European Internet Security Strategy

Report written by
Progress Consulting S.r.l. and The National and Kapodistrian University of Athens.
This report does not represent the official views of the Committee of the Regions.

More information on the European Union and the Committee of the Regions is available on the Internet at http://www.europa.eu and http://www.cor.europa.eu respectively.

Catalogue number: QG-02-13-240-EN-N
ISBN: 978-92-895-0734-9
DOI: 10.2863/84685

Contents

Summary

Cybersecurity has become an increasingly important aspect of public policy as internet traffic increases and mounting cyber-threats affect the operation of governments and businesses as well as the everyday life of citizens. Cybersecurity policy-making is at a turning point, becoming a national policy priority with explicit strategies in several countries. Even if sovereignty considerations have become increasingly important, there is evidence that the participation to international cooperation or policyframeworks is positively related to the cybersecurity performance of a country; additionally, cyber-threats are not confined by administrative borders as network and information systems are globally interconnected.

In February 2013, as part of the commitment to an ‘*open, safe and secure cyberspace’,*the EU Cybersecurity Strategy was published along a proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union. These latest initiatives complement and are consistent with existing ones related to electronic communications and data protection regulatory frameworks, as well as to the protection of European critical infrastructure.

While in some countries (e.g. the USA) the role of local governments in fostering internet security is clearly acknowledged and supported, at EU level there is a general appreciation of the need to promote a holistic effort by all stakeholders, including at the regional level, to ensure the security and resilience of ICT infrastructure.In fact, the complexity and volatility of cybersecurity make a distribution of roles among the different levels of authority rather difficult. In technical terms, standards need to be defined at national level or higher to ensure economies of scale and interoperability, but there is ample role for local and regional authorities (LRAs) to intervene in some key areas related to: the protection of e-Governance systems working through regional and/or local applications or platforms; real-time collection of data on cybercrime; and awareness and training initiatives for both civil servants and citizens.

Options for implementation by LRAs refer to four main domains: (i) establishing a risk assessment and management processto secure and constantly improve local/regional network and information systems; (ii) enforcing information security policy by means of obligations, sanctions as well as rights; (iii) increasing perception of cybersecurity issues and improving digital literacy and skills in terms of recognition and management of threats; and (iv) seeking support beyond the local/regional public administration to achieve economies of scale, effectiveness, piloting and/or dissemination.

Such options can be implemented through diverse interventions, depending on the different level of competencies of LRAs across Member States. Three broad hypotheses, not mutually exclusive, are outlinedfor better protection against cyber-attacks, faster promotion and implementation of internet security, and increased efficiency and use of e-Government by LRAs. These hypotheses include: (1) developing optimal arrangements for information availability;(2) focussing on factors accelerating cybersecurity, such as training, competence and awareness creation, reliance on external agents for the provision of security services, or access to mechanisms for piloting and/or disseminating; (3) systematically monitoring cybersecurity developments towards an internet security strategy or risk assessment & management process to allow an increased efficiency and use of e-Government as well as a better provision of services to citizens and businesses.

Several local and regional initiatives concerning cybersecurity were reviewed via bibliographical research; ten of these initiatives have been described in detail with a view to draw proposals for the promotion of internet security at the local and regional level.

There is an important role for LRAs to play in the area of internet security but this importance is not sufficiently reflected in the limited number and types of cybersecurity-related initiatives described within literature or on the web. An inadequate participation of LRAs to EU-funded cybersecurity projects was also noted, with partnerships mostly including academic, research and industry organisations. Thus, as a preliminary remark, the participation of LRAs to research and technology projects addressing internet security and privacy protection should be encouraged, with the double aim of improving cybersecurity at the local or regional level, and testingresearch outputs within real-life situations.

Better protection against cyber-attacks requires, in the first instance, LRAs to be aware of the need to articulate an effective central-local interaction mechanism, allowing access to external resources (e.g. cybersecurity research and development, tailored information, certified training) and experiences (e.g. cooperation). Formal approaches for information sharing on threats and vulnerabilities, as well as on modalities to mitigate and recover, seem to be the most effective as they facilitate the building of trust among participants.

In a rapidly changing cybersecurity landscape, awareness of threats by LRAs is not enough. They need to implement concrete actions to allow smarter and safer access to services to increasingly demanding citizens. Infrastructural solutions, common rules, standards and specifications need to be implemented.

Additionally, LRAs are expected to actively interact with citizens on cybersecurity issues, allowing, for example, end-users' reporting and feedback.

With regard to critical infrastructure, LRAs need to work on both awareness on cybersecurity needs and challenges, and preparedness. Information exchange platforms are crucial to the correct functioning of infrastructure and infrastructure services that rely on interconnected information systems.Thus, efforts may focus on establishing a risk assessment and management process also through the implementation of public-private partnerships with ICT companies.

LRAs are still below the level of the state of the art for much of known cyber-threats. This calls for a systematic and continuous focusing on factors that enhance online security.While the potential for intervention differs from one LRA to the other, training of both civil servants and citizens is a responsibility that needs to be enforced at the lowest possible level.Faster promotion and implementation of cybersecurity measures may be achieved by LRAs through tailored training and empowerment of end-users. Main proposals to be considered in this regard include: recognise that knowledge and behaviour of end-users is the first line of defence against cyber-threats; be aware that European collaboration in the awareness of the general public works and offers a cost-effective solution; coordinate, particularly in small countries,the efforts by diverse stakeholders under nation-wise structures, umbrella or nodes; encourage the private andacademic sectors to contribute to the development of specific cybersecurity know-how and competence, on the assumption that cyber-threats are a matter of concern also for research institutions and businesses (for example with regard to technology, innovation and intellectual property rights); introduce curricula on cybersecurity within schools; apply professional certification programmes or modern learning standards on cybersecurity to teachers; benefit from the multiplier effect provided by regularly training educators and by participating to national and/or international networks.

Focusing on known challenges is insufficient, due to the rapid technological development and increased activity for internet fraud. It is only through systematic monitoring and knowledge of the changes in the cybersecurity landscape that LRAs can ensure effective strategies of early warning, risk assessment and management, and, consequently foster increased efficiency and use of e-services. Proposals for a systematic monitoring of cybersecurity developments refer to the need to create, or access, the necessary intelligenceto guide appropriate decision-making with regard to cybersecurity matters, including results (processes, techniques) harvested from research; in regions where the business sector is strong and sensitised there is also room for establishing intelligence based on the cooperation with the private sector.

Part 1: Set of policy options/hypothesis

1.1 Introduction

Internet Security, known also as cybersecurity,has become an increasingly important aspect of public policy as internet traffic increases. Cybersecurity affects the operation of governmentsandbusinesses as well as the everyday life of those European citizens commonly using the internet. Mounting cyber-threats are not limited by borders. Network and information systems are,in fact, globally interconnected and '*network-based threats are continually increasing in breadth, volume, and sophistication and represent an existential risk to organizations around the globe'*[1]; hence, the need for an intervention at EU level, complemented by bilateral and multilateral international initiatives.

On March 2012, the Commission adopted a Communication on the establishment of a European Cybercrime Centre; a permanent Computer Emergency Response Team for EU institutions, agencies and bodies was set upinSeptember 2012.InFebruary 2013, as part of the commitment to an '*open, safe and secure cyberspace'*,theEU Cybersecurity Strategy was published along a proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union. These initiatives intend to complement and be consistent with the existing ones related to electronic communications and data protection regulatory frameworks, as well as to the protection of critical infrastructure[2].

