy. There were other cases when emergency services could not obtain the same information to find lost or distressed individuals due to prosecution fears of service providers if they provided the information. Applicable laws were subsequently updated to require court of law orders for service providers to issue such information about individuals with potential exceptions in urgent situations. Therefore, it is essential that a multistakeholder effort and research is carried out to ensure laws and regulations are up to date with the latest technology and its usage.

Big technology companies that dominate new but widely deployed technologies often regulate these emerging domains if applicable laws are absent or have limited capabilities. Then individuals or societies might feel that these companies might be above the law and might operate with impunity. As these companies innovate, they have the right to the associated economic returns. However, their operations and actions need to support the society and abide by the essence of the laws until laws catch up with the market realities.

2.2.1 Recommendations

R.2.2.1: Encourage efforts to raise the profile of disruptive or emerging technologies among law makers and society at large, to study adequately its legal and regulatory challenges well in advance of their wide adoption in society. A use case and process based approach would help reveal the potential issues. Universities, standards bodies and patent organizations together with related government departments should be at the forefront of these efforts.

R.2.2.2: Support research in the field of digital identity management that will build a balanced approach between security and traceability requirements and personal privacy rights and obligations that will also enable anonymity in the digital world.

R.2.2.3: Support awareness raising activities on ethical issues in research, innovation and business in technology companies and universities to create a sense of responsibility to contribute to society while creating new technologies and domains of activity.

2.3 Transparency and Accountability

Transparency is a fundamental component of open and democratic societies. All activities in the public domain, such as the functioning of the government, economy, organizations and the relationship of individuals with the state are carried out in a transparent and accountable manner. All the actors in this field behave in a way that can be observed, questioned and evaluated. There are public organizations that carry out audits and hold officials and individuals to account. For these checks and balances to take place, there is a need for observability, measurement and recording of activities and events. Activities in the personal sphere, that are protected by privacy principles and human rights are outside the scope of these controls.

When ICT systems were introduced to most processes of the society, economy and the government, collecting and processing data have become much easier. However, complex, virtualized systems have also enabled hiding and obscuring internal processes and events from external observation. For example, today cloud computing and virtualization at all levels, including network virtualization, make it possible that a lot of transactions and communications can take place without ever leaving a single hardware domain hence not necessarily observable to the outside world. In non-virtualized systems made up of separate hardware components, control points were available, such as communications channels, input/output points among processes and external storage

systems. When all systems are implemented as virtual machines and processes, these control points disappear hence making observations and accountability very difficult. These developments make transparency and accountability hard to assure.

Another example is big data applications where very large data sets are collected, derived and correlated about individuals, companies and all on-line activities without their explicit consent. What is being done with this data is opaque and is not usually subject to government or individual oversight since control points are not easily defined. Commercial, competitive concerns are also to be taken into account as well as not impeding innovation and growth. Therefore, governments are cautious in imposing any constraints and requirements in such emerging areas. Yet, this leaves many opportunities for exploits and uncontrolled behavior to the potential detriment of consumers and society.

One opportunity that the society has for learning about the inner workings of obscure ICT systems and processes is when incidents lead to data breaches which are reported or leaked to the public domain. This emphasized the importance of incident reporting and event management in complex ICT systems once more to enhance transparency and accountability.

Surveillance operations of governments and security companies often make use of the obscurity in complex ICT systems as well. However, when the public suspects these activities and what they are used for, this acts as an inhibitor for the public to use these systems for their rightful purposes.

When ICT systems, their vulnerabilities and their complexity enable a subset of users to avoid transparency and accountability mechanisms of the society, this erodes trust in these systems and the digital world and has a detrimental effect for the well being of all. Lack of control points in systems and moving towards a “block-box” relationship with ICT systems need to be avoided.

2.3.1 Recommendations

R.2.3.1: Support research into making complex virtualized systems and big data applications more transparent and accountable by adding control points to these systems for observability while including privacy assurance mechanisms.

R.2.3.2: Create frameworks for the relationships among governments, companies and individuals to govern data collection and surveillance

activities to make sure all know what is collected and used for which purposes with the appropriate oversight mechanisms.

2.4 Freedom of Expression

Freedom of expression is a right democratic societies defend vigorously. Yet, everyday we witness websites or blogs blocked or corrupted, messaging or social media accounts taken over or communications channels disconnected, using ICT vulnerabilities in these systems or the ones they depend on. Regardless of their content, when such actions occur outside the requirements of the law, they prevent people or organizations from expressing themselves freely, leading to the violation of the right to free speech and freedom of expression.

Using cyber security vulnerabilities, certain individuals, groups or organizations could also be manipulated or coerced. Technologically capable adversaries can exploit security and privacy vulnerabilities to stifle free speech and access to information. It is very difficult to trace and hold to account the perpetrators of such attacks which target individuals, vulnerable groups, civil society organizations and even states.

Managing such attacks as risks is a fundamental approach. Enhancing the available technology and its accessibility by the public at large to create a level playing field is also essential. Governments would also need to extend their safeguards for free speech to these new and emerging communication channels.

2.4.1 Recommendations

R.2.4.1: Encourage public-private partnerships for research into creating more robust communication channels and applications that individuals and groups can use without being interrupted.

R.2.4.2: Support research in the forensics domain to trace and identify perpetrators of on-line attacks on freedom of expression.

2.5 Privacy

In the emerging data centric digital world, personal privacy is threatened more than it has ever been before. Every on-line activity creates a data footprint and is potentially traceable in real time or off-line. Privacy is a broad and complex subject and the individual is at the center of the debate. Preserving the privacy rights and freedoms of the individual enjoyed in the conventional, physical environment also in the digital world is fundamental. Balancing these rights and freedoms with the needs of societies for security requires trade-offs and win-win approaches.

Some of the major threats to personal privacy can be listed as follows:

- Exploitation of vulnerabilities in ICT systems for unauthorized access to personal data,
- Data breaches or insider threats in service providers,
- Big data analytics techniques leading to correlation and profiling,
- Surveillance.

Vulnerabilities in ICT systems provide criminals and fraudsters opportunities to gain access to information systems and steal or manipulate personal data for economic gains. Stealing credit card or bank account information or holding individuals to ransom to release their hijacked systems or data are some of the exploits often seen, which damages the personal sphere of individuals. Raising awareness of such threats and providing adequate protection mechanisms is essential in these cases.

Organizations, institutions and governments which hold and manipulate personal data are liable for the adequate protection of this data. However, threats often emerge from these service providers in the form of accidental data breaches or leaking of information by insiders. There is an emerging privacy risk management approach for these organizations to manage and mitigate these threats. Much like security risk management, this approach enables organizations to protect their critical processes against privacy incidents.

OECD sees big data driven innovation as a major growth enabler for the digital economy [25]. From customized services to better efficiencies and competitive intelligence there are ample opportunities to exploit data for the good of individuals and societies. However, there are major risks associated with the potential exploits of these data for unlawful use [22], [23], [24], [26]. Linking separate databases to correlate data and profile and identify individuals is a very sensitive area. While such applications might be helpful, for example, to provide better healthcare services, they may lead to discrimination and loss of entitlements in other settings. Therefore, appropriate safeguards are needed around big data innovations.

Surveillance by state or private organizations have always had privacy implications. However, with the latest revelations of state agency activities and spying and surveillance claims in cyber space, there is an

unprecedented reaction from the public and civil society organizations to protect personal data and privacy. This is the area where the security requirements of nations as represented by state organizations and personal privacy needs of individuals and groups confront and seemingly contradict each other. However, this need not be so. Establishing appropriate oversight is the key to reconciling security and privacy needs. Security without intrusiveness and privacy without absolute immunity are needed and appropriate levels of public oversight on well known mechanisms in each area would ensure personal and public trust in these systems. However, how this would be achieved is a research area in both technology and policy domains.

2.5.1 Recommendations

R.2.5.1: Support extensive awareness raising programs for personal privacy and safety in the digital world so that unsuspecting individuals and groups do not fall victim to privacy attacks. While the technology to achieve this might be available, its adoption by children, the elderly and other vulnerable groups in society is not assured.

R.2.5.2: Support research and innovation programs into the creation of privacy risk management methods and tools for institutions and companies (especially SME's) to protect their users' data (Covered by recommendation R.2.1.1 as well).

R.2.5.3: Encourage research to add privacy by design modules and features into big data analytics tools and techniques.

R.2.5.4: Support multidisciplinary research into devising appropriate privacy protection oversight mechanisms on surveillance activities of security organizations and operations to ensure public trust.

R.2.5.5: Support research into evaluating the trade-offs between anonymity and traceability for personal privacy versus public accountability.

2.6 Ownership and Control

Asset ownership and exerting control over these assets is a mechanism civilizations have built over time to share the resources around them and to own what they produce through their means of production in economy. By controlling these assets, economic relationships are built and assets are protected for their rightful owners. Debates on how assets and means of production are distributed and controlled in society led to different political systems over time.

In the digital world, classical approaches to the definition of assets, ownership and control are changing dramatically. With the digitization of everything, digital assets are created. These data items are protected with innovative digital rights management (DRM) tools. However, vulnerabilities in the DRM tools lead to exploits and loss of control over digital assets which may be made freely available on the Internet. This leads to the lively debates on intellectual property rights (IPR) in the digital domain.

Another part of this debate is the open source movement which considers many of the assets created in the digital world as common/public goods for the free and open consumption of all. The open source movement also harbors a collective and collaborative means of production approach with licensing schemes like Creative Commons which leads to a more equal distribution and sharing of assets.

With new business models like cloud computing, the virtualization of ICT assets has been accelerating. This time complete ICT systems are virtualized, including networks, processors, memory, storage, data and applications. This has led to more erosion of control as assets have been handed over to service providers to operate. Loss of control has been a real challenge for many IT systems administrators and businesses. New threats that emerged in these virtualized systems are even more difficult to handle due to their lack of traceability and observability.

