Cybersecurity at European Level: The Role of Information Availability

Fabio BISOGNI, Simona CAVALