SEVENTH FRAMEWORK PROGRAMME

Information & Communication Technologies
Trustworthy ICT

NETWORK OF EXCELLENCE

syssec

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

Deliverable 4.5: Social, Legal and Regulatory Aspects of Network and Information Security in the Future Internet

Abstract: This deliverable provides a look at the social, legal and regulatory aspects of network and information security in the Future Internet. It will indicate how likely are the future threats identified in the project to cause serious impacts on the society and the economy, whether or not European legislation is in place to deal with them, if the countermeasures developed for them are applicable in the existing legal and regulatory framework. It will also indicate interdisciplinary research directions in these areas which should be carried out in parallel with the technical research activities.

Contractual Date of Delivery	August 2013
Actual Date of Delivery	September 2013
Deliverable Dissemination Level	Public
Editor	TUBITAK-BILGEM
Contributors	All SysSec Partners
Quality Assurance	Davide Balzarotti, Stefano Zanero

[†] The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 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

Contents

1 Introduction

Cyber attacks and their associated countermeasures are increasing rapidly on the Internet. They are set to increase further in quantity and sophistication in the future [1], [2], [3]. These attacks and the countermeasures deployed are having profound effects in the social, legal and regulatory spheres. Potential loss of trust of users in the functioning and services of the Internet and concerns for the preservation of privacy against both cyber threats and their countermeasures seem to be the largest impact in the social domain. The legal and regulatory fields are dominated by the motivation of governments to protect their citizens and their critical infrastructures to maintain a stable environment for the society and the economy to function.

While these endeavours were present before the introduction of the Internet, the critical role that ICT's have started to play as a transversal element in all social and economic activities created a new dimension in these challenges. The rapidity with which the ICT transformation occurred created difficulties for citizens and governments in adapting to these technologies. Network and Information Security (NIS) issues have further complicated a situation which was already complex.

This report presents the NIS landscape from a social, legal and regulatory point of view. The future threats identified in the technical deliverables of the project will be assessed with respect to their potential to cause societal impact and the readiness of the European legal framework to deal with them will be presented. The countermeasures for the threats will be evaluated with respect to their ability to function in the existing legal and regulatory constraints. Future research directions in these fields will also be presented.

2 NIS Policy Making - The Building Blocks

The main building blocks of Network and Information Security (NIS) policy making can be summarized as follows.

2.1 A Long-term Perspective

Communication theorist Marshall McLuhan famously said that the medium is the message [4]. McLuhan indicated that rather than focusing on the obvious choice of content regarding new technologies, one would benefit from focusing on the subtle long term effects of the use of these technologies to understand how they will transform individual and societal behaviour. For print media, cinema, television and the like the transformations created have not been through the stories they told, but rather through the effects of the presence of these various media forms in individual and societal life. The same has been true for the Internet and mobile technologies: the content that these technologies carry are obviously important for our immediate consumption and needs but what has been more impressive is how they transformed our relationships, businesses and societies through their presence and use. They have created these changes because they affected our life and work processes.

Similarly, cyber security challenges create a dual effect too. On the one hand, threats and incidents on the Internet pose immediate risks and have visible consequences. On the other hand, the perception of the presence or the lack of cyber security is also slowly transforming on-line and off-line behaviour for individuals and societies. People and governments react to cyber security threats not only by taking short term counter measures but also by creating designs and policies that have long term effects on how they live and operate. Both the short-term and the long-term effects of cyber security challenges need to be researched and studied.

How botnets are detected and mitigated, how mobile malware spreads or how fraud takes place using NIS vulnerabilities have immediate effect on the way we deploy Internet technologies. Where the presence of such NIS incidents and phenomena are pushing people and governments in terms of technical, societal and legal re-organization in the long term is also a key research challenge.

2.2 An Interdisciplinary Field

The study of the societal, legal and regulatory aspects of NIS and cyber security is invariably an interdisciplinary field. A number of new research centres around the world have emerged and are making significant contributions in the field [5], [6], [7], [8], [9]. Efforts to bring Internet technologists and social scientists to analyse cyber security phenomena in this field is an important step.

2.3 Based on Measurements and Data

Building policies and long term strategies upon solid data and evidence is another key pillar of this endeavour. Measurements and data collection is therefore an important component of such initiatives. On what evidence are policies based? Are they making any difference towards their goals? However, it is difficult to measure and collect data concerning NIS events, sometimes due to technical difficulties but often also due to commercial, legal or regulatory restrictions and lack of collaboration frameworks. Therefore, efforts to implement cyber security indicators and their continuous measurement [10], [11] needs to be supported by research and innovation.

2.4 An International Effort

One cannot emphasize enough the international character of Internet technologies and accompanying processes and policies to maintain and advance them. Therefore, international collaboration and consensus building are indispensable tools in this endeavour as well. Building these bridges over the trust and security of legal and regulatory frameworks would relieve both researchers and practitioners. Yet, doing so must also take into account the principle of an open and inclusive Internet.

2.5 Open, inclusive, transparent

Openness, inclusiveness and transparency are basic principles in the sphere of Internet technologies. Yet, increasingly, the realm of cyber security is clouded by secrecy and exclusiveness, since there are a lot of economic and national security concerns at play. How to create an environment for collaborative research in this area, where data, tools, policies and ideas are shared, is also a major challenge. In the absence of international regulations to govern cyber security challenges and as the global Internet gets sectioned at national borders, bringing about a comprehensive environment for international collaboration is more important than ever.

2.6 Privacy friendly

Attempts to secure cyber space invariably have privacy implications, even though cyber security measures are aimed at protecting the privacy and property of citizens and enterprises. Creating a balance between privacy and security concerns holds the potential to create a win-win situation. Otherwise, if people turn away from security measures due to the perception of privacy loss, the existing threats and vulnerabilities could have detrimental effects for not only security but also privacy. Personal information and assets could be targeted as is commonly done in social engineering attacks.

Monitoring network and information assets and their usage is a tool in cyber security efforts. However, if misused, this could potentially lead to infringements on the privacy of users and enterprises. This major challenge brings the potential for research and innovation in this field.

2.7 A Balanced Approach to Regulation and Legislation

Defining what constitutes a security incident, how it will be responded to, how it will be reported, and who has responsibility are key concepts in regulating the cyber security domain. Carrying out risk assessments and and taking preventive measures accordingly are also important elements [12]. Protecting national critical infrastructures necessary for a stable society and economy, exerting control over Internet governance and national security concerns are among the motives. Regulations in sync with existing technologies and innovation mechanisms as well as personal and societal expectations would create positive results. Experimentation and simulations in this field could support policies and regulations for beneficial results.

2.8 Risk Management

Threats and vulnerabilities in ICT assets combined with the value and importance of the assets determine the risks that potential incidents could impact the systems and their users, affecting their confidentiality, integrity and availability. Doing proper risk assessments helps to discover the vulnerabilities of the systems and evaluate the impact of their exploitation which in turn leads the way to the improvement of the systems and the deployment of countermeasures and risk mitigation strategies. Risk assessments and awareness would lead to calculated risk taking: not all systems need to be protected at the same security assurance levels since their assets have varying value and importance. As calculated risks are taken, the corresponding expectations are adjusted and mitigation strategies are prepared accordingly. If risks materialize, these mitigation activities are carried out to keep damages within expectations.

A realistic and effective approach to ensuring trust in the Internet includes the adoption of a culture of risk awareness and management supported by countermeasures and associated research and innovation activities.

3 Emerging Threats and Countermeasures

There have always been exploits and attacks on information infrastructures, well before the introduction of ICTs. If we think of the three classical principles of NIS, namely, Confidentiality, Integrity and Availability, these attributes have always been under threat, even in the era prior to electronic communications, storage and processing. Yet, the introduction of ICTs, and the Internet in particular, increased the scale of vulnerabilities, threats and the resulting risks by leaps and bounds.

Vulnerabilities in the implementation of the hardware, software and communications systems used, as well as the ones created during the operation of these systems, including the human factor, have created an environment that is ripe for exploits. The novelty factor of ICTs, with people struggling to adapt to them for their day-to-day activities, have prevented many people from paying attention to NIS concepts. Yet people and societies started integrating ICTs in the most critical aspects of their lives, without adequate risk assessments. This created further ground for exploits to occur. As the opportunity of financial gain from these exploits emerged, the area turned into a major field of activity. Exploits with classical motivations such as political gain or espionage have also increased.

3.1 The Threats

The SysSec consortium has been assessing the threats landscape since its inception with reports coming out in 2011 [1] and 2012 [2]. The consortium produced the Red Book: A Roadmap for Systems Security Research [3] during its third year of activities. In this compilation of emerging threats, grand challenges and the research roadmap to handle these threats, several domains are singled out. The Red Book presents these threats from not only technical and research perspectives but also from a personal and societal one to present what is at stake. Therefore, it is an excellent resource to understand the multi-faceted nature of cyber security risks. We will look at a few critical threat domains here and evaluate their impact from a social and regulatory perspective.

In the personal domain, loss of anonymity, authentication and authorization breaches, social network exploits and social engineering attacks can be listed, as well as the grand challenge of maintaining control over personal data. These threats undermine the identity and the integrity of individuals, and infringe on their personal rights and freedoms, in addition to the economic losses. When individuals are targeted by these attacks, their response cannot be predicted easily. Much like the response of a human being in danger in the physical world, the fight-or-flight-or-freeze principle [13] might also apply here. Some people will escape the sites and services that try to exploit them, some will fight them by taking legal action or seeking help from experts and some will do just nothing and carry on as before.

Exploits that revolve around identity and anonymity are of particular concern. Rule of law and the relationship between the state and the individual are defined in national and international law. Personal rights and freedoms are protected under these laws. As these notions are eroded not just by the threats but also by the countermeasures installed by the states to mitigate them, the individual might lose its strong position in the current social order and this might have profound effects in all aspects of life. This perspective could be a very strategic research area.

Threats to critical infrastructures may lead to very risky situations since these infrastructures support the stability of societies and countries. Although at the beginning, the critical infrastructures were exposed to the same general threats as in other domains, targeted attacks and APT's have changed this. There are specific threats in this domain now, such as the Stuxnet, Duqu and Flame infections [3]. Additionally, these infrastructures often employ legacy systems, thus, maintaining an acceptable level of security in these systems is a challenge. The human factor in creating vulnerabilities is a major concern as well. When critical infrastructures are connected to the Internet without adequate risk assessment and management procedures, major vulnerabilities emerge.

Governments are keen to regulate critical infrastructures more readily and incident reporting and handling are major parts of these strategies. Yet, there does not seem to be a consensus on how these regulations would be implemented. The private sector is a key part of the critical infrastructure operations and by its nature, it is not very keen on regulation and mandatory reporting of incidents, for example. These competing views create interesting research challenges once more.

The mobile domain, in the personal, societal or national scale deserves special mention. The SysSec consortium has produced a specific deliverable on the threats that target mobile systems [14]. The mobile domain has been a relatively protected environment, due to the business model of the operators and the organization of the operating systems and applications used on the devices. Yet, new threats emerge as the sophistication and the diversity of mobile devices increase. The dominant role mobile devices play in our lives also increases the risks. More of our activities are moving to the mobile domain every day and this creates opportunities for new exploits. Therefore, there should be more emphasis on research and strategy initiatives in the mobile sphere.

ENISA also produces periodic assessments of the threats landscape. The 2012 assessment was delivered in January 2012 [15] and a mid-year review of 2013 was just released in September 2013 [16]. Threats are classified and their evolution in years is traced in these assessments.

An interesting observation in the latest reports is the increase in targeted attacks and the decrease in spam. There is a shift from general exploits to more specific and targeted ones. As targeted attacks are custom made and sophisticated, their mitigation is quite difficult. These attacks play out at national and international levels and require major human and monetary resources. As such, they are unlikely to be produced by individual attackers and require a more coordinated and institutionalized organization of production. As these threats are specific, very often they might not gather the attention of the public at large. In such scenarios, raising awareness and creating countermeasures becomes a challenge. APT's have the potential to be used for national defence and security purposes either in an offensive or defensive manner, and brings us to the subject of countermeasures.