Due to vulnerabilities in ICT systems exploited by criminals and fraudsters, it is becoming more and more difficult to protect digital economic assets and this is creating a challenge for their owners as well as for insurance companies and governments.

2.6.1 Recommendations

R.2.6.1: Support multidisciplinary research into how the concepts of ownership and assets in the conventional world extend into the digital world and if there is a case to modify them for the public good.

R.2.6.2: Support research into creating innovative insurance models for the digital world.

2.7 Economic growth and an equitable society

Economic growth and sharing of the wealth and opportunities created by this growth fairly help create a more prosperous, peaceful and equitable society. Exploitation of cyber security vulnerabilities for economic advantage by criminals and fraudsters is creating a black market and a parallel economy, leading to unlawful gains by a few in the

expense of the general public. It is hurting inclusiveness and fairness in society.

Another key element of an equitable society is diversity and non-discrimination. Societies spent a lot of time and effort to build tolerance and multiculturalism into their societal fabrics. Individuals and groups from different backgrounds add to the richness and resilience of societies. While these principles are firmly established and non-questionable in most societies, they are debatable in others. On-line tools and environments might be used for discrimination and intolerance towards differing individuals and groups due to the relative anonymity the Internet environment provides to these perpetrators. On social media, bullying and threats are well known but are hard to trace and bring to justice. Targeted attacks motivated by discrimination and intolerance have also been reported. Such attacks lead to insecurity for many groups and diminishes the potential usefulness of the on-line environment. Therefore, they are detrimental for a well functioning, equitable society.

2.7.1 Recommendations

R.2.7.1: Support awareness programs to alert the public on the scale and mechanisms of the underground economy created by on-line fraud and criminal activities and on how to minimize them.

R.2.7.2: Support research on reducing on-line discrimination, intolerance and bullying by both technical and non-technical methods.

2.8 Innovation

Innovation is a major enabler of development and growth. Innovation depends on an open environment that supports free flow of information, assets and people so that innovators can achieve their potential. Collaboration is also a building bloc of incremental innovation. Due to its open and interconnected nature, Internet and ICTs in general supported innovation since their inception. However, security measures to counter the effects of cyber threats and to some extend those being brought in for privacy protection could potentially limit the openness of these systems and limit their contributions to innovation. Therefore, there are often questions about security and privacy measures stifling or burdening innovation.

Some states are even building walled-off and tightly controlled Internet sub domains for their countries out of concerns for security. This impedes the innovators' ability to reach out to the world. Innovations from other parts of the world cannot reach the consumers in these

countries easily either. Therefore, growth associated with innovation is hurt by such moves.

2.8.1 Recommendations

R.2.8.1: Support research into Internet governance models that promote both openness and necessary controls to ensure security and stability of the systems.

2.9 Globalization and Europe

Like in many areas of ICT technologies, a large number of the tools and technologies used in NIS are created and sourced from outside Europe. This creates many dependencies for the users to sources outside of their realm of influence, at individual, organizational or national level. This could be seen as an extension of the “globalization” phenomenon. However, the concentration of tools and technologies in a few number of hands seems to be more acute in the field of NIS. National governments sometimes find it difficult to include such foreign NIS tools and products in their environments and look for national solutions but these are often in short supply. Open source tools and technologies provide some improvements in this area. However, questions about service and sustainability provide challenges that are often difficult to resolve.

In many countries, the absence of qualified and educated NIS personnel and NIS industries and marketplaces also exacerbates this situation. Therefore, availability of such personnel and companies are to be encouraged.

Dependencies create a problem for transparency as well. Once the chain of suppliers gets longer and longer, traceability, observability and hence transparency become more difficult. Especially when some of the key players fall outside national jurisdictions, enforcement may become impossible.

These concepts all erode trust in the digital environment and limit its potential.

2.9.1 Recommendations

R.2.9.1: Encourage and stimulate the creation of NIS SME's and flagship companies in Europe by creating economic incentives and guarantees for start-ups and by encouraging competitiveness in this field.

R.2.9.2: Support the proliferation of open source NIS technologies and the development of their service and support eco-systems at local and national levels by creating “blue-print” frameworks and toolsets that are

tried and tested at government institutions and implemented by SME's that are also accredited by governments.

R.2.9.3: Invest more in NIS education and training to guarantee the availability of NIS personnel and creation of “home-grown” NIS companies by the creation and accreditation of dedicated programs at vocational and university levels.

R.2.9.4: Use public procurement as a tool to counter the effects of globalization on NIS related tools and technologies.

R.2.9.5: Support research programs into determining requirements in skills, key technologies and business models that would support a free standing European NIS market.

2.10 Standardization

Standards play a proven role in interoperability. When there are well established and accepted standards for a technology or a methodology, its proliferation is greatly facilitated. In the NIS domain, there are various standardization efforts but there is also a need for a coordinated standardization strategy among different standards bodies that would help build trust in the digital environment. These standards bodies include ITU, ISO, ETSI, IETF and many national and regional standards organizations.

The subject of NIS is a fast moving one with new domains emerging very frequently, therefore, standardization is a difficult subject. However, frameworks are emerging to tackle such difficult questions. These frameworks are often favoring one product set or the other and their adoption becomes a competitive economic issue. To avoid such limitations, global frameworks could be researched. Another limitation of frameworks is their high level approach and abstraction of technology. When a framework is kept at a too high level, its usefulness may diminish since it fails to address key technical issues and users may not know how to implement and benefit from the framework. If the framework goes into too much detail, then it may be quickly outdated by fast moving technology. Research is needed to address this challenge to create enduring and relevant NIS frameworks and standards.

Standards also provide opportunities for transparency. When products and solutions use standards with well-known control points, parameters and components, then tools and techniques to collect information from such systems can be developed. These in turn render the observability of these systems possible, hence improving

transparency. Yet, not all standards are written with such requirements in mind.

To achieve its stated benefits, standardization procedures and environments need to be open, transparent and inclusive. This guarantees that all requirements and interests are represented. Especially if standards are to cover more than just technology, diverse groups and stakeholders, such as social, legal and regulatory experts, need to be present. This is not to mean that purely technical standards would need to deal with such concepts. Instead, standardization bodies need to include such representatives to perform key gate reviews of standards and provide feedback and recommendations. As well, the above mentioned frameworks including such concepts could be carried to standards levels. In this effort, a more interdisciplinary approach would be beneficial.

Due to its diverse nature, the social aspects of NIS are hard to standardize but as mentioned above, analyses of the impact of standards in the NIS domain on society would help with their success and adoption as well as improving the societal conditions. In the legal and regulatory aspects standards could be more applicable and would help with the harmonization of national laws and regulations to help build a seamless global NIS environment that favors international collaboration.

2.10.1 Recommendations

R.2.10.1: Encourage social, legal and regulatory impact analysis gate reviews for NIS standardization activities.

R.2.10.2: Support research on how to create standardized frameworks that are both general enough to be relevant over a long period and relevant enough to cover key technical challenges.

R.2.10.3: Support research on the creation of standardization strategies for NIS technologies and frameworks by creating task forces or support actions in existing and new NIS programs. This research would need to take into account the trade-off between competitive commercialization considerations and standards for wider adoption and interoperability. An element of these strategies should be on cooperation among standardization organizations.

3 Societal Actors and NIS

Society is an eco-system within which feedback among its different actors helps establish an equilibrium. A holistic systems approach to society will be helpful for successful NIS policy making. Below we analyze the role of various societal actors and their NIS challenges.

3.1 Individuals

Individuals are the main players of all societal processes. They are also the key players in the NIS domain. Their actions create the risks in this domain and they are primarily affected by these risks. Every consideration in the NIS realm has a component related to individuals.

Individuals or consumers approach cyber security issues with varying levels of risk awareness and acceptance. While some users will ignore NIS issues altogether, others limit their usage of ICTs and auto-censure their contributions to the Internet out of fear of surveillance or data breaches or potential for attacks and losses. For example, some users will not use Internet banking from their home devices while others do not refrain from using terminals in public Internet cafés for accessing their bank accounts. Therefore, it is not easy to create a general model for the attitude of individuals towards NIS concepts. Yet the following are common themes:

Risk Awareness: While ICT usage is increasing rapidly, especially with the proliferation of mobile devices, the novelty factor of new applications and services is masking many risks for the users. For example, when a new mobile application automatically accesses location information from the mobile device without the user's permission or accesses the microphone of the device for voice commands automatically, not many users object but there are NIS and privacy risks associated with such decisions. By constantly collecting location information from a capable mobile device about its user, it is possible to trace and monitor an individual. Users need to be made aware of these risks and encouraged to make informed choices. One approach might be “security and privacy labeling” of applications and services.

Security and privacy labeling can be thought of in a similar fashion as food labeling. It should inform the user of the contents of the product and the implications of consuming it in a very concise manner. The current long and detailed security and privacy policy information and terms of service texts that are provided to users for acceptance are not

serving this purpose. Most users accept these without reading them. Website security certification and accreditation labels are helping in a limited way but their focus is not generally transparency. Just like food labels, the proposed security and privacy labels could list in a tabular format the contents of the package and what it does and some key information about security and privacy risks. The key information that would make sense to display and its potential impact could be the subject of research. Just like controversies on what to include on food labels, these are also sensitive matters and there could be a need for both regulatory and voluntary approaches.

Loss of trust: As stated in the prior chapter on trust, many users are loosing trust in the digital environment and are giving up on the open Internet model due to surveillance risks to their privacy or security threats and risks to their digital assets or even to their personal safety.

User centricity and empowerment: Many of the problems related to new technologies occur because their developers do not consider how they will be used and how they will affect their users. If the individual user is placed in the center of the development process, then developed technologies would be user friendly and would empower users rather than pushing them aside. In this sense ICT's and NIS tools and technologies have a mixed score card. Usually, concerns for the security and privacy of individuals comes as an afterthought in most technology developments. When vulnerabilities are detected they are handled by add-ons which are often ineffective. To be effective, NIS and privacy requirements for individuals need to be brought into design cycles early on and in an interdisciplinary fashion. Individuals also need to be in control of their behavior and their data in the digital world.