Extensive research by OECD reveals that cybersecurity policy-making is at a turning point, becoming a national policy priority with explicit strategies. Even though a single definition of cybersecurity cannot be derived from these strategies, nevertheless all new strategies are becoming integrated and comprehensive, the key challenge being to pursue security '*while preserving the openness of the internet as a platform for innovation and new sources of growth*'. These strategies'*approach cybersecurity in a holistic manner, encompassing economic, social,educational, legal, law-enforcement, technical, diplomatic, military and intelligence-related aspects*'[3]. While '*sovereignty considerationshave become increasingly important*'[4], a recent research by MicrosoftCorporation shows that the cybersecurity performance of a country is positively related to its participation to international cooperation or policy

[1] Juniper Networks (2012)

[2] Framework Directive 2009/136/EC of 25 November 2009 concerning the processing of personal data and the protection of privacy in the electronic communications sector; Directive 2002/58 of 12 July 2002 on privacy and electronic communications; Directive 2008/114 of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

[3] OECD (2012)

[4] OECD (2012)

frameworks such as the London Action Plan or the Council of Europe Convention on Cybercrime[5].

1.2 Policy options for LRAs in cybersecurity

1.2.1 Aspects of involvement of the local and regional level

In a document studying the key objectives and concepts in cyberspace strategies, the OECD identifies an explicit reference to the local level only in the US strategy and Canadian individual activities[6] (Box 1).

Box 1: The US model
In the USA, local governments are expected to play a more active role than in the EU in facing risks connected to cyber dangers. Their role for internet security is, in fact, recognised as crucial and the U.S. Department of Homeland Security (DHS) has created the Multi State Information Sharing and Analysis Center (MS ISAC), a voluntary and collaborative organisation based on a strong partnership with the National Cyber Security Division within the DHS, to provide free services at all government levels. The Center's mission is to improve the overall cyber security posture of state, local, territorial and tribal governments(SLTT). It operates by collaboration and information sharing among members, private sector partners, and the DHS. It is designated as the key resource for cyber threat prevention, protection, response and recovery as well as situational awareness for the nation's SLTT. SLTT can become members at no cost as the Center, being acknowledged as serving national interests, is supported by the Federal Government. All USA States and many more governments at sub-national levelhave joined. MS ISAC provides to its members: advisories (incident response resources, cyber event notifications, daily cyber trips, network monitoring); information bulletins regarding the latest cyber-threats and vulnerabilities; a variety of educational, awareness, and training resources and opportunities; and services, some of which are made available to the public (e.g. cybersecurity webcasts, training and awareness videos and guides).
Source: MSISAC website

With regard to the EU, within Pillar III of the Digital Agenda, dedicated to Trust and Security, it is emphasized *'the need for all stakeholders to join forces in a holistic effort to ensure the security and resilience of ICT infrastructure, by focusing on prevention, preparedness and awareness, as well as to develop effective and coordinated security mechanisms*'[7].Additionally, in the general provisions, where the Digital Agenda stipulates for a sustained level of commitment at both EU and Member State level, it is mentioned explicitly that this is '*including at regional level'*[8]. A recent ENISA Report on cybersecurity recognises that cybercriminals can be organised on international,

[5] Kleiner A., Nicholas P., Sullivan K. (2013), Microsoft Corporation | Measuring the Impact of Policy on Global Cybersecurity
[6] OECD (2012), p. 21 and 49
[7] COM(2013) 48 final
[8] COM(2010) 245 final: Digital Agenda for Europe

national or even "local" level[9].

Technically, cybersecurity is a complex matter[10]; it also deals with several fast-evolving factors, from changing business needs, regulations and policies, to new technologies and computing infrastructure.The complexity and volatility of cybersecurity make a distribution of roles among the different levels of authority rather difficult. In technical terms, standards need to be defined at national level or higher to ensure economies of scale and interoperability, ascyber-attacks are becoming increasingly regional (supra-national) or international. However, there isample role for LRAs in the spirit of optimal design and subsidiarity. In particular, LRAs need to intervene in the following areas:

e-Governance protection: While e-Governance systems are often designed at the national level, regional/local applications and platforms exist and may or may not be connected to higher administrative levels; for example, health information systems may be connected through a national or regional network or be hospital-based (hospital information systems). However, the more developed a system in an LRA the higher the internet risk, i.e. the more attractive it is for attacks. Protection systems in terms of both hardware and software are then necessary at the LRA level. This includes the design and implementation of communication channels dedicated to address security events.

Real-time data collection: National and international systems are highly complex and the identification of fraud, successful or failed efforts to attack the system and other forms of cybercrime may take a long time. Conversely, at the local level the identification of bugs and attacks can be real-time. Collecting local data, transmitting it on time and aggregating it may prove crucial for preventing the generalisation of cyber-attacks and the correction of systemic bugs. In this regard, LRAs need to invest in communication to help protect data security, inICT unitsfor data flows handling, and in security operation centerslocated either internally or externally to the public administration.

Awareness and training: e-Government addresses all LRA functions, while the largest share of both the civil servants and users belong to a generation that is not used or trained to use such systems. In order to achieve the protection and data collection roles mentioned above,a new culture among public officials is needed, as well as the delivery of a wide spectrum of training, from teachingthegeneral users very simple protocols (the relevance of switching off

[9] ENISA (2013)

[10] Internet security can be described to address at least three types of threats (not exhaustive): cybercrime, including in particular illegal activities and attacks to e-infrastructure; identity theft for direct economic benefits, such as bank transfers (e.g. misappropriation of credit card data, electronic ID through phishing and pharming); theft of personal data for indirect benefits (used for marketing purposes, insurance or any personal reasons).

the system properly, control for viruses, etc.) totraining qualified operators (e.g. anti-hacking)and auditors, the latter to systematically assure the respect of security procedures and protocols.

According to a recent Eurobarometer survey, 71% of EU citizens access the internet. Internet users are usually concerned about cybersecurity, for example with regard to disclosing personal information online. Two thirds (66%) of the users '*agree that they are concerned that information is not kept secure by public authorities*', while 59% of the citizens '*do not feel very or at all well informed about the risks of cybercrime*'[11]. LRAs have a role to play also in promoting the recognition of cyber-threats, in defining and raising awareness of the digital rights of citizens, as well as in providing training and information to users (public officials and citizens) on a regular basis to cope with the rapid changes occurring in ICT in general, and in the information systems used by local and regional governments in particular.

1.2.2 Possible set of policy options for implementation at the local and regional level

The outlining of policy options has been guided by the results of a survey carried out in 2008 in three Scandinavian countries(Denmark, Norway and Sweden) on security awareness management in local governments (regions and municipalities)[12]. Although these countries are to be considered advanced in this regard and notwithstanding the fact that competencies are in these countriesgenerally decentralised in a wide range of sectors (from health care and hospital management to social services, public transport, regional planning and development), results shows that the role of LRAs is limited to certain aspects of internet security but that these aspects are crucial for the future and reliability of the whole web. This role can be combined into fouroptions for implementation:

Option 1- Establishing a risk assessment and management process

This option prioritises the internal processes of the local/regional public administration and the way to secure and constantly improve its own network and information systems.