3.2 The Countermeasures: defensive and offensive.

The current world of cyber security is governed by the paradigm of asymmetrical threats [17]. The attackers are one step ahead of the defenders. To attack is easier than to defend since the defence surface is much larger. Therefore deploying countermeasures against cyber threats is a very challenging task. This is easily observed in the technical domain. In addition to its technical difficulties, countermeasures also raise concerns w.r.t. their legitimacy.

While it is relatively easy to brand cyber threats as legally and morally unacceptable, countermeasures are harder to categorize one way or the other. This is especially the case with offensive countermeasures and countermeasures that involve monitoring and surveillance. Countermeasures taken at a personal level do not often raise concerns, but as soon as institutional or state-level policies are enacted, many stakeholders raise concerns. OECD also acknowledges this in their report on the views of non-governmental organizations regarding national cyber security strategies [18]. NGO's are concerned that as soon as sovereignty considerations enter the domain, transparency would be reduced and the multistakeholder, inclusive nature of the debate might be lost. Additionally, openness might slowly disappear as a characteristics of an innovative Internet.

As stated above, the two cases when major concerns are raised about countermeasures are (i), when at national level monitoring and surveillance is used and (ii), when they are part of a set of defence capabilities that could be used in an offensive manner.

Monitoring and surveillance can be used to restrict the personal freedoms of users when not used in accordance with their intended purpose of analysing trends and detecting anomalies. News reports have been emerging on the examples of governmental intelligence and security departments collecting and processing data on individuals and populations in general, not always sanctioned by the law. Adequate regulation and legislation of these activities are needed. Research to enable anonymity and privacy under surveillance and monitoring also needs to be supported.

When countermeasures are used as defensive capabilities at the international level, the potential of their use as offensive tools emerges. Additionally, there is a market emerging where zero-day exploits are being turned into offensive tools for government use. At this point, international law and norms begin to apply, and there is currently much debate surrounding this issue [19]. These debates have only begun and they will be going on for some time.

Due to their novelty, many activities in cyber space raise questions of legality and ethics. For example, when an international team of defenders detect the source of a Botnet, how would a take-down of this site be handled, respecting both national and international laws? Or are offensive measures to mitigate such botnets legal and ethical [20]? This area is full of potential for research collaboration among technologists and social and legal experts.

4

National Cyber Security Strategies

A recent OECD publication on the comparative analysis of national cyber security strategies in ten OECD countries [21] indicates that cyber security has become a national policy priority and that the produced strategies are increasingly holistic: including economic, social, educational, legal, law-enforcement, technical, diplomatic, military and intelligence-related aspects. The report also recognizes the challenge of balancing the security priorities with those of an open Internet promoting innovation and growth.

The OECD review indicates that most strategies aim to increase coordination and the free flow of information, while preserving privacy and freedom of speech provisions. These strategies assign roles and responsibilities regarding cyber security. They encourage a multistakeholder approach to policy making and provisions for public-private partnerships in this domain. Most strategies include action plans, and the key pillars of these plans are the importance of research and development in this field as well as monitoring of key national infrastructures for cyber threats. The importance of the economic drivers for cyber security is recognized and a drive to create a cyber security industry sector is included. Yet, the possibility of security-related barriers to trade that could inhibit innovation and global deployment of effective security solutions is also mentioned.

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 remains a major challenge. OECD indicates that cyber security policy making is at an early stage and will take time to develop and take effect along the principles mentioned above. Therefore, the possibility of cyber incidents remains and governments are advised to take necessary countermeasures without stifling the open innovation culture of the Internet.

Comprehensive national cyber security strategies, policies and legislation are in the making. However, currently, they remain less advanced than the technical status quo to address the challenges. Additionally, these strategies need to cover not just the technical aspects of the issues, but also many societal challenges of great magnitude. As mentioned, there needs to be a solid Research and Development support for the development of these strategies and policies. The research and development efforts to support strategy and policy would need to enable a long term trial and test of policy components and give an idea about the impact of these policies on the society, businesses, individuals and international relations, among many others. Therefore, an interdisciplinary approach with a large number of stakeholders should be organized. International cooperation frameworks for such research are essential.

5

EU Cyber Security Strategy and Proposed Directive

On February 7, 2013 the European Commission published its new Cyber Security Strategy and an associated proposed directive on network and information security [22] to ensure a common level of cyber security across all countries of the European Union. EC 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.