Identity management: Identity management in the digital world is not just a reflection of its meaning in the conventional, physical world. Data derived by digital systems about their users create profiles and information about them when they are linked and correlated which are beyond what individuals would like to reveal about themselves. The meanings of public sphere and personal/private sphere are changing rapidly, not necessarily within the control of individuals. Identity theft has also been an ongoing threat to individuals.

Surveillance: A recurring theme in the relationship of individuals and ICTs is the surveillance by state and other organizations. This damages the trust of individuals and leads to self-imposed restrictions. This theme will be analyzed further in the following sections.

3.1.1 Recommendations

R.3.1.1: Support research into user centric security and privacy tools and technology design and implementation.

R.3.1.2: Bring to the forefront the empowerment of individuals, especially in relation to the management of their data and identity in the digital world.

R.3.1.3: Support research into the feasibility and effectiveness of security and privacy labels on applications and services.

3.2 Businesses

Businesses hold the means of production that individuals may not possess. They organize their assets and employees to reach their goals of producing and earning. They are the providers, the supply side in the economy. Accordingly, they provide most of the tools and techniques used in the NIS domain. However, they also help create the risks in the digital domain by their products, services or processes. In the past, implementing security was merely seen as a cost for companies but now, modern companies see security as an enabler for doing better business. Important NIS concepts for businesses can be listed as follows:

Risk management: Large companies and organizations have been early adopters of security risk management processes largely due to the availability of standards and certification and audit mechanisms [38], [39]. Putting in place continuous processes of risk assessment and mitigation helps companies to protect their critical and vital processes and ensure business continuity under cyber attacks. Risk management processes protect not only the companies themselves but also their customers and suppliers as there are heavy dependencies among them. OECD promotes a risk based approach for all actors in the digital economy. The challenge now is to enable the wide adoption of risk management procedures among SME's and to extend these processes for privacy risk management.

Data collection: Businesses in the digital economy collect and produce very large amounts of data about their own operations and about their customers and users. Some of this data is personal and can directly identify individuals. While there are general data collection principles and terms of use published for most businesses, these are not negotiable and users generally surrender their rights to companies. While there are now improvements in this area due to the advocacy efforts of civil society groups and governments, there are still obstacles to privacy preserving policies to be implemented. On the other hand, data is part of the assets

of a company by which they can create innovative products and services. Its these innovations that would create competitive products, enlarged markets and economic growth. Therefore, any policies to be enacted to regulate data collection needs to strike a balance between privacy needs and competitive innovation.

Security and privacy by design: When security and privacy features come as afterthoughts in products and services, they can only be partially effective and their implementations become very costly, also reducing the performance and usability of these products and services. While companies use risk management approaches for their operational needs to protect themselves and their stakeholders, they do not necessarily apply these techniques to their products and services. The security and privacy implications of business products and services need to be thought as part of product design and measures need to be implemented as fundamental features. Security and privacy by design techniques need to be given prominence in businesses as much as time-to-market and profitability concerns.

Transparency versus competition: As companies become more transparent with respect to their security and privacy risk management processes, their customers can also manage their own risks in a better informed manner. Transparency could build trust in the products and services of a company. However, there is a debate if incident reporting in a transparent way builds trust in the operations of a company or damages its reputation to the advantage of its competitors. The answers could lie in short and long term points of view. While reporting incidents and breaches can have negative impact on a business in the short term, they can help build trust in the long term if these incidents are handled effectively by the employment of adequate risk management and mitigation actions. It is not often easy to build such a perspective in the fast changing short term focused technology markets.

Critical infrastructures: Many critical infrastructures in societies are run by private businesses today. Many examples in energy, water and sanitation, transportation, telecommunications and healthcare sectors exist after the wave of privatizations of the last decades. As these critical services and infrastructures start to operate outside the government sphere, they are subject to competitive and profit-making concerns and they also acquire a level of freedom from government oversight. The regulatory agencies created for such sectors after they are privatized try to provide assurances, best practices and standards in these domains. Ensuring NIS and consumer privacy and protection are part of their

activities. However, as in all regulatory processes, their effectiveness depends on their ability to create a level playing field for competition and growth that also provides adequate protection. This is not easily achieved as policies may not always take into account technology and market realities and may not be implementable.

3.2.1 Recommendations

R.3.2.1: Support research into creating cost effective and simple to use security and privacy risk management processes and tools for SME's to use in a sustainable way (Covered by recommendation R.2.1.1 as well).

R.3.2.2: Encourage research into policy making and new technologies for a balanced approach to regulate data collection and use practices in businesses that would both protect privacy and maintain a competitive advantage.

R.3.2.3: Support the adoption of security and privacy by design methodologies in businesses by creating research programs to integrate these methodologies into design tools widely used in industry.

R.3.2.4: Encourage businesses to conduct risk assessment and mitigation procedures for their products and services by regulation or by creating incentives. This will in return help streamline the users of these products and services to carry out their own risk assessment for their operations.

R.3.2.5: Encourage businesses to report on security and privacy incidents, leading by example in governments and by publicizing best practices where proper risk management has protected critical processes and minimized damage to companies and their users.

R.3.2.6: Support multidisciplinary research into regulatory policy making in the critical infrastructure sectors that encourages the adoption of latest security and privacy technologies and processes without disrupting these critical services and market realities.

3.3 Governments

Governments at national, regional and local levels have a major role in organizing societies and economies. As such, they are critical actors in the governance of NIS and privacy domains. Emergence and proliferation of Internet technologies and their wide adoption seems to have occurred largely outside government control or initiative. When security and privacy concerns about the use of these technologies emerged and it is seen clearly that these technologies are transforming societal relationships and economies, many individuals and groups turned to

governments to act. Below, we look at the role of some of the branches of government in the NIS and privacy domain.

3.3.1 Law Enforcement

Many national law enforcement agencies have formed cyber security divisions against cyber crime, on-line fraud and on-line abuse. Their efforts are being hampered by the rapid changes in technology and capabilities of the criminals and the fraudsters as well as the inadequacy of the applicable laws which remain behind technology and market realities. Some of the challenges met by law enforcement agencies can be listed as follows:

- *Capacity building:* The curricula used in the education and training programs of law enforcement agencies often fall short in technology areas they need to track and bring to justice on-line crimes. These programs also do not have enough practical experience. Therefore, lack of qualified personnel is a major issue in these organizations.
- *Privacy awareness:* Activities of law enforcement agencies often have implications for privacy since they might have to manipulate personal data or trace individuals on-line. Drawing a distinction between what is a criminal activity and what is not in the digital world is not an easy task. Awareness of law enforcement personnel about the privacy concerns of the society and individuals is of paramount importance and appropriate privacy safeguards are essential.
- *Forensics challenges:* There are many technical difficulties with identifying, time stamping and staging on-line and off-line ICT activities. Tools used by forensics experts might fall short on these aspects. Therefore law enforcement agencies might often have to work with limited data and evidence. Another challenge is the difficulty of identifying individual identities on-line.
- *Lack of international cooperation:* Many of the on-line activities that are of concern for law enforcement agencies could be sourced from outside their own jurisdictions. When such incidents occur it becomes very difficult to collect evidence or trace on-line activities. International cooperation in this field is hampered by the lack of international laws and norms governing this space. When sharing information across borders could be breaking local laws, investigations suffer.

There are attempts to harmonize laws and increase such cooperation but different governance systems and societal perceptions pose difficulties.

3.3.2 Surveillance

The 30 year review of OECD privacy guidelines indicates that “if people feel that any surveillance of them is for appropriate reasons and they are aware of it, then trust is strengthened” [20]. The key to establishing this appropriateness is “oversight”. Appropriate oversight mechanisms could ensure that surveillance operations do not infringe on personal rights and freedoms unnecessarily and the collected information is used for its intended purpose and duration. In most countries there is a judicial authorization component of surveillance to help establish this oversight.

Recent revelations about surveillance practices of some nations for the purposes of national security have brought to light the limitations of the current oversight mechanisms in those countries and globally. As the Internet and the sphere of activity of its service providers extend many jurisdictions, regulating surveillance activities across multiple countries is a very difficult challenge. Democratic oversight in one country would not be sufficient to cover end to end compliance.

Creating effective governance mechanisms for surveillance and oversight is a debate and problem at the heart of reconciling security and privacy in the digital world.

3.3.3 Regulators

As in many domains of ICTs today, regulators have been called to action to remedy shortcomings in the security and privacy domains in the digital world. Regulators' role is essential in society but they wield a double edged sword: security and privacy related regulations should protect the rights and freedoms of consumers and societies while at the same time ensuring a competitive, open, growth oriented and innovation-friendly business environment.

If regulators can build effective frameworks for security and privacy in the digital world, they will foster thriving economies that are built on user trust. However, this remains an elusive task. Take the case of incident reporting of security and privacy breaches: make it mandatory and businesses will stop taking risks and innovate, make it voluntary and businesses will avoid it and consumers will suffer. Generating regulations for security and privacy in cloud and big data environments is also another example. OECD has put a lot of effort into defining the drivers,

enablers and inhibitors of a data driven economy which could guide such efforts but still, these are areas where building consensus remains a challenge.

Regulators would need to seek consensus in society and economy among consumers and businesses with a broad based stakeholder participation. The challenges of capacity building and lack of international cooperation also apply to regulators.