[11] Special Eurobarometer 390 (2012)

[12] ENISA (2008)

In particular it includes:

- ⇨ Identifying critical business processes and information assets (systems and data) as well as concerned risks for their protection and use.

- ⇨ Creating frameworks for information security management (e.g. information security policy and guidelines, as well as an organisational structure for management).

- ⇨ Improving networks and systems.As risks emerge from the communication within and beyond the local systems, hence the improvement of the intranets and access to the wider community is also in need of permanent monitoring and upgrade.

- ⇨ Modernisation of software/hardware.

Option 2 – Enforcing information security policy

Policy enforcement is necessary both within (among employees) and outside (with respect to higher government levels) the public administration. As pointed out above, internet security is increasingly a national and international matter. Creating standards that prevent attacks or fraud is done within international agreements. In this case, LRAs cannot play an active role but need to adapt to new developments.

Thus, information security policy enforcement includes in particular:

- ⇨ Defining, within the public administration, obligations, sanctions as well as rights. Accountability is an important element of a system's success. To avoid confusion in case problems arise, clear rules have to be agreed and circulated in advanceto mitigate risks (reduce the damage and attribute responsibilities) in case they occur.

- ⇨ Ensuring systematic linkages to national and international security standards and platforms.After selection (Option 1), such standards need to be enforced within local systems.

Option 3 – Increasing perception of cybersecurity issues and improving digital literacy and skills

Continuous training is important for the success of local e-Government. Because of the rapid technological change and the continuous improvement of fraud techniques, all producers and users (actual and potential) of the system need to be trained and improve their knowledge as technology develops.

LRAs play an important role also in providing information and guidance to citizens to properly use systems and recognize threats.In particular, this option includes:

- ⇨ Recognition of cyber-threats. It is crucial when a threat emerges to identify it in real time, block its potential to proliferate and inform systems beyond the local level to avoid its spreading. It is also important to increase the public perception of cyber-threats to allow citizens to recognise problems, avoid them and implement safety measures.

- ⇨ Confidence with operating systems. Employees creating and maintaining the system need to be aware of its potential and vulnerabilities.Further, actual users of the system need training as they may be the victims of cyber-attacks and become the means to carry them further.

Option 4 - Seeking support beyond the local/regional public administration

When financial or human resources at the local or regional level are insufficient and/or a higher scale is necessary to achieve effective operations, cooperation beyond the public administration is necessary.

This may include:

- ⇨ The reliance on and/or creation of security operation centers serving more regions and hence allowingeconomies of scale.

- ⇨ The setting up of public and private partnerships to raise funding for mutual benefit in the case of externalisation of services that can be more economically and more effectively operated by the business sector.

- ⇨ Funding from national and EU sources with a view to pilot operations for system/network development, international learning, and good practices.

1.3 Hypotheses for better protection, faster promotion and increased efficiency

The above mentioned options can be implemented through diverse interventions depending on the different level of competencies of LRAs across Member States. Three broad hypotheses, not mutually exclusive, are outlinedfor better protection against cyber-attacks, faster promotion and implementation of internet security, and increased efficiency and use of e-Government by LRAs:

- *Hypothesis 1: Developing optimal arrangementsfor information availability.*

  Information availability plays an essential role in cyber-risk assessment by operators and it is also critical for improving the cybersecurity of other stakeholders[13]. Additionally, LRAs need to constantly liaise with national and international authorities/systems creating new security standards to better protect from new types of crimes and attacks. Hence, the need for effective communication tools and structures (e.g. platforms, forums) allowing: the sharing of information from the local/regional level to ICT/critical infrastructure operators and from ICT operators and national public authorities/bodies to LRAs; the general spreading of information on cyber-crimes and attacks to all stakeholders, including citizens; and the availability of information within the same network and information systems for their optimum functioning.

- *Hypothesis 2: Focussing on factors accelerating cybersecurity.*

  LRAs prioritise to focus on those factors enabling a faster uptake and implementation of new standards, improved networks and systems, modern software/hardware, etc. Examples of such factors include training for the creation of both cybersecurity competence and awareness; cooperation with external agents or companies for the development of systems through public procurement or to rely on SOCs not located within the LRA; and accessing national or EU funds to develop pilots to be further extended through a leverage effect.

[13] Bisogni F., S.Cavallini, S.Di Trocchio (2011)

- *Hypothesis 3: Systematically monitoring cybersecurity developments towards an internet security strategy or risk assessment & management process.*

  This implies intelligence gathering for local e-Government needsby LRAs to identify and permanently monitor the performance of their systems as well as the new developments in e-Government services delivery. Without such intelligence a region can be very vulnerable not only for its own systems but also as an entry point to wider cyber-attacks. Such intelligence allows increased efficiency and use of e-Government as well as better provision of services.

Part 2: Inventory

e-PRODAT: European Data Protection Best Practices in e-Government services	
Option 4 Hypothesis 3	*Creating an intelligence of local needs in the field of data protection while delivering e-Government services through EU project partnering and the identification of best practices and standards.*
Authorities involved	Data Protection Agency of the Community of Madrid, and City of Santa Cruz de Tenerife (ES); City of Bologna, and Abruzzo Region (IT); Region of Western Greece, and the Association of local Authorities of the Prefecture of Kavalas (EL)
Other project partners	Estonian Data Protection Inspectorate (EE); University King Juan Carlos (ES); University of Patras (EL)

Implementation period: February 2005 – January 2007

Financing: Total project budget: EUR 820.000 out of which EUR 515.000 provided by the INTERREG IIIC-South programme (ERDF).

Description: The project aimed at promoting knowledge and (best) experiences exchange between agencies and other public bodies for the protection of personal data used by Governments and public administrations for the provision of services, with a focus on e-Government. Key objectives were: knowledge/experience exchange on personal data protection between public bodies belonging to different European countries; creation of an internet based 'European e-Government data protection observatory' for the assessment of compliance with European laws and principles as well as citizen awareness raising; and identification of best practices to increase data protection standards in the public sector. Main project's outputs included : an 'Assessment on Data Protection and e-Government in European Regions and Cities'; an Internet-based European observatory of best practices along a preliminary list of such practices on e-Government and Data Protection; and a set of marketing products and initiatives including events, meetings, workshops, brochures, press releases, etc.

Target groups: European cities and regions and their administrations.

Implementation procedures: The project partnership was set up to include regional data protection authorities and regional bodies with previous successful experience in data protection in e-Government deployment processes. Project activities were structured around five components: management and coordination; assessment exercise; identification of best practices; production of publishing materials; and communication.

Difficulties encountered: Problems were faced in gathering the necessary data for the assessment exercise that led to the production of the report on 'Data Protection and e-Government Services in European cities and regions'.

Sustainability: Positive synergies and feedback mechanisms were created.Municipalities and regions participating to the projects gained expertise from partner research institutions through the deepening of the analysis of their own ‘case study’ and those of other cities or regional governments, with the chance to improve their own e-Government services; research institutions gained access to empirical evidence on e-Government services; and data protection authorities gained the possibility to improve data protection standards in the public sector by testing data protection principles and regulations with real experiences.

Evaluation: Within the ex-post evaluation of INTERREG III 2000-2006, e-PRODAT was considered a successful example of project focusing on information society and e-governance.

References: e-PRODAT website; e-PRODAT Report Book; Ex-Post Evaluation of INTERREG III 2000-2006 Final Report; INTERREG IIIC Five Years of Bringing Europe’s Regions Together, Report December 2007.