Like many other governments worldwide, there is an expectation that the social norms and values that apply in the offline world would similarly be valid in the on-line world, like for example, individual rights and freedoms, rule of law and the right to privacy. In many countries, this leads to a tendency to make amendments to existing laws and regulations to extend their coverage on-line. Yet, this could be a short-term perspective to mitigate immediate threats and incidents. ICT's and the Internet, in the long term, are affecting social norms, organizations and processes. Therefore, a native approach to cyber law to regulate this space might provide a better solution to the challenges of cyber security and cyber crime. Protection of critical sectors such as finance, health, energy and transport is a recurring theme. The strategy also recognizes the importance of the private sector in running these sectors as well as the ICT infrastructure. Therefore, the private sector is seen as a key stakeholder in all cyber security strategy and policy initiatives.

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. These research efforts would benefit from not only covering the technological domain but also the societal domain. An interdisciplinary point of view would not only help sustain a long term viability but also influence the underlying strategies and policies. The associated proposal for a directive on NIS [12] 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. These observations are valid not just for Europe but globally as well. Much like the successful standardization efforts in the technical domain to operate networks and systems worldwide in a seamless way, the cyber security domain also requires such standard procedures and regulations to provide consistent protection worldwide. When the source or destination of a communication, operation or attack spans across multiple continents, anything less would be insufficient. Yet, the current state of cooperation in this area is far from this target.

Another key challenge for the proposed directive is the unwillingness of industry to accept mandatory incident reporting rules. Commercial interests and reputations could be at risk. The ICT world is an interdependent realm of many small elements providing service to the end users. When something fails, intentionally or unintentionally, it is difficult to determine the root cause of the fault. Overall, industry seems to have a tendency to lean towards a voluntary approach to incident reporting. However, many incidents would go unreported as a result.

This is just one of the challenges of trying to regulate such a multistakeholder space. Again, large scale prototypes and experiments where such regulatory policies could be tried and tested would provide enormous benefit to both the regulators and the industry as well as the users building confidence in the regulatory framework. Therefore, such research and experimental facilities need to be supported on a global scale.

6

The Research Framework

As indicated in the preceding sections, there is a need for research and experimentation to support the creation of new policies, legislation and countermeasures to meet the challenges of cyber security. The following elements are essential for successful research and innovation in this domain.

6.1 Interdisciplinary research

The field of cyber security is so convoluted that no single domain could cover it alone. Technical experts, social scientists, legal experts, law enforcement specialists, economists all have a role to play to grasp the complete picture. As they come together, they can have a better insight into the challenges of cyber security. They can explore not just the short term but also the long term implications. They can influence not only products and services but also strategies, policies and the future.

Many leading universities around the world have dedicated resources in their interdisciplinary research centers to the study and research of cyber security phenomena. Berkman Center for Internet and Society at Harvard University [5], Oxford Internet Institute [6], Stanford Center for Internet and Society [7], The Citizen Lab at the University of Toronto [8] and Tech and Law Center in Milano [9] are leading examples. Europe needs to invest more in supporting such interdisciplinary research centers to advance on topics at the intersection of technology and social sciences to inform policy and strategies as well as to support innovation.

6.2 Experimental Facilities for Policy Research

The Internet is a very widespread collection of diverse systems. More significantly, the Internet is used by a very large number of people with different aims and perspectives. Predicting how certain policies and strategies will play out in the future Internet is a major challenge. In the field of cyber security this is even more of a challenge because when systems are not used for their intended purpose but exploited through their vulnerabilities, the possibilities and combinations of outcomes becomes almost endless. Therefore, studying such systems is a daunting task.

Yet, this needs to be done, because misguided policies could cause great harm to the future success of the Internet as an open, inclusive and innovative domain. The creation of a framework of distributed, interconnected labs that can operate in cohesion could be explored as a solution. The Living Labs concept [23] could be a good starting point for this.

6.3 A Legal Framework for NIS Research and Innovation

Cyber security research often involves collecting data from networks and hosts, performing test attacks and experimenting with network configurations. Yet, this might not always be allowed. Although several anonymization techniques could be deployed to protect the privacy of users and organizations, there could still be liabilities. Researchers as well as users need to be protected. This would pave the way for more innovative countermeasures to be developed as well as more effective techniques to be developed and tried.