3.3.4 National Strategies

Cyber security has become a national policy priority in many countries and produced strategies are increasingly holistic: including economic, social, educational, legal, law-enforcement, technical, diplomatic, military and intelligence-related aspects [21]. The challenge of balancing security priorities with those of personal privacy and an open Internet promoting innovation and growth is recognized in policy spheres. Most strategies aim to increase coordination and the free flow of information, while preserving privacy and freedom of speech provisions [21]. These strategies encourage a multistakeholder approach to policy making and provisions for public-private partnerships in this domain.

One of the key pillars of national strategies is the monitoring of key national infrastructures for cyber threats and securing them. The importance of the economic drivers for cyber security is recognized and a drive to create a cyber security industry sector is included. Compliance and enforcement are usual parts of government legislation and regulation. For these to function appropriately, indicators and criteria for compliance should be well defined. In the cyber security realm, defining these criteria and assigning responsibilities remain major challenges.

Non-exploitation: Many of the threats and risks that emerge in the NIS domain are results of zero-day vulnerabilities. The general and preferable principle of such vulnerabilities has been to report them to the responsible parties for patches to be released and make general announcements for these patches to be adopted by the general users.

However, it has also been seen, especially within the recent revelations on surveillance practices, that such vulnerabilities have been exploited for advantage – be it for economic competitiveness or offensive purposes, by state or non-state organizations. Such practices further erode user trust in such systems.

“Non-exploitation” principles are beginning to appear in national strategies and international cooperation manuals. However, more needs to be done to build mechanisms at legal and regulatory levels to facilitate

the management of unknown vulnerabilities. How this can be done to the benefit of both users and nations is still an open area of research.

Critical Infrastructures: Critical infrastructure protection appears in most national cyber security strategies and associated frameworks [17]. Advancing ICT use in critical infrastructures creates new operational and societal challenges more than technological ones. When these critical systems come on-line, their risks grow and due to their societal importance the management and mitigation of these risks are essential. Yet, ICT related risk awareness and preparedness in these infrastructures and their operators seem to be generally low due to their legacy operational models and systems. It would be worthwhile to explore if specific risk management approaches and methodologies would be beneficial for this sector.

3.3.5 Recommendations

R.3.3.1: Encourage capacity building programs for law enforcement and regulatory agencies with both technological and societal components.

R.3.3.2: Support the implementation of privacy awareness programs and the installation of privacy safeguards in law enforcement agency operations.

R.3.3.3: Support research into the development of up-to-date forensics tools that have built in privacy and personal rights and freedoms safeguards.

R.3.3.4: Support the establishment of international cooperation fora and frameworks for law enforcement and regulatory agencies that are sensitive to local and international laws and regulations. Such efforts would benefit from the creation of international pilot programs.

R.3.3.5: Support research into effective oversight mechanisms into surveillance and tracing operations of law enforcement and national agencies to ensure personal rights and freedoms are protected (Covered by recommendation R.2.5.4 as well).

R.3.3.6: Support interdisciplinary and international research into creating regulatory frameworks that can effectively balance business requirements of open innovation and growth and consumer requirements of privacy and security.

R.3.3.7: Support research to define and implement effective indicators and measurements for cyber security and privacy to inform policy making.

R.3.3.8: Support research into international mechanisms to be created to manage zero-day vulnerabilities before their exploitation.

R.3.3.9: Support NIS awareness raising and capacity building programs in the critical infrastructure sector.

R.3.3.10: Encourage research into the feasibility and benefits of new security risk management approaches specific to the critical infrastructure sector.

3.4 State Institutions

3.4.1 Legislators

A major trend in law making for the digital world has been the preservation of the rights, freedoms and societal values of the physical world in the digital world. Using this approach it is possible to project the accumulated know-how of civilizations to the digital world hence supporting established societal norms and ways of life. However, many concepts are relatively different in the digital world:

Identity and anonymity: On the one hand digital identities could be difficult to verify but they are somewhat traceable. On the other hand, absolute anonymity in the digital world is not assured. This makes assigning responsibility or performing anonymous actions (such as voting in elections) difficult in the digital world, respectively.

Ownership and copyright: As a consequence of digital/virtual media being distinct from physical media, ownership rights, means of production, copyright and protection of intellectual property are all different and laws governing these concepts, their enforcement and associated punishment are different. In the big data world, who owns the collected or generated data?

Consent: Online applications and services, social media tools and most websites rely on some sort of consent from its users on their activities. Most of the time the amount of information to be read and controlled to give explicit consent is huge and most users either approve without reading or implicit consent upon usage is assumed.

Control and responsibility: What are the limits of an individual's responsibility in the digital world, especially if he/she cannot exert control over data generated by or for him/her?

Timescales: Long timescales in law making seem to be incompatible with the very fast pace of developments in the digital world. Laws in this domain might become obsolete if not enacted fast enough.

International cooperation: In the interconnected world of the Internet, systems can be reachable across nations, applications run on a number of distributed servers worldwide and the source and destination of a communication or data flow can be at opposite ends of the world [15]. Accordingly, legislating only within national borders does not cover the necessary elements of ensuring NIS. International law and harmonization and cooperation among legislators and regulators are essential.

All of the above challenges in the digital world apply to legislating NIS and privacy domains as well. Laws that create a level playing field for all societal actors need to be enacted in due time to build trust in the digital world. It is particularly challenging to catch up with the pace of technology, assess its societal implications and establish laws to regulate it. Interdisciplinary expertise is mostly needed in this domain and it is not easy to find. The work of organizations such as the OECD in creating guidelines in this area is a welcome relief.

3.4.2 Judiciary

As the rule of law is the fundamental component of a democratic and equitable society, the judiciary is one of the main actors to implement and deliver this rule. As in all domains, in the NIS domain as well, the judiciary is the safeguard for the fair and equitable implementation of the laws in cases of conflict or otherwise.

In the ICT domain in general and the NIS domain in particular, it has repeatedly been stated that laws have not been able to catch up with what is possible technologically and what is happening on the ground in society. While this is a matter for the legislators and the policy makers in general to correct, it places extra burden on the judiciary. In the absence of applicable laws, the judiciary decides on conflicts in this domain with limited guidance and by relying on external experts and the resulting decisions could be controversial and challenged.

The judiciary makes its decisions on cases based on provided evidence. Due to limitations on available forensic tools and the capabilities of law enforcement authorities, the evidence presented to courts might be insufficient or inconclusive to decide on cases. These shortcomings need to be overcome for justice to be delivered with respect to NIS related cases.

3.4.3 Privacy and data protection authorities

Many countries have set up independent privacy commissioners or data protection authorities. These organizations aim to protect the

privacy and the personal rights and freedoms of individuals in an equitable society [12]. Some of these authorities could rule on cases brought before them and have the power to sanction companies due to their practices infringing on personal rights and freedoms.

There have been high profile cases where very large global companies have been forced to change their data collection and manipulation practices, how they implement opt-in, opt-out rules for their new features or details in their security and privacy terms of use because of the diligent work of privacy and data protection authorities.

However, privacy and data protection authorities are often understaffed and under financed capable only to handle a fraction of the potential cases they may need to cover. Additionally, they fall behind in technology know-how. It would be beneficial to raise the profile and resources of these authorities to expand on their function to create a balance between consumers and businesses as well as security and privacy.

3.4.4 Recommendations

R.3.4.1: Support research into how legal concepts in the physical world and the digital world differ and which ones can be carried forward from the physical world to the digital world and how new concepts like digital identity, digital rights and others affect existing laws.

R.3.4.2: Support research into if and how timescales in law making for the digital world can be shortened to keep up with the pace of technology.

R.3.4.3: Support research into how the evidence base in NIS related legal cases may be improved. Also support capacity building in the legal system so that reliance on external experts can be reduced.

R.3.4.4: Support privacy and data protection authorities by enhancing their technical capacities and staff and financial resources to cope with the ever increasing challenges of privacy and consumer protection in the digital world.

R.3.4.5: Encourage international collaboration at every level of policy and strategy making, and legislation to harmonize laws and policies so that a coordinated effort to ensure NIS can be possible across national borders.

3.5 International Organizations

International organizations facilitate much needed collaboration and cooperation in the NIS domain among nations. They might have economic, developmental, legal or human rights perspectives. They

approach NIS and privacy matters from their own perspectives. Standards organizations can also be considered as international organizations and they have already been covered in a previous section.

In the NIS domain, while some organizations like the OECD try to produce policy and strategy guidance on NIS [18], privacy and data protection subjects for governments to use, others like the Council of Europe, try to establish norms in national laws to protect human rights and personal rights and freedoms across nations [3], [4], [5]. As a UN agency, ITU provides technical and policy assistance to developing nations in the NIS domain [36]. The Internet Society (ISOC) encourages a multistakeholder dialogue on technical and societal matters concerning an open and free Internet [37].

International organizations help distribute best practices and know-how in the NIS domain worldwide. What they produce is usually not binding and they have to be accepted or ratified by national authorities or institutions. Therefore a system of international NIS law or governance has not yet been established. This is to the detriment of law enforcement or regulatory agencies or legislators and judiciary who seek international cooperation to resolve local NIS problems to no avail. The ongoing Internet governance debates are good examples of the challenges facing international organizations and their effectiveness. However, there are also international organizations like the European Court of Human Rights that have binding international authority, which could provide a good example and encouragement for such collaboration in the NIS domain in the future.

3.5.1 Recommendations

R.3.5.1: Explore the feasibility of creating international organizations that would help operate binding NIS and privacy and data protection mechanisms worldwide.

3.6 Civil Society Organizations

Civil society organizations defend the interests of individuals, groups and the environment in general. In the context of NIS, these organizations strive to ensure that policies, strategies, tools and techniques respect the public interest. Individuals' rights and freedoms and an open, free and interconnected Internet are also defended by civil society. In the wake of the recent revelations on the surveillance and spying activities of some states, civil society organizations have been playing a critical role to defend individuals' rights. What individuals cannot achieve to defend their interests in cyber space, civil society

organizations can. Transparency, data protection, oversight, diversity, privacy, empowerment, inclusiveness are defended by civil society in NIS policy making. Including the civil society perspective in strategy and policy making ensures that the produced strategies have a better chance of adoption and acceptance by users.