SERSCIS: Semantically enhanced resilient and secure critical infrastructure services	
Option 1 Hypotheses 1,2	*Developing a risk assessment and management process for critical infrastructure services through the permanent monitoring of performance of the interconnected information systems.*
Authority involved	*Autoridad Portuaria de Gijón*,Principado de Asturias (ES)
Other project partners	Center for Security Studies (EL), IT Innovation Centre (University of Southampton),QinetiQ (UK); Joanneum Research, Austro Control (AT)

Implementation period: October 2008–September 2011

Financing: Total cost of the project: EUR 3.101.100, with EC contribution of EUR 2.000.000 under the 7^{th}FP, sub-programme area ‘critical infrastructure protection’.

*Description:*The project was to support the use of interconnected ICT systems used to plan and manage operations in critical infrastructure by developing technologies that enable such information systems to (i) survive faults (arising, for example, from the impact of natural events), mismanagement (accidents) and malicious attacks; and (ii) allow ‘*dynamic adaptation to manage changing situations, and counter the risk amplification effect of interconnectedness*’, i.e. adapt ICT composition in response to events and support‘slow’ human-initiated management with automated and assisted management of ICT components and services.Proposed solutions respond to the need to manage dependability and interdependency; they‘*use semantic models of the critical infrastructure, including its ICT services, to identify faults and potential risks and to increase human awareness of them.*’In practice, the project approach is expected to produce greater awareness of risks and new risk management capabilities addressing interdependency and cascading threats.

Target groups: The Port of Gijón (PAG) and managers of critical infrastructure in general.

Implementation procedures: The project was developed around: system modellingaccounting for interdependency and other risks; system governance and orchestration;and decision support based on semantic system models to assist human operators and application services. Dynamic security and trust management to control threatpropagation between services were also conceived in the approach.

*Difficulties encountered:*No difficulties were reported.

Sustainability: PAG management and security services depend on its ICT & CCTV network. Although the project focussed on the analysis of airports security systems, the participation of PAG to the project implied the possibility to transfer the project technology to the ports sector on the assumption that principles of maritime traffic control are similar to those of air traffic control. Further, the SERCIS architecture and approach was included in the Port Management Training Programme jointly held by PAG and the Asturias Business School. Dissemination reliedon PAG membership to (i) the Port Safety and Security Group, a benchmarking group for technology and best practices transfer including the Spanish ports of Bilbao, Barcelona Valencia and Algeciras; and to (ii) the Port Safety and Security Working Group at ESPO, gathering some 100 main European ports.

Evaluation: The project approach was successfully validated in an information-intensive critical transport infrastructure using highly interconnected ICT networks, i.e. an Airport Collaborative Decision Making (A-CDM)scenario, where '*the failure or underperformance of any of the interlinked ICT systems may compromise the ability of airports to plan their use of resources to sustain high levels of air traffic, or to provide accurate aircraft movement forecasts to the wider European air traffic management systems*'.

References: SERSCIS website; CORDIS project website;Martin Hall-May M., Surridge M. (2010), Resilient Critical Infrastructure Management using Service Oriented Architecture; Puerto de Gijón website.

BEE SECURE: a common initiative for more information security	
Option 3 Hypotheses 1,2	*Awareness raising and training of citizens and public actors to promote a safer use of new ICTs, increase skills and perception on internet security.*
Authorities involved	Ministry of The Economy and Foreign Trade, Ministry of Education and Vocational Training, and Ministry of Family of the Grand Duchy of Luxembourg; *Service National de la Jeunesse*(SNJ); SMILE GIE - Security made in Lëtzebuerg, an economic interest group owned by the three above national ministries; two local government associations: SIGI (*Syndicat Intercommunal de Gestion Informatiqu*) and SYVICOL (*Syndicat des Villes et des Communes Luxembourgeoises*).
Other stakeholders	Associations, foundations, public administrations, law enforcement bodies, educational and research institutes, and private sector stakeholders.

__Implementation period__: November 2010 – on-going

__Financing__: Total project cost: EUR 710.000. EU contribution EUR 230.000 under the Safer Internet 2009 - 2013 programme.

__Description__: The project is aimed at promoting a positive use of information and communication technologies by educating people, creating a culture of security and establishing a technical view on ICT security through the use of several communication channels. BEE SECURE embraces a wide range of services, ranging from general support to very personal assistance, such as: yearly campaigns; awareness raising sessions and training courses targeting specific age groups (e.g. kids, teens, parents, teachers, adults); public events and contribution to local initiatives; offline tools distribution (e.g. flyers, brochures); help-lines to report illegal websites; web platform information sharing; international networking; research, monitoring and information security activities to identify new and relevant trends or threats. BEE SECURE is the Luxembourg node of the European Safer Internet Programme, which coordinates,among other activities, the Luxembourg celebration of Safer Internet Day and constitutes the umbrella label for all governmental information security awareness initiatives including CASES (Cyber Awareness Security Enhancement Structure) and LuSI (Luxembourg Safer Internet).

__Target groups__:European citizens, public and private associations, public administrations, small and medium enterprises.

__Implementation procedures__:The core of the initiative is powered by a symbiosis of SNJ and SMILE GIE, where the latter has strong ties to the information technology area, while SNJ background relates to the social aspects of the topic. An Advisory Board representing associations, public bodies and bodiesfromtheprivateindustry is regularly consulted to outline new topics, needs and initiatives.

Difficulties encountered:None reported.

Sustainability:The project's web platform is running and benefits from regular feedback on threat levels and vulnerabilities from CIRCL (Computer Incident Response Centre Luxembourg, the national CERT/CSIRT - Computer Emergency Response Team/Computer Security Incident Response Team – for Luxembourg). The Advisory Board is dynamically open to include new partnerships and is regularly consulted on emerging trends, national and local campaigns. The project is member of the InSafe (the European network of Awareness Centres promoting safe, responsible use of the internet and mobile devices to young people) and the INHOPE (the International Association of Internet Hotlines) networks.

Evaluation:In 2011, about 23.000 people attended the annual BEE SECURE "Safer Internet" campaign and from November 2010 to April 2012, around 68.000 offline tools (flyers, brochures) were distributed. During the same period, 1990 kids aged 5-11 years, 4.100 aged 12-16, and 40 aged 17+ were reached, as well as 280 parents, 500 teachers and 40 other types of adults; 811 reports on illegal websites were collected; and a total of 107 phone calls were received. SMILE GIE and SNJ continuously monitor the quality of services through regular evaluations. External evaluations were related to: (i) sessions held at schools in 2010/2011: the University of Luxembourg reported that teachers largely judged the training sessions as efficient; (ii) parent's information sessions: by means of an external survey ACORD International reported that 95% of the respondents labelled the usefulness of the sessions as "good" or "very good" while the clarity of the explanations was judged "good" or "very good" by 99% of them; (iii) coordination (including reaction time and organisational flexibility): the ACORD evaluation assessed the action as "excellent"according to the very positive judgment of more than half of the respondents.