Due to the international character of the technologies and threats under investigation, it is often necessary to share data across borders. Yet, sharing such cyber security threat/incident information can be a legal challenge. The WOMBAT project [11] has produced several deliverables and workshop proceedings, sharing experiences in this field. If research is to succeed and researchers are not to be stopped in their tracks by legal concerns, then a framework needs to be drawn in this area. Like all other aspects of cyber security, this effort needs to be a multistakeholder endeavour as well, addressing the concerns of not just researchers but all the users, regulators and infrastructure operators as well. Holding international consultations on the governance of cyber security research could be a good starting point, followed by concrete steps towards a working system.

7 Conclusion

Concerns about NIS vulnerabilities and exploits are affecting the way individuals, societies and governments are using ICT's. While protective countermeasures are being used to improve NIS, there are also governmental efforts to regulate and to enforce policies in this space for long term effect. The amount of trust users place in ICT's affect their success and potential to bring about positive change in societies.

The number of stakeholders in the organization and regulation of the societal aspects of NIS is huge. Politics and perceptions have a role to play in policy making. Building consensus to create policies to induce trust in the Internet is therefore a challenging task. The evidence base to direct and support policies is relatively small and the outcome and effects of the policies are difficult to measure. Research and innovative approaches are needed to help with these challenges.

Open and inclusive processes and frameworks at national and international scale are needed to create and enforce effective policies in the NIS domain. A multi-stakeholder, interdisciplinary research field where technologists and social scientists come together needs to flourish to support lasting and constructive policies. Such research requires the support of the public and the private sectors. Real life scale experimental facilities and organizations to test out policies and to observe their long term outcomes are needed. A balance needs to be found between efforts to regulate and monitor cyber space for increasing security and to keep it a domain for continuous innovation and progress for the benefit of all.

Bibliography

[1] D. Balzarotti (Ed.), D4.1: First Report on Threats on the Future Internet and Research Roadmap, September 2011, Technical report, SysSeC Consortia.

[2] D. Balzarotti (Ed.), D4.2: Second Report on Threats on the Future Internet and Research Roadmap, September 2012, Technical report, SysSeC Consortia.

[3] E. Markatos, D. Balzarotti (Eds.), The Red Book: A Roadmap for Systems Security Research, August 2013, SysSeC Consortia.

[4] M. MacLuhan, Understanding Media: The Extensions of Man, 1964, New York, McGraw Hill.

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

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

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

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

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

[10] OECD-DSTI Working Party on Information Security and Privacy, Improving the Evidence Base for Information Security and Privacy Policies, OECD Report JT03320836, May, 2012.

[11] WOMBAT Project, Deliverable D6.4: Second Open Workshop Proceedings, May 2011, http://www.wombat-project.eu/ .

[12] 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.

[13] Fight-or-flight-or-freeze principle Wikipedia entry, http://en.wikipedia.org/wiki/Fight-or-flight-response .

[14] S. Ioannidis, et.al. (Eds.), D7.3: Advanced Report on Cyberattacks on Lightweight Devices, September 2013, SysSeC Consortia.

[15] L. Marinos and A. Sfakianakis, ENISA Threat Landscape, September 2012, Technical report.

[16] ENISA Threat Landscape, Mid-year 2013, September 2013, Technical report.

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

[18] OECD-DSTI Working Party on Information Security and Privacy, Non-Governmental Perspectives On a New Generation of National Cybersecurity Strategies, OECD Report JT03330865, November 2012.

[19] M.N. Schmitt, International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed, Harward International Law Journal, volume 54, December 2012.

[20] F. Leder, T. Werner and P. Martini, Proactive Botnet Countermeasures, An Offensive Approach, In Cooperative Cyber Defense Center of Excellence - CCDCOE, March 2009, Tallinn, Estonia.

[21] OECD-DSTI Working Party on Information Security and Privacy, Cyber Security Policy Making at a Turning Point, OECD Report JT03330862, November, 2012.

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

[23] European Network of Living Labs, ENOLL, http://www.openlivinglabs.eu/ .