Creative commons licensing schemes, open source software and tools, many free on-line educational programs using Massive Open Online Courses (MOOCs), crowd sourcing and crowd funding initiatives, fighting the digital divide are all happening through civil society organizations.

While a lot has been achieved by civil society organizations regarding representation, there is still much to be done to achieve multistakeholder participation in NIS strategy and policy making. Civil society organizations usually participate in these activities on an observer status and their contributions are often considered in an elective way. However, as the examples given above show, the output of civil society can be measured and can be shown to be effective. Therefore, they deserve much more space in current debates on cyber security and privacy.

3.6.1 Recommendations

R.3.6.1: Ensure that civil society organizations participate on an equal footing with all other stakeholders in NIS strategy and policy making activities.

R.3.6.2: Encourage individuals to support and participate in civil society organizations, especially those who belong to disadvantaged groups in the digital world.

R.3.6.3: Support civil society organizations in the NIS domain to acquire adequate technical expertise, tools and capabilities by creating programs for financial independence, awareness raising and education.

3.7 European Union

The European Commission published its Cyber Security Strategy [13] and its associated proposed Network and Information Security (NIS) Directive [14] in February 2013 to ensure a common level of cyber security across all countries of the European Union. The NIS Directive was subsequently adopted by the European Parliament in March 2014.

The European Commission recognizes the positive impact of an open and free Internet on freedom of expression, on political and social inclusion and on collaboration across national borders. The EU strategy maintains that for cyberspace to remain open and free, the same norms,

principles and values that the EU upholds offline, should also apply online. Fundamental rights, democracy and the rule of law need to be protected in cyberspace. Development of the industrial and technological capabilities is defined as a strategic priority, especially since many of the software and hardware components in use in Europe are produced elsewhere. Therefore, research towards self sufficiency in this domain is encouraged.

The EU NIS directive [14] is aiming to bring all countries in the EU to a common level of proficiency with respect to managing cyber security risks. Emphasis is again on critical infrastructure sectors and government installations. A common framework for incident response and information sharing is a cornerstone of the directive, where mandatory reporting of incidents is considered. It is indicated that the lack of a coherent and coordinated response to NIS incidents and risks among member states is creating an environment of divergent regulations and standards that in fact reduces the level of cyber security. It is also indicated that when companies try to comply with divergent regulations and standards in multiple countries, this increases their cost of operation and discourages them from innovation and growth. The fundamental elements of the NIS Directive can be summarized as follows:

- Adoption of national cyber security strategies, including national competent authorities and national CERTs;
- Cooperation and coordination among member states and the European Commission;
- Mandatory security risk management and incident reporting for government installations and critical infrastructure operators;
- Use of NIS standards;
- Enforcement of the NIS directive requirements.

These elements are recurring themes in NIS policy making and have been emphasized in the previous sections of the current document.

Since the establishment of the EU Cyber Security Strategy and the NIS Directive, an important societal challenge emerged related to the revelations about the alleged surveillance and spying practices of state agencies around the world. These allegations have significantly eroded public trust in the digital world in Europe. To regain the trust of the public, safeguards on personal rights and freedoms and oversight

mechanisms over surveillance and security operations could be included in policy and strategies.

3.7.1 Recommendations

R.3.7.1: Support initiatives to include in the European Cyber Security Strategy and the NIS Directive safeguards on personal rights and freedoms and appropriate oversight mechanisms over surveillance and security operations.

4 Emerging NIS Domains and Society

In this chapter, we look to the future and cross-check our largely platform independent findings with the NIS implications of new and emerging ICT domains which will have strategic impact on society. These emerging domains have been highlighted in the annual systems security roadmap deliverables of SysSec [30], [31], [33], including notably the Red Book [32], as well as the EU NIS Platform Secure ICT Research Landscape deliverable [10].

4.1 Big Data

Big data technologies and a data driven economy are identified as major innovation and growth opportunities for the future. It is also one of the areas that keep national privacy and data protection authorities busy. Big data provides both challenges and opportunities in the NIS domain. The challenges usually come in the privacy and transparency area. There are also opportunities to create proactive security tools by using big data analytics techniques:

- Due to the very large amount of data being collected and manipulated in big data systems, the speed and scale at which these systems operate and the complexity of the analytics tools involved, it is very difficult to monitor and audit these systems with event logging and management tools. Accordingly, incident reporting, ensuring transparency or providing safeguards for privacy protection are major challenges with social, legal and regulatory implications.
- Big data analytics systems have very advanced capabilities for correlation among different data sets, creating opportunities for profiling. Discrimination and loss of privacy could become possible threats for individuals and groups.
- Collected and derived data ownership is an area open for exploits since exerting ownership rights and control over such data in big data systems could be a significant challenge. This could lead to many threats including identity theft.
- Big data analytics technologies provide a multitude of decision support systems from suggesting one's next on-line purchase, to the next movie one will see. It is indicated that these systems might streamline people's on-line behavior and choices and reduce

diversity and distort free will. Less diversity, more uniformity will lessen the richness and robustness of a society and therefore are serious challenges for the future.

- Usage of big data analytics tools on NIS meta data, such as logs and traces from different network elements and servers in real time could lead to the creation of new security tools that can predict imminent threats and attacks and deploy countermeasures. These can lead to ethical issues if false positives lead to unwarranted accusations and counter measures.

4.1.1 Recommendations

R.4.1.1: Encourage research into the development of tools and techniques for effectively monitoring and auditing big data systems.

R.4.1.2: Support research into analyzing and characterizing the potential of big data systems for profiling and discrimination.

R.4.1.3: Encourage research into the potential impact of big data systems on diversity in society and individuals' free will.

R.4.1.4: Support research into the ethical implications of real-time, proactive NIS tools and countermeasures that are derived using big data analytics technologies.

4.2 Internet of Things

In the not so distant future there will be sensors and nodes collecting information about all aspects and locations of the physical world and our activities in it. Moreover, these sensors and nodes will also be able to communicate with each other and share information and decisions in an autonomous fashion, aided by artificial intelligence technologies. This will create a multitude of challenges for security and privacy processes and systems:

- Privacy will be very difficult to achieve when there are so many data collection points and surveillance opportunities.
- Maintaining transparency in the Internet of things: Legislating, regulating and enforcing security and privacy safeguards in the Internet of things will be much harder than today due to the difficulty of having control and observability points in these systems. Scalability and dynamicity of the configuration of this huge network of intelligent nodes will be hard to tackle.

- Internet of things entities will be able to function and operate without human intervention hence creating questions about ethics, code of conduct and trust in general.
- Due to their small scale and cost constraints protecting the sensors and nodes in IoT from cyber attacks could be difficult since they will not have the resources to implement sophisticated mechanisms. As such, these devices could be easy targets and once compromised, could lead to serious threats due to their adoption in most aspects of the environment and our daily lives.
- As human interaction gets removed from the operation of autonomous Internet of things, identity management, as well as authentication and authorization will have new meanings and bring about new challenges. The definition of free will, will also be altered.
- Operating and protecting critical infrastructures in an IoT environment with the autonomous behaviour of these devices as well as their potential vulnerabilities will be a challenge.

4.2.1 Recommendations

R.4.2.1: Support advance research into innovative, small-scale, low resource utilization technologies to maintain privacy, security and transparency in the Internet of things.

R.4.2.2: Create research programs into the ethical implications of IoT systems that operate autonomously without human intervention, their code of conduct and trust models.

R.4.2.3: Implement research programs for identity management in the Internet of things.

R.4.2.4: Encourage research into governance models for critical infrastructures running on the Internet of things.

4.3 Mobile Devices

Mobile devices are proliferating in a rapid way. Due to their business and operational models, some of these devices are creating tightly controlled, streamlined interfaces and applications. They have adopted the so-called “appliance model”. Any unauthorized behavior is not permitted and only applications certified by the manufacturer can run on them. This is a big challenge for diversity and freedom of choice.

Mobile devices are becoming an interface to the world for their users. They see the world from the perspective and content of the

applications on their mobile devices. Especially the young people are not aware of their environment or fellow people or phenomena if they are not represented on mobile devices. Mobile devices become the predominant ICT resource of individuals. This is a major dependency for individuals affecting their autonomy. Mobile devices also represent a significant portion of the identity of an individual, creating challenges in the identity management domain.

The mobile market is a tightly controlled space where a small number of providers and technologies are controlling the market. This is alarming for the sustainability and resilience of these systems.

Mobile devices are also the focal point for sensor deployment. As such they carry many of the challenges of the Internet of things with them.

It is undeniable that mobile devices play a key role in accessibility and affordability of ICT services and applications, helping to mitigate the “digital divide”. However, their potential could be reduced due to the lack of freedom of choice presented by some of the current suppliers who try not only to control the devices but also their users' behavior.

4.3.1 Recommendations

R.4.3.1: Support research into the impact of mobile devices in the fundamental societal concepts of diversity, freedom of choice, individual's autonomy and identity.

R.4.3.2: Encourage research into how the current mobile device business model and market conditions are affecting long term sustainability and resilience of the mobile market and innovation.

5 EU NIS Platform Activities

The EU Network and Information Security (NIS) Platform was created “to foster the resilience of networks and information systems in Europe” as part of the EU Cybersecurity Strategy and in line with the associated NIS Directive [6]. The NIS Public-Private-Platform is intended to help the implementation of the NIS Directive across the EU.

The NIS Platform had its first meeting on 17 June 2013. In this meeting, three working groups were formed:

1. WG1 on risk management, information assurance, risk metrics and awareness raising;
2. WG2 on information exchange and incident coordination, incident reporting and risk metrics for the purpose of information exchange;
3. WG3 on secure ICT research and innovation.