References:BEE SECURE website; Safer Internet Centre (SIC) of Luxembourg, InSafe network; Insafe website; INHOPE website; Safer Internet Programme; BEE SECURE Final Project Report (2010-2012); ENISA Country Report – Luxembourg (2011).

e-GUARDIAN: Development and certification of skills for European Educators focused on Safe ICT and Cyber threat prevention	
Option 3 Hypothesis 2	*Targeting the recognition capacity of students through a certified improvement of the skills and knowledge of teachers and the introduction of international standards into national education systems.*
Authority involved	-
Other project stakeholders	Public institution Informaciniu technologiju institutas (LT), The Latvian Information Technology And Telecommunications Association (LV), Association “Langas į ateitį” (LT), Bremen University (DE),Association APTES (CH)

Implementation period: November 2010 - May 2012

Financing: Funded by European Commission, Lifelong Learning Leonardo da Vinci Transfer of Innovations programme. Total budget: EUR 214.942

*Description:*The aim of the project is to create an e-safety training and professional certification programme for educators in Lithuania, Latvia and Germany. The programme helps teacher to become more knowledgeable about internet threats and modalities to overcome these threats, so as to be capable to transfer this information to their students. Among the project outcomes are: syllabus, methodology guide, student’s guide, training programme, e-course, barometer tests and certification tests (i.e. automated evaluation tests). The syllabus relates to: basic knowledge on e-safety (including ‘be aware of cyber crime, online predators, financial scams and who to contact if discovered illegal data’); understand computer infection threats (viruses, Trojan horses, spyware, dishonest adware, etc.) and know when and how malicious software can get into computer system; privacy and data management; security tools and network security (for example, safety means of computer networks such as Firewall, Antivirus, Anti-spyware, Spam blocker, Password protection, Connection encryption – wireless; or be able to use standard OS integrated protection tools); minors and newcomers on the net; and social networks and safe usage of the internet.

Target groups: Parents, employees/trainers of educational institutions at primary or higher school wanting to protect children against potential internet dangers and unauthorised access to their computers.

*Implementation procedures:*There are 30 questions in the e-Guardian exam. An e-Guardian candidate must answer to at least 80% of the questions to achieve certification. The tests are conducted on an online test engine platform; questions are selected from the Automated Question and Test Base using a special randomization algorithm.

Difficulties encountered: None reported.

Sustainability: e-GUARDIAN is an ECDL Foundation Endorsed Programme, meaning that it is possible to be distributed as an international programme to the ECDL Foundation network of National Operators. The certification covers: online communication (including social networking sites, chat, and email); safeguarding of children from online sexual predators, cyberbullying and websites with adult content; protecting computers from malicious software and virus attacks; awareness of security issues when shopping online.

Evaluation: The product was successfully tested through pilot training in all partner countries. It is considered a modern learning standard to be introduced in EU education systems.

References: e-GUARDIAN website; Projects and Products Portal for Leonardo da Vinci; ECDL Foundation project's web page; Langas į ateitį PPT presentation.

STORK: Secure idenTity acrOss boRders linKed	
Options 2,4 Hypotheses 1,2	*Improving networks and systems, making easier for citizens and businesses a secure access to online public services by developing common rules and specifications for the mutual recognition of national electronic identity. Developing Europe-wide interoperable cross border platforms while relying on pilots to achievea leverage effect towards increased efficiency and security of the use of e-services.*
Authorities involved	Lombardia Region (IT), Service Public Federal Technologie de l'information et de la communication (BE)
Other project stakeholders	The project involves35 partners belonging to national and local authorities, non-profit organisations, private companies and academic bodies from 13 EU countries plus Iceland.

Implementation period:June 2008 - December 2011
Financing: Total project cost: 26 MEUR. EU contribution rate: 50%.Co-funded by the EU ICT Policy Support Programme under the Competitiveness and Innovation Framework Programme (CIP).
Description:The scope of this cross-border project is*'making access smarter'* by: (i) simplifying administrative formalities; (ii) enabling businesses, citizens and government employees to use their national electronic identities in any Member State; and (iii) providing them with secure online access to public e-Government services across borders, while fully respecting their privacy. Common specifications and rules for secure and mutual recognition of eID between participating countries were developed and tested through the implementation of six pilots. Security and privacy were serious concerns within the project and an effort was made to make identity theft extremely difficult and to develop *"circles of trust"* at a European scale through the promotion and implementation of robust and transparent technology, safer transactions, less frauds, better control over personal data and simplified procedures.
Target groups:European citizens, public administrations, private business sector. *Implementation procedures*: Project implementation was structured around seven working packages including: management; eID inventory, trust and application groups; eID and upcoming technologies; eID process flows; eID and common specifications; specification, definition, implementation, and evaluation of pilots; communication and sustainability. The six pilots were implemented over a 12-month period to test the proposed eID architecture and common specifications related to: 1) cross-border authentication platform for electronic services;2) safer chat;3) student mobility;4) electronic delivery;5) change of address;6) ECAS (European Commission Authentication Service)integration. Part of the project work was subcontracted to the private sector; other organisations and government authorities (municipal, regional,

national) participated in the pilot activities. The project was intended to cover the entire value chain '*by including both those who build the infrastructures for the services, as well as those who provide them in real life to the end users, the citizens*'.

Difficulties encountered:Various legal and organisational barriers to the widespread implementation of STORK were faced and handledthrough a dedicated *"STORK Sustainability Action"*.

Sustainability:Building on the results and success of STORK, a STORK 2.0 phase startedin April 2012. STORK 2.0 will run up to March 2015, with a total budget of EUR 18.655.151, co-funded by the ICT Policy Support Programme under the CIP with EUR 8.762.974. STORK 2.0 will be a step forward towards the creation of a single European electronic identification and authentication area.

Evaluation:The project successfully delivered: a set of common specifications; common quality assurance standards; common codes; six pilots,integrated into existing real live portal services of the underlying STORK interoperability platform and accessible by the end-users through their micro-sites linked to the STORK official site. In addition, an*"Industry Group"*, a *"Member State Reference group"* and a *"Community of Interest"* were set up as open forumsto keep industry stakeholders, governments, institutions and citizens informed onproject developments and to receive their feedback and comments. In 2011, a final evaluation assessed the success ofall pilots in reaching their objectives andinproving the technical applicability of the STORK infrastructural solution for cross border authentication. In November 2011, theproject was awardedthe EPSA (European Public Sector Award) 2011 Best Practice Certificate for Theme2: *"Opening Up the Public Sector Through Collaborative Governance"*and listed among other 58 Best Practice Certificate Recipients*"Assess Yourself and Learn from the Best"*.

References:STORK project website; STORK D6.6 Evaluation Report; STORK Pilots website; EPSA 2011 Best Practice Certificate Recipients; STORK 2.0 project website

JYVSECTEC - Jyväskylä Security Technology

Options3,4 Hypotheses 2,3	*Creating business development opportunities and mutual benefits in the field of cybersecurity (competence, services and products) through project-based partnering between the private and public sector.*
Authority involved	Jyväskylä Regional Development Company Jykes Ltd. (FI)
Other project partners	JAMK University of Applied Sciences(coordinator), Descom Oy, Relator Oy, Ajeco Oy, Cassidian Finland Oy.

Implementation period: September 2011–December2013

Financing: Financial support is provided by the Regional Council of Central Finland and the European Regional Development Fund.The cost estimate of the project is 2.4 MEUR.

*Description:*The project aims at developingcybersecurity solutions and a competence cluster in the Jyväskylä region to create operational preconditions for business development in the security industry. The project will produce cybersecurity monitoring, maintenance and simulation services, information security audit services, and tailored education services to improve both cybersecurity personnel knowledge and operational processes. The know-how gained within the project will be used ina Master Degree Programme of cybersecurity to be started in 2013.