The NIS Platform convenes general plenary sessions where working groups report on their activities to the general constituency. Working groups themselves organize their meetings generally around these plenary sessions and at other dates as needed. The platform brings together a wide range of participants from the public, private and voluntary sectors and academia. It employs participatory and innovative methods during its sessions to encourage openness and inclusion.

SysSec partners have been participating in the NIS Platform plenary meetings and its working groups from their first inception. The focus of SysSec partners has been Working Group 3 to contribute to the shaping of the secure ICT research landscape in Europe. The following NIS Platform Plenary and WG3 meetings have taken place in Brussels to date:

1. NIS Platform First Plenary Meeting: 17 June 2013;
2. NIS Platform WG3 Kick-off Meeting: 27 September 2013;
3. NIS Platform Second Plenary Meeting: 11 December 2013;
4. NIS Platform WG3 Meeting: 29 April 2014;
5. NIS Platform Third Plenary Meeting: 30 April 2014;
6. NIS Platform WG3 Meeting: 16 July 2014;
7. NIS Platform Fourth Plenary Meeting: 25 November 2014.

5.1 NIS Platform Working Group 3 (WG3)

The main *objectives* of WG3 are:

- Contributing to the coordination of European activities in research and innovation in connection with the European Cybersecurity Strategy;
- Producing high quality deliverables summarizing its main findings.

The *scope* of WG3 are given as follows:

- Identifying key challenges and desired outcomes in the research and innovation context of the EU Cybersecurity Strategy and the NIS Directive;
- Promoting multidisciplinary research to foster collaboration among researchers, industry and policy makers;
- Examining ways to increase the impact and commercial uptake of research results.

The main *deliverables* of WG3 are:

- Secure ICT Research Landscape [7];
- Business Cases and Innovation Paths [8];
- Snapshot of Education and Training [9];
- Strategic Research and Innovation Agenda as informed by the previous deliverables and driven by three Areas of Interest (individual layer, collective layer and infrastructure layer) [10].

Each of the deliverables and the contribution of SysSec partners to these deliverables are detailed in the following sections. SysSec project coordinator Professor Evangelos Markatos of FORTH has been a member of the WG3 Steering Committee and Ali Rezaki from TUBITAK – BILGEM has been a member of WG3. Both have been attending the NIS Platform WG3 and NIS Platform Plenary meetings and have actively been contributing to its deliverables and discussions in person and on the collaboration platform set up by ENISA for the NIS Platform. There has been an exchange of information, ideas and documents both from SysSec to the NIS Platform and back.

5.1.1 NIS Platform WG3 Secure ICT Research Landscape Deliverable

After a number of internal iterations the first public release of the Secure ICT Research Landscape deliverable, version 1 [7] was issued in

July 2014. SysSec project coordinator Professor Evangelos Markatos of FORTH is one of the four editors of this deliverable. In addition, individual contributors from SysSec partners have been acknowledged in the deliverable as: Magnus Almgren (Chalmers), Elias Athanasopoulos (FORTH), Sotiris Ioannidis (FORTH), Thanasis Petsas (FORTH) and Ali Rezaki (TUBITAK – BILGEM). SysSec has also been listed as a supporting project in the contributions section of the document.

The goal of the Secure ICT Research Landscape deliverable has been to describe the current state of the art in cyber security technologies and application domains and to identify the current threats and the corresponding short term research challenges. This deliverable starts with the basic building block cyber security technologies, then focuses on cloud computing and the Internet of things and subsequently analyzes application domains such as e-government and critical infrastructures to identify research challenges.

It has been the decision of the NIS Platform leaders and the European Commission to keep the scope of this deliverable purely technical and include the societal dimensions of the research landscape in the other platform deliverables and the SRA, notably its individual and collective Areas of Interest.

5.1.2 NIS Platform WG3 Business Cases and Innovation Paths Deliverable

The Business Cases and Innovation Paths deliverable [8] has been focused on rapid exploitation of cyber security research results. The content of this deliverable is the result of extensive discussions in face-to-face meetings of WG3 and on-line collaboration. SysSec attendees to the WG3 meetings as stated above have provided input to these discussions. This deliverable is in draft format and has not yet been released publicly. It is scheduled for release in early 2015.

The deliverable introduces use cases for priority research areas in cyber security. These use cases have been derived from initial sample market and industry analyses and user requirements in these domains. After high-impact use cases have been selected, their cost-benefit and economic impact analyses have been made. The deliverable also covers innovation models and best practices and successful innovation management examples, concluding with recommendations for EU research and innovation programs.

5.1.3 NIS Platform WG3 Snapshot of Education and Training Deliverable

The goal of the Snapshot of Education and Training deliverable [9] is to provide a picture of the cyber security education and training programs in Europe and produce recommendations to fill the gaps in skills requirements and available education and training programs. This deliverable has been informed by face-to-face discussions during WG3 meetings, on-line contributions and surveys. SysSec attendees in WG3 as stated above, have provided their input and filled in surveys for the data collection efforts of this deliverable. This deliverable is in draft format and has not yet been released publicly. It is scheduled for release in early 2015.

5.1.4 NIS Platform WG3 Strategic Research and Innovation Agenda Deliverable

The Strategic Research and Innovation Agenda deliverable [10] is the flagship deliverable of WG3. Its goal is to define a strategic research and innovation agenda in cyber security, starting from desired vision states (Areas of Interest) that are wished to be achieved by 2025. The deliverable considers not only technological but also social, legal, business and educational aspects of cyber security and privacy. It aims to provide strategic recommendations for policy and research. It is supported by all the previous WG3 deliverables and parallel activities in the three Areas of Interest. The deliverable is in its final stage of editing and is scheduled for public release in early 2015.

SysSec project coordinator Professor Evangelos Markatos from FORTH and project partner Ali Rezaki from TUBITAK – BILGEM have provided extensive input and feedback to this deliverable and the Areas of Interest as acknowledged in the document itself. AoI1 and AoI2 focus on societal aspects of Cyber Security and privacy and have been concentration areas for SysSec partner contributions with respect to the supporting efforts related to the current SysSec deliverable D4.5, release 2.

The deliverable contents and structure have been formed during the WG3 meetings. The main concepts covered were summarized in the following three Areas of Interest (AoIs):

- AoI1: Individuals' Digital Rights and Capabilities (Individual layer);
- AoI2: Resilient Digital Civilisation (Collective layer);

- AoI3: Trustworthy (Hyperconnected) Infrastructures (Infrastructure layer).

While AoI1 provides a perspective on the individual with his/her rights and enablement, AoI2 looks from the point of view of organizations to provide trustworthy digital institutions and societies. AoI3's focus is on the infrastructures of the future to support the individuals and societies. Three subgroups were formed to focus on each AoI. AoIs describe their vision, the challenges to reach this vision, the enablers and inhibitors from technological and societal perspectives and provide gap analyses leading to research and innovation recommendations. Below, we go into the details of each AoI.

SRA AoI1: Individuals' Digital Rights and Capabilities (Individual layer):

The individual is at the center of the challenge on reconciling security and privacy in Europe. With ever more data being generated about individuals, claims of surveillance practices infringing on personal rights and freedoms and increasing number of threats and vulnerabilities for individuals in mobile and cloud environments, maintaining a secure, open and transparent environment for a productive and healthy lifestyle for individuals is getting more and more difficult. AoI1 provides a citizen centric view and vision. It provides a view towards enhancing technological aspects with social, legal and regulatory aspects of security and privacy. Loss of trust of individuals towards the digital world is a recurring theme and how to counter and build a trustworthy environment forms an important part of AoI1's contribution. AoI1 also requests that the major societal concepts outlined at the initial chapters of this current deliverable are also given priority in building ICT systems.

After the citizen centric vision is presented, societal, political and educational challenges are detailed in AoI1. Enablers and inhibitors at technology, policy and regulation areas are listed. The AoI then provides a list of technological as well as social, political and governance gaps to reach its citizen centric vision.

SRA AoI2: Resilient Digital Civilisation (Collective layer):

The scope of AoI2 is building trust in organizations and institutions that make up governments, businesses and civil society in the digital world. Like AoI1, AoI2 also looks at both technological and societal requirements. The impact of emerging technologies on institutions and their ability to serve citizens and society are detailed in this AoI. This is followed by societal and political challenges and economic and educational ones with respect to increasingly interdependent

organizations in a connected global civilisation. Technology and policy enablers and inhibitors are presented followed by a statement of technological, societal and governance gaps. Many of the challenges and issues raised in AoI2 resonate with the contents of the previous chapters on societal concepts and actors of this document.

SRA AoI3: Trustworthy (Hyperconnected) Infrastructures (Infrastructure layer):

The vision of a hyperconnected ICT infrastructure that supports the individual and institutional visions is depicted in AoI3. Critical infrastructures that support all societal processes are the main focus of this AoI. After a general description of the challenges, enablers, inhibitors and gaps, these items are elaborated on each critical infrastructure sector, such as energy, transportation, healthcare and finance. These sectors reflect the contribution of NIS Platform WG3 members from different sectors of the economy that support such critical infrastructures. They have highlighted their everyday challenges in a fast changing ICT landscape and their security and privacy obligations and priorities. This AoI demonstrates how technology directly affects the most critical processes of the society and economy and the role of security and privacy technologies in creating challenges and opportunities in this area.

After the AoIs, the SRA deliverable includes a cross analysis section to identify the common research and innovation priorities among the AoIs followed by their divergences. Finally, the SRA provides a synthesis of the contents of the business case and educational snapshot documents with a societal, educational and economic point of view.

Going forward, NIS Platform WG3 deliverables and especially, the Strategic Research Agenda document will be maintained as living documents that will be regularly updated to reflect the changes in technology and society. WG3 will also bring its findings to the other working groups of the NIS platform and strive to build on the relationships formed among all the stakeholders in the group, with an emphasis on SMEs for the benefit of European NIS research and innovation policy making. SysSec partners in WG3 will continue to support these efforts well beyond the completion of the project.

6 Recommendations

By analyzing our target space through concepts, actors and emerging technology view points in the preceding chapters, we identified research and policy challenges and gaps which led to the recommendations under each subsection. Some of these recommendations were overlapping since they arrived at the same conclusion from different points of view. In this chapter, we consolidate the recommendations to a single list by eliminating repetitions. We have also classified the recommendations into the following six categories for easier reception and handling by their respective actors:

- Research recommendations on social and economic aspects;
- Research recommendations on legal and regulatory aspects;
- Research recommendations on technology aspects;
- Policy and strategy recommendations on social and economic aspects;
- Policy and strategy recommendations on legal and regulatory aspects;
- Policy and strategy recommendations on technology aspects.

When one recommendation presented action in more than one category the dominant category is chosen. The resulting list of recommendations below covers the research and policy challenges we see in the NIS societal landscape without any particular order or priority.

It is recognized that there should also be feedback from the social, legal and regulatory aspects of NIS to the technological aspects leading to concrete changes in technology to address societal challenges and requirements. Hence our inclusion of recommendations in the technology category for both research and policy domains.

A prominent example of this feedback loop is the push-back received from the public and the NGOs on security measures that do not sufficiently protect personal data and infringe on personal rights and freedoms while trying to secure cyberspace. Therefore, the subject of “oversight” has been repeatedly identified as a key research and policy area that brings security and privacy challenges together.

6.1 Research Recommendations on Social and Economic Aspects (RSE)

R.2.1.2: Support research into how current organizational security and privacy risk management procedures can be applied to individuals.

R.2.1.4: Support research into how a viable cyber insurance market can be created that includes effective measurement of NIS risks and accurate estimates of the value of digital assets.

R.2.5.4: Support multidisciplinary research into devising appropriate privacy protection oversight mechanisms on surveillance activities of security organizations and operations to ensure public trust.

R.2.5.5: Support research into evaluating the trade-offs between anonymity and traceability for personal privacy versus public accountability.

R.2.6.1: Support multidisciplinary research into how the concepts of ownership and assets in the conventional world extend into the digital world and if there is a case to modify them for the public good.

R.2.6.2: Support research into creating innovative insurance models for the digital world.

R.2.7.2: Support research on reducing on-line discrimination, intolerance and bullying by both technical and non-technical methods.

R.2.9.5: Support research programs into determining requirements in skills, key technologies and business models that would support a free standing European NIS market.

R.4.1.3: Encourage research into the potential impact of big data systems on diversity in society and individuals' free will.

R.4.1.4: Support research into the ethical implications of real-time, proactive NIS tools and countermeasures that are derived using big data analytics technologies.

R.4.2.2: Create research programs into the ethical implications of IoT systems that operate autonomously without human intervention, their code of conduct and trust models.

R.4.3.1: Support research into the impact of mobile devices in the fundamental societal concepts of diversity, freedom of choice, individual's autonomy and identity.

R.4.3.2: Encourage research into how the current mobile device business model and market conditions are affecting long term sustainability and resilience of the mobile market and innovation.

6.2 Research Recommendations on Legal and Regulatory Aspects (RLR)

R.2.1.3: Support research into increasing and streamlining incident reporting that will use a balanced approach between incentives for voluntary reporting and tight regulation that will create an environment which is neither ineffective for reporting nor stifling for innovation and competitiveness.

R.2.8.1: Support research into Internet governance models that promote both openness and necessary controls to ensure security and stability of the systems.

R.3.2.2: Encourage research into policy making and new technologies for a balanced approach to regulate data collection and use practices in businesses that would both protect privacy and maintain a competitive advantage.

R.3.2.6: Support multidisciplinary research into regulatory policy making in the critical infrastructure sectors that encourages the adoption of latest security and privacy technologies and processes without disrupting these critical services and market realities.

R.3.3.6: Support interdisciplinary and international research into creating regulatory frameworks that can effectively balance business requirements of open innovation and growth and consumer requirements of privacy and security.

R.3.3.7: Support research to define and implement effective indicators and measurements for cyber security and privacy to inform policy making.

R.3.4.1: Support research into how legal concepts in the physical world and the digital world differ and which ones can be carried forward from the physical world to the digital world and how new concepts like digital identity, digital rights and others affect existing laws.

R.3.4.2: Support research into if and how timescales in law making for the digital world can be shortened to keep up with the pace of technology.

R.3.5.1: Explore the feasibility of creating international organizations that would help operate binding NIS and privacy and data protection mechanisms worldwide.

R.4.2.4: Encourage research into governance models for critical infrastructures running on the Internet of things.

6.3 Research Recommendations on Technology Aspects (RT)

R.2.1.1: Support research into how security and privacy risk management methodologies can be made widely affordable and sustainable by creating tools and services, particularly for SMEs.

R.2.2.2: Support research in the field of digital identity management that will build a balanced approach between security and traceability requirements and personal privacy rights and obligations that will also enable anonymity in the digital world.

R.2.3.1: Support research into making complex virtualized systems and big data applications more transparent and accountable by adding control points to these systems for observability while including privacy assurance mechanisms.

R.2.4.1: Encourage public-private partnerships for research into creating more robust communication channels and applications that individuals and groups can use without being interrupted.

R.2.4.2: Support research in the forensics domain to trace and identify perpetrators of on-line attacks on freedom of expression.

R.2.5.3: Encourage research to add privacy by design modules and features into big data analytics tools and techniques.

R.2.10.2: Support research on how to create standardized frameworks that are both general enough to be relevant over a long period and relevant enough to cover key technical challenges.

R.3.2.3: Support the adoption of security and privacy by design methodologies in businesses by creating research programs to integrate these methodologies into design tools widely used in industry.

R.3.3.3: Support research into the development of up-to-date forensics tools that have built in privacy and personal rights and freedoms safeguards.

R.3.3.10: Encourage research into the feasibility and benefits of new security risk management approaches specific to the critical infrastructure sector.

R.3.4.3: Support research into how the evidence base in NIS related legal cases may be improved. Also support capacity building in the legal system so that reliance on external experts can be reduced.

R.4.1.1: Encourage research into the development of tools and techniques for effectively monitoring and auditing big data systems.

R.4.1.2: Support research into analyzing and characterizing the potential of big data systems for profiling and discrimination.

R.4.2.1: Support advance research into innovative, small-scale, low resource utilization technologies to maintain privacy, security and transparency in the Internet of things.

R.4.2.3: Implement research programs for identity management in the Internet of things.

6.4 Policy and Strategy Recommendations on Social and Economic Aspects (PSE)

R.2.3.2: Create frameworks for the relationships among governments, companies and individuals to govern data collection and surveillance activities to make sure all know what is collected and used for which purposes with the appropriate oversight mechanisms.

R.2.5.1: Support extensive awareness raising programs for personal privacy and safety in the digital world so that unsuspecting individuals and groups do not fall victim to privacy attacks. While the technology to achieve this might be available, its adoption by children, the elderly and other vulnerable groups in society is not assured.

R.2.7.1: Support awareness programs to alert the public on the scale and mechanisms of the underground economy created by on-line fraud and criminal activities and on how to minimize them.

R.2.9.1: Encourage and stimulate the creation of NIS SME's and flagship companies in Europe by creating economic incentives and guarantees for start-ups and by encouraging competitiveness in this field.

R.2.9.3: Invest more in NIS education and training to guarantee the availability of NIS personnel and creation of “home-grown” NIS companies by the creation and accreditation of dedicated programs at vocational and university levels.

R.2.9.4: Use public procurement as a tool to counter the effects of globalization on NIS related tools and technologies.

R.2.10.1: Encourage social, legal and regulatory impact analysis gate reviews for NIS standardization activities.

R.3.1.2: Bring to the forefront the empowerment of individuals, especially in relation to the management of their data and identity in the digital world.

R.3.1.3: Support research into the feasibility and effectiveness of security and privacy labels on applications and services.

R.3.2.4: Encourage businesses to conduct risk assessment and mitigation procedures for their products and services by regulation or by creating incentives. This will in return help streamline the users of these products and services to carry out their own risk assessment for their operations.

R.3.2.5: Encourage businesses to report on security and privacy incidents, leading by example in governments and by publicizing best practices where proper risk management has protected critical processes and minimized damage to companies and their users.

R.3.3.9: Support NIS awareness raising and capacity building programs in the critical infrastructure sector.

R.3.6.1: Ensure that civil society organizations participate on an equal footing with all other stakeholders in NIS strategy and policy making activities.

R.3.6.2: Encourage individuals to support and participate in civil society organizations, especially those who belong to disadvantaged groups in the digital world.

R.3.6.3: Support civil society organizations in the NIS domain to acquire adequate technical expertise, tools and capabilities by creating programs for financial independence, awareness raising and education.

6.5 Policy and Strategy Recommendations on Legal and Regulatory Aspects (PLR)

R.2.2.1: Encourage efforts to raise the profile of disruptive or emerging technologies among law makers and society at large, to study adequately its legal and regulatory challenges well in advance of their wide adoption in society. A use case and process based approach would help reveal the potential issues. Universities, standards bodies and patent organizations together with related government departments should be at the forefront of these efforts.

R.3.3.1: Encourage capacity building programs for law enforcement and regulatory agencies with both technological and societal components.

R.3.3.2: Support the implementation of privacy awareness programs and the installation of privacy safeguards in law enforcement agency operations.

R.3.3.4: Support the establishment of international cooperation fora and frameworks for law enforcement and regulatory agencies that are sensitive to local and international laws and regulations. Such efforts would benefit from the creation of international pilot programs.

R.3.3.8: Support research into international mechanisms to be created to manage zero-day vulnerabilities before their exploitation.

R.3.4.4: Support privacy and data protection authorities by enhancing their technical capacities and staff and financial resources to cope with the ever increasing challenges of privacy and consumer protection in the digital world.