Target groups: Regional businesses and public sector authorities

*Implementation procedures:*An operational collaboration model (Living Lab) is implemented for the production of development, testing, and education services to be used within the networkof security sector companies and other organisations in the Jyvaskyla area. Testing and simulation is within a ‘cybersecurity situation room’ to ensure that new process models and applications are developed on the basis of real-life situations.

Difficulties encountered: None reported.

Sustainability: Jyväskylä Regional Development Company Jykes Ltd. (FI) is owned by the four municipalitiesof the Jyväskylä Region, and namely: City of Jyväskylä, Laukaa, Muurame and Uurainen. The company is to provide advisory and development services to regional small and medium enterprises, as well as networking and internationalisation support. Its involvement in the project will ensure that research, development and innovation in the security sector are developed in collaboration with the public sector and in response to its needs.

Evaluation: Not available.

*References:*JAMK University of Applied Science project web page; JYVSECTEC project website; ICTAALTO Jyväskylä article.

EISAS Large-Scale Pilot: Collaborative Awareness Raising for EU Citizens & SMEs	
Option 3 Hypothesis 2	*Awareness raising initiative to increase perception and skills of citizens and SMEs about cybersecurity on the assumption that awareness of end- users is the first line of defence against cyber-threats.*
Authority involved	CESICAT, the agency responsible for promoting information and communications technologies security on behalf of the *Generalitat of Catalonia* (ES)
Other stakeholders	ENISA, European Network and Information Security Agency; DTAG, Deutsche Telekom AG (DE); NorSIS, Norwegian Centre for Information Security (NO); CERT, Computer Emergency Response Team Hungary, *Biztonsagosinternet* ["Safe Internet"] (HU); CERT Polska (PL); *Caixa, Caja de Ahorros y Pensiones de Barcelona* (ES)

Implementation period: 2012, within the framework of EISAS (European Information Sharing and Alert System) project (2006 – on-going).

Financing:Co-funded by the EU.

Description:The pilot aims at raising the level of cybersecurity awareness through collaborative and cross-border cooperation in security information. Building on the rationale that increased connectivitybrings increased cyber-threats both at home and at work, the initiative is to empower citizens with the knowledge and behaviour needed to fight these threats. Further, the initiative was intended to fill the knowledge gap across citizens belonging to different EU Member States (MS). The pilot focused on two main goals: (i) to foster collaboration and (ii) to promote sharing and distribution of good-practice information. Innovative awareness-raising material disseminated to citizens and SMEs within the pilot exercise mainly addressed the following issues: safe surfing and Botnets, phishing,identity theft and '*social engineering'* (i.e. the art of manipulating people into performing actions or divulging confidential information).

Target groups:Citizens and SMEs across Europe.

Implementation procedures:Following EISAS Feasibility Study (2007), EISAS Roadmap recommendation (2010), and EISAS Report on Implementation (2011), the need for a pilot specifically targeting SMEs and citizens was highlighted. The pilot project was structured around five work packages: monitoring the risks to identify cyber-threats most in need of awareness raising; producing or gathering awareness materials adapted to address attitudes and behaviour of citizens and SMEs; selecting awareness materials tailored for distribution and processing; converting awareness materials into a form suitable for distribution in the various MS; and monitoring dissemination and awareness-raising through appropriate communication channels such as social media, large public websites, and mailing lists.

Difficulties encountered:Technical constraints were faced in the uploading of complex material into existing websites. Difficulties were also faced in the design of advanced interactive e-learning material and in buildinga collaborative environment for the involvement of people from very diverse countries in terms of '*culture, time zones, local context, language, motivation, collaboration and technology readiness*'.

Sustainability: Building on lessons learnt from the EISAS Pilot initiative and following the creation of the FISHA (Framework for Information Sharing and Alerting)consortium, the Network for Information Sharing and Alerting (NISHA) project was launched in 2012 to respond tothe need, highlighted by the Pilot, to have an entity able to act as '*information broker*' and facilitator (i.e. connecting information providers and disseminators).

Evaluation:More than 1.500citizens (at home and at work) were reached in three countries (Spain, Hungary and Poland). Participating stakeholders and users considered the awareness material used in the pilot to be of high quality. The pilot went beyond awarenessraising as it also demonstrated that '*European collaboration in awareness raising works and offers a cost-effective solution to better prepare EU citizens facing ever-evolving cyber threats*'.

References:EISAS Large-Scale Pilot Report (2012); EISAS website; ENISA and EISAS website; EISAS Feasibility Study (2006-2007); EISAS Enhanced Roadmap (2010); EISAS Report on Implementation (2011); EISAS Basic Toolset (2011); NISHA project website.

SECURE CHANGE: Security Engineering for Lifelong Evolvable Systems	
Option 1 Hypothesis 3	*Establishing the way to secure and constantly improve networks and systemsby developing techniques and tools to modernise software andto ensurecompliance to evolving security and privacy requirements.*
Authorities involved	Public authorities are potential beneficiaries of the project.
Other project stakeholders	13 project partners from nineEU countries(ES, EL, IT, UK, DE, HU, FR, IE, AU) plus Norway, belonging tothe academic and industrial sector

Implementation period: 2009 – 2012

Financing:Total project cost: EUR 7.069.259, with EU contribution of EUR 5.100.000under the 7th FP, ICT - FET (Future and Emerging Technologies) Proactive Initiative: ICT forever yours (ICT-FY).

Description: The project aimed at developing methodology, processes, techniques and tools to make software lifecycle - fromrequirements engineering to design, testing, verification, re-configuration, up-dating, deployment and configuration - more efficient, flexible and secure to respond to the growing demand to continuously evolve and meet changing business needs, new regulations and policies, novel technologies and computing infrastructures.In other words, the main challenge of the project was "*to support evolution while maintaining security at all levels of the software development process*".

Target groups:European citizens, public and private sector.

Implementation procedures:The first year was dedicated to develop new models and processes addressing security assurance during software evolution. In the second year results were consolidated by focusing on specific industrial case studies; in the third, and last, year project's results were validated using real industrial scenarios in the domains of Air Traffic Management, Smart Cards Software Evolution, and Home Appliances.

Difficulties encountered:None reported.

Sustainability:Seventeen tools have been developed within the timeframe of the project, eightnew ones and nine pre-existing. Most of the tools are made available on the weband some are in the process of being adopted in the production process. Project partners have been very active in developing research prototypes and in providing feasibility analysis and practical validation of scientific results.Roughly, the project delivered 50 presentations, 11 tutorials and 11 invited talks; more than 100 project-related papers were published. Additionally, 8 courses and 8 lectures integrating SecureChange results were developed and 21 PhD theses were completed or are close to completion – all of which researching around SecureChange topics.

Evaluation: The promising results of the projectcontributed to the establishment of a spin-off company.

References:SecureChange website; SecureChange project information; SecureChange Cordis project page; SecureChange Final Publishable Summary (2012); Digital Agenda for EuropeNewsroom (15/08/2012).

ANIKETOS: Secure and Trustworthy Composite Services	
Option 1 Hypothesis 1	*Developing a platform forinteroperable service implementation, composition, adaptation and management in a secure environment according to standards and certification work.*
Authorities involved	Public authorities at the local and national level are explicitly considered among the beneficiaries of the project's outputs
Other project stakeholders	17 project partners from nine EU Member States plus Norway, belonging to the private and academic sector

Implementation period: August 2010 – January 2014

Financing: Total budget: 13.9 MEUR , EU funding: 9.6 MEUR under the 7th FP, strategic objective 'Secure, dependable and trusted infrastructures'

Description: The project is intended to '*establish and maintain trustworthiness and secure behaviour in a constantly changing service environment*' by: developing a platform for the creation and maintenance of methods and support tools for secure interoperable service implementation, composition, adaptation and management; defining the way to analyse, solve and share information on threats and vulnerabilities and modalities for these to be mitigated; contributing to the identification of best practices, standards and certification work (to be eventually included in European reference architectures); and evaluating within end-users trials (case studies) the use of the methods and tools outlined. The platform is intended as a tool for service developers, service providers and service consumers; it may be used for marketing purposes (e.g. e-business), within the industry sector (e.g. banking, tourism, ICT), or by the public sector at the central or local level for the provision of services to citizens. Additionally, socio-technical aspects will be considered within the project by developing a socio-technical security modelling language that '*captures security requirements at the organisational (business) level, and enables requirements analysts to represent and reason about security and trust properties that are fundamental for the design of secure and trustworthy service-oriented applications*'.

Target groups: Businesses, industry and public sector authorities

*Implementation procedures:*The project is structured around the following main components: architecture and requirements specification; prototype of trust management, security-by-contract and verification modules; prototype of secure service composition; prototype of the mechanisms for response to changes and threats: project platform integration; validation and evaluation. Further, three case studies dealing with air traffic management, future telecom services, and e-Governance (land buying) will be developed.

*Difficulties encountered:*Only technical concerns were highlighted in the 2012 validation and evaluation report.

Sustainability: -

Evaluation: An intermediate evaluation highlighted some problems related to the scalabilityand integration of modules and tools outlined so far within the project, while their usability and learnability were considered satisfactory. With regard to the platform, the main concern was on how the platform will support the composite service trustworthiness calculation.

*References:*ANIKETOS project brochure; Results of the first validation and evaluation of the Aniketos platform report (2012).

ECENTRE: England’s Cybercrime Centre of Excellence Network for Training Research and Education

Options2,3,4 Hypotheses 1,2	*Providing high-quality education, training and research in cybercrime. Improving cyber-threats recognition and the standardization of Cybercrime Forensics education. Developing central-local interaction platforms and networks for information availability and dissemination.*
Authority involved	Cheshire Constabulary (UK)
Other project stakeholders	17 partners, networked into five regional clusters bringing together law enforcementorganisations, universities and companies from all across England.

Implementation period:December 2012 – on-going (18 months)
Financing: Total project cost: over 1 MEUR.Co-funded with EUR 899.482 under the Programme Prevention of and Fight against Internet Crime (ISEC) INT (Illegal use of Internet)
Description:The project scope is to provide education initiatives and academically accredited training courses in cybercrime, together with high-quality research in forensic computing, law enforcement and commercial cybercrime security. Dissemination activities,raisingawareness and knowledge on cybercrime, in liaison withthe 2Centre EU-wide network, complement the project’s rationale. Main objectives are: establishing five regional clustersincluding law-enforcement, academia and commerce organisations; creating and delivering new teaching materials (case studies, presentation DVDs, software tools); enhancing the quality and applicability of training courses through a close cooperation with 2Centre; organising workshops and trainingto law enforcement practitioners; and becoming a body of reference in developing high-quality cybercrime forensics training and research.
Target groups:European citizens, academia, law enforcement bodies, private sector.
Implementation procedures:The project is implemented through 15 activities structured around four main domains: (1) ‘Training’ domain: Cybercrime Forensics Training; Cybercrime Master-Classes/Presentations. (2) ‘Research’ domain: Definition of Standard Templates; Creation and Management of ECENTRE Repository; ECENTRE Regional Groups Needs Analysis.(3) ‘Forensic Tools for cybercrime investigations’ domain: Cybercrime Forensic Tools. (4)‘Dissemination’ domain.
Difficulties encountered:None reported.
Sustainability:The project ismember of a growing European network (2Centre) of national centres of excellence sharing expertise, educational materials, research and best practice to fight cybercrime. The close collaboration between

ECENTRE and 2Centre builds a complementary synergy: ECENTRE is the suitable infrastructure for developing expertise, experience and good practice within England, while 2Centre provides the project with experiences of excellence all across Europe and disseminates results with an amplifier effect.

Evaluation: Not available.

References:ECENTRE project website; 2Centre Cybercrime Centres of Excellence Network – England; Cybercrime Centres of Excellence Network website; EC, DG Home Affairs projects database.

Part 3: Recommendations

There is an important role for LRAs to play in the area of internet security.However, difficulties were faced in identifying cybersecurity-related initiatives by European local and regional governments, also within the framework of EU-funded projects. In fact, most cybersecurity projects seem to be implemented by partnerships includingacademic, research and industry organisations. Although testing hypotheses within end-users trials or pilots appears to be a common practice, the opportunity to involve public administrations within research projects, and thus of testingresearch outputs within real-life situations, is often missed.

⇨ A preliminary suggestion is to encourage the participation of LRAs to research and technology projects addressing internet security and privacy protection, also considering the growing share of funds earmarked by the European Commission to these increasingly important issues that are directly related tocybersecurity policy-making[14].

The following proposals for the promotion of internet security at local and regional level are structured around the three main hypotheses outlined under section 1.3; reference to the initiatives described under Part 2 is also provided.

3.1 Proposals for developing optimal arrangements for information availability

LRAs, even the smallest and least internet-penetrated ones, need to be aware of their role and responsibility for cybersecurity,as a consequence of the interconnected nature of the internet. The latter implies that locally operating hardware and software, network and information systems represent,altogether,an entry point for destabilisation at both local and higher government levels. Accordingly, no LRA can afford neglecting its internet security. At the same time interconnection allows economies of scale deriving from standardisation, making cooperation and interaction crucial in terms of savings.

⇨ A recommendation for all LRAs is to be aware of the need to articulate the central-local interaction level by means of arrangements that allow the exploitation of opportunities to improve their protection level, as well

[14] *For the period 2007-2013, the European Commission has spent about €350 million in cyber security research; from 2013 to 2020, €400 million is earmarked to support key enabling & industrial technologies such as cyber security, privacy and trust technologies, and an additional €450 million is earmarked for 'Secure Societies' research which includes aspects of cybersecurity*' (European Commission MEMO/12/899).

asthe benefits arising from external resources (e.g. research and development, information, training) and experiences (e.g. cross-border cooperation). While LRAs in the USA are massively supported in this task by the Federal Government (Box 1) a similar system does not exist in Europe.

- Formal approaches for information sharing on threats and vulnerabilities, as well as on modalities to mitigate and recover, seem to be the most effective as they facilitate the building of trust among participants[15]. *ANIKETOS* shows how trustworthiness and secure behaviour are necessary components within a constantly changing service environment for interoperable service implementationin a safe modality, whether it is related to business, industry or e-Government. *ECENTRE*, on the other hand, is a concrete example of development of central-local interaction platforms and networks for information availability and dissemination on a specific topic (cybercrime).