R.3.4.5: Encourage international collaboration at every level of policy and strategy making, and legislation to harmonize laws and policies so that a coordinated effort to ensure NIS can be possible across national borders.

R.3.7.1: Support initiatives to include in the European Cyber Security Strategy and the NIS Directive safeguards on personal rights and freedoms and appropriate oversight mechanisms over surveillance and security operations.

6.6 Policy and Strategy Recommendations on Technology Aspects (PT)

R.2.2.3: Support awareness raising activities on ethical issues in research, innovation and business in technology companies and universities to create a sense of responsibility to contribute to society while creating new technologies and domains of activity.

R.2.9.2: Support the proliferation of open source NIS technologies and the development of their service and support eco-systems at local and national levels by creating “blue-print” frameworks and toolsets that are tried and tested at government institutions and implemented by SME's that are also accredited by governments.

R.2.10.3: Support research on the creation of standardization strategies for NIS technologies and frameworks by creating task forces or support actions in existing and new NIS programs. This research would need to take into account the trade-off between competitive commercialization considerations and standards for wider adoption and interoperability. An element of these strategies should be on cooperation among standardization organizations.

R.3.1.1: Support research into user centric security and privacy tools and technology design and implementation.

6.7 Analysis

Our recommendations are fairly evenly distributed in the three research categories with 13 recommendations for Social and Economic Aspects (RSE), 10 recommendations for Legal and Regulatory Aspects (RLR) and 15 recommendations for Technology Aspects (RT). This illustrates that as much as the implications of technology on the societal concepts, there has also been a relatively strong feedback from the social, economic and regulatory aspects of NIS towards the technology field, so that we could provide recommendations for technology to improve itself and to have positive impact on society.

In the policy and strategy domains, we provided 15 recommendations for the Social and Economic Aspects (PSE), 8 recommendations for the Legal and Regulatory Aspects (PLR) and 4 recommendations for the Technology Aspects (PT). Rather than technology, our recommendations on policy and strategy focus more on social, economic, legal and regulatory aspects which is in line with the targets of this deliverable. Technology policies in the NIS domain are relatively well established while policy and strategy support in the social, legal and regulatory aspects of NIS is much more needed.

7 Conclusions

This deliverable provided an account of the activities of SysSec partners in the social, legal and regulatory aspects of Network and Information Security (NIS) in the future Internet. This is the second release of this deliverable with a particular focus on actionable recommendations for research and policy making as well as on the activities SysSec partners carried out in the EU NIS Platform Working Group 3 (WG3) on secure ICT research and innovation.

To capture the NIS research and policy requirements and gaps, the societal landscape was first analyzed from the perspective of its fundamental concepts in Chapter 2, to determine how these concepts are transformed by NIS and privacy developments and the challenges they face as a consequence. An analysis was then performed from the perspective of leading societal actors in Chapter 3, to evaluate how their roles and responsibilities are affected by NIS challenges. A perspective from a number of emerging new technology domains has also been added to the analysis in Chapter 4. At each analysis stage, research and policy challenges were identified and more than 60 recommendations were produced to tackle these challenges.

For ease of reception, we grouped our recommendations. For each of the research and policy categories, our recommendations were classified under the three sub-domains of:

- social and economic aspects,
- legal and regulatory aspects, and
- technology aspects.

The societal analyses were carried out in parallel with SysSec activities in the EU NIS Platform, Working Group 3 (WG3) on secure ICT research and innovation. After a brief introduction to the EU NIS Platform and its WG3, the deliverable provided an account of the contributions of SysSec partners to the WG3 efforts and its deliverables. The results of the contributions of SysSec partners in the field of social, legal and regulatory aspects of NIS are not only reported in this current deliverable but are also in the deliverables of the NIS Platform WG3, as acknowledged in those documents, in particular, the Strategic Research and Innovation Agenda (SRA) deliverable.

The recurring societal themes that have emerged during our research and analyses are:

- Risk management approach to security and privacy assurance;
- Oversight mechanisms for surveillance operations;
- Transparency;
- Identity management;
- International cooperation;
- Awareness raising and capacity building.

Looking to the future, we can see that new technologies will create a more complex and challenging NIS landscape for all the societal actors. Big data systems, Internet of things and proliferation of mobile devices will together create a hyperconnected, complex, difficult to control environment which will further challenge the trust of individuals and societies in the digital world.

These are challenges but also opportunities for research and innovation, not just in technology but also in policy making and strategy for societal development.

8 Bibliography

[1] Berkman Center for Internet and Society, http://cyber.law.harvard.edu/.

[2] The Citizen Lab, University of Toronto, https://citizenlab.org/ .

[3] Council of Europe web page: http://www.coe.int/en/web/portal/home .

[4] Council of Europe: Action against economic crime: cybercrime: http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp .

[5] Council of Europe Data protection web site: http://www.coe.int/t/dghl/standardsetting/dataprotection/default_en.asp .

[6] EU NIS Platform web page: https://resilience.enisa.europa.eu/nis-platform .

[7] EU NIS Platform Working Group 3, Secure ICT Research Landscape Deliverable, July 2014: https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents .

[8] EU NIS Platform Working Group 3, Business Cases and Innovation Paths Deliverable, to appear in early 2015, draft available at https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents .

[9] EU NIS Platform Working Group 3, Snapshot of Education and Training Deliverable, to appear in early 2015, draft available at https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents .

[10] EU NIS Platform Working Group 3, Strategic Research and Innovation Agenda Deliverable, to appear in early 2015, draft available at https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents .

[11] ENISA. “Incentives and barriers of the cyber insurance market in Europe”, 2012.

[12] European Commission, Article 29 Data Protection Working Party and the Working Party on Police and Justice, “The Future of Privacy” (02356/09/EN, WP 168) (2009), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf .

[13] European Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, February, 2013.

[14] European Commission, Proposal for a Directive of The European Parliament and of the Council, concerning measures to ensure a high common level of network and information security across the Union, February, 2013.

[15] Kuner, C. (2011), "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future", OECD Digital Economy Papers, No. 187, OECD Publishing. http://dx.doi.org/10.1787/5kg0s2fk315f-en .

[16] Morrone, A., N. Tontoranelli and G. Ranuzzi (2009), " How Good is Trust? Measuring Trust and its Role for the Progress of Societies", OECD Statistics Working Paper, OECD Publishing, Paris.

[17] NIST (2014), "Framework for Improving Critical Infrastructure Cybersecurity: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf .

[18] OECD WPSPDE Web Site: http://www.oecd.org/internet/ieconomy/informationsecurityandprivacy.htm .

[19] OECD (2011a), "Trust", in Society at a Glance 2011: OECD Social Indicators, OECD Publishing. http://dx.doi.org/10.1787/soc_glance-2011-26-en .

[20] OECD (2011b), "The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines", OECD Digital Economy Papers, No. 176, OECD Publishing.http://dx.doi.org/10.1787/5kgf09z90c31-en .

[21] OECD (2012b), "Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy", OECD Digital Economy Papers, No. 211, OECD Publishing. http://dx.doi.org/10.1787/5k8zq92vdgtl-en .

[22] OECD (2013a), "Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013); Supplementary Explanatory Memorandum" (2013): http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

[23] OECD (2013b) "Guidelines governing the Protection of Privacy and

Transborder Flows of Personal Data" (2013): www.**oecd**.org/sti/ieconomy/**2013-oecd-privacy-guidelines**.pdf .

[24] OECD (2013c) "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value", (2013): http://dx.doi.org/10.1787/5k486qtxldmq-en .

[25] OECD (2013d), "Exploring Data-Driven Innovation as a New Source of Growth: Mapping the Policy Issues Raised by "Big Data"", OECD Digital Economy Papers, No. 222, OECD Publishing. http://dx.doi.org/10.1787/5k47zw3fcp43-en .

[26] OECD (2014) DSTI/ICCP/REG(2014)3: Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines, (2013),: http://dx.doi.org/10.1787/5k3xz5zmj2mx-en.

[27] Oxford Internet Institute, http://www.oii.ox.ac.uk/ .

[28] Stanford Center for Internet and Society, http://cyberlaw.stanford.edu/.

[29] The SysSec Project, main web page, http://www.syssec-project.eu/ .

[30] The SysSec Consortium. Deliverable d4.1: First report on threats on the future internet and research roadmap, September 2011. http://www.syssec-project.eu/m/page-media/3/syssec-d4.1-future-threats-roadmap.pdf .

[31] The SysSec Consortium. SysSec D4.2: Second Report on Threats on the Future Internet and Research Roadmap, September 2012. http://www.syssec-project.eu/m/page-media/3/syssec-d4.2-future-threats-roadmap-2012.pdf .

[32] The SysSec Consortium. D4.3: The Red Book: A Roadmap for Systems Security Research, September 2013. http://red-book.eu/ .

[33] The SysSec Consortium. SysSec D4.4: Final Report on Threats on the Future Internet: A Research Outlook, September 2014. http://www.syssec-project.eu/m/page-media/3/syssec-d4.4.pdf .

[34] The SysSec Consortium. SysSec D4.5, release 1: Social, Legal and Regulatory Aspects of Network and Information Security in the Future Internet, September 2013. http://www.syssec-project.eu/m/page-media/3/syssec-d4.5-social-legal-regulatory-aspects.pdf .

[35] Tech and Law Center, http://www.techandlaw.net/ .

[36] United Nations, International Telecommunications Union (ITU), Telecommunication Development Sector (ITU-D) web site: http://www.itu.int/en/ITU-D/Pages/default.aspx .

[37] Web site of the Internet Society: http://www.internetsociety.org/ .

[38] 27001:2013, ISO/IEC Information technology -- Security techniques -- Information security management systems – Requirements: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en .

[39] 27005:2011, ISO/IEC, Information technology -- Security techniques -- Information security risk management: https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-2:v1:en .