- Further to the development of Europe-wide interoperable cross-border platforms and the increasing expectations by citizens to benefit from online public services, LRAs need not only to be aware of threats but also to practically allow smarter and safer access to services by citizens and businesses. *STORK* focuses on one of the key aspects of security, i.e. identity theft and safe treatment of personal data, demonstrating how collaborative governance is possible through appropriate infrastructural solutions, common rules, standards and specifications co-developed at different hierarchical levels (i.e. common codes and specifications become the elements around which the central-local interaction is articulated).

- Reporting and feedback by citizens and other e-services end-users is crucial for ICT operators. LRAs, most of which have nowadays a website online, may consider opening direct communication channels ontheir sites, for example by using social networks or internet-based help-lines. *BEE SECURE*relies on several solutionsto communicate and actively interact with citizens.

- LRAs need to pay particular attention to awareness on cybersecurity needs and challenges of the critical infrastructure they own or for which they share management responsibility. A recent report by ENISA on cybersecurity aspects in the maritime sector, underlines how low awareness and preparedness regarding cyber-risksare indeed concrete

[15] Bisogni F., Cavallini S., Di Trocchio S. (2011)

problems[16]. From a different perspective, information exchange platforms are crucial to the correct functioning of infrastructure and infrastructure services that rely on interconnected information systems. *SERSCIS*provides a good example of the type of risk assessment and management process that should be pointed to by LRAs, also through the implementation of public-private partnerships with ICT companies.

3.2 Proposals for focussing on factors accelerating cybersecurity

LRAs are still below the level of the state of the art for much of known cyber-threats. This calls for a systematic and continuous focusing on factors that enhance online security. Prevention and fight against attacks need to be incorporated into regional and local systems and be constantly upgraded.However, continuous training of human resources and increase of perception of threats and solutions are the most crucial elements that may accelerate cybersecurity,with external funding opportunities that can be tapped into to widen the impact.

While the potential for intervention differs from one LRA to the other, depending on its level of internet use, size and technological maturity, training of both civil servants and citizens is a responsibility that needs to be enforced at the lowest possible level. In fact, it is within this area of intervention that most of the initiatives presented under Part 2 were found. According to these initiatives, faster promotion and implementation of cybersecurity measures may be achieved by LRAs through tailored training and empowerment of end-users. In particular:

⇨ *EISAS* pilot clearly outlined that knowledge and behaviour of end-users is the first line of defence against cyber-threats and that European collaboration in the awareness of the general public works and offers a cost-effective solution. In this sense, LRAs need to be proactive in identifying and publicizing externally- (e.g. by the EU) funded large initiatives to take locally and regionally advantage of their leverage effect. Alternatively, especially within small countries, LRAs need to coordinate their efforts and input into nation-wise structures, umbrella or nodes as articulated by the *BEE SECURE* project in Luxembourg. Importantly, the project highlighted the need to consider both IT and social aspects while educating people, paying also attention to develop both general and tailored assistance to target specific age groups.

[16]ENISA (2011)

⇨ Considering that cyber-threats are a matter of concern not only for governmental authorities but also for research institutions and businesses (for example with regard to technology, innovation and intellectual property rights), there is scope for LRAs to encourage the private andacademic sectors to contribute to the development of specific know-how and competence. An example of such collaborative effort is represented by the *JYVSECTEC* project where a competence cluster is developed to improve both cybersecurity personnel knowledge and operational processes. *ECENTRE* provides another example of development of high-quality education, training and research in cybercrime jointly tackled by law enforcement organisations, universities and companies.

⇨ LRAs, especially in those countries where they are charged with educational responsibility, have an important role to play in introducing curricula on cybersecurity within schools. Alternatively, *E-GUARDIAN*demonstrates that the cyber-threats recognition capacity of students may be targeted through the enhancement of the skills and knowledge of teachers. In both cases, LRAs have the opportunity to identify on the marketprofessional certification programmes or modern learning standards on cybersecurity and to consider their introduction into local and regional education systems or curricula.

⇨ Dealing with the continuous changing world of new technologies requires that new skills against cyber-threats spread rapidly in the society. Multiplier effects towards the creation of a culture of cybersecurity may be achieved by investing at the local level on teachers and educators (for example with continuous training or refreshing courses) or by participating to national or international information sharing networks, as shown by the *BEE SECURE* and *ECENTRE* initiatives.

3.3 Proposals for a systematic monitoring of cybersecurity developments

Focusing on known challenges is insufficient, due to the rapid technological development and increased activity for internet fraud. It is only through systematic monitoring and knowledge of the changes in the cybersecurity landscape that LRAs can ensure effective strategies of early warning, risk assessment and management, and, consequently foster increased efficiency and use of e-services.

- ⇨ LRAs, in particular in smaller regions, do not always have the resources to create their own policies and guidelines for information security management but need to be informed, to monitor changes in national and international contexts, and to make selections. This implies decisions that may lead to lock-ins and thus need to be taken with the best possible knowledge on available alternatives. *E-PRODAT* provides an example of an internet-based observatory helping in the assessment of compliance with European laws and principles related to data protection thus providing the necessary intelligence to guide decision-making.

- ⇨ Risk management relies on research findings in order to cope with changes and support evolution while maintaining security. In practical terms, LRAs need specific techniques and tools to make risk management effective.*SECURE CHANGE* shows how these requirements can be met by academic &industry research jointly developing processes, techniques and tools to make software lifecycle more efficient, flexible and secure to respond to continuously evolving business needs, new regulations and policies, novel technologies and computing infrastructures.*SERSCIS* focuses on resilient and secure critical infrastructure services relying on highly interconnected network and information systems further to faults, mismanagement or malicious attacks.

- ⇨ In regions where business development is delegated to local or regional authorities and where the business sector is strong and sensitised there is room for establishing intelligence based on the cooperation with the private sector. The *JYVSECTEC* project provides an example of such cooperation within the framework of a project-based partnership whose main scope is to develop a cybersecurity competence cluster in the Jyväskylä region to create operational preconditions for business development in the security industry.

References

Bisogni F., Cavallini S., Di TrocchioS. (2011), Cybersecurity at European Level: The Role of Information Availability. COMMUNICATIONS & STRATEGIES, 81, 1st Q. 2011, p. 105.

COM(2013) 48 final: Proposal for a Directive of the European Parliament and the Council concerning measures to ensure a high common level of network and information security across the Union.

COM(2010)245 final: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Agenda for Europe.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

CouncilDirective 2008/114 of 8 December 2008on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

Directive 2009/136/ECof the European Parliament and of the Council of 25 November 2009, amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

ENISA (2011), Analysis of Cyber Security Aspects in the Maritime Sector

ENISA (2008), Security Awareness Management in Local Governments: Approaches in Scandinavia.

ENISA (2013), Threat Landscape, Responding to the Evolving Threat Environment.

Jupiter Networks (2012), White Paper, The evolving ThreatLandscape: Where the Key security Battles are Taking place Today - and essential strategies for Winning Them.

Kleiner A., Nicholas P., Sullivan K. (2013), Linking Cybersecurity Policy and Performance,Microsoft Trustworthy Computing. Microsoft Corporation | Measuring the Impact of Policy on Global Cybersecurity.

OECD (2012), 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.

Special Eurobarometer 390(2012), CYBER SECURITY, Conducted by TNS Opinion & Social at the request ofthe European Commission,Directorate-General Home Affairs, July 2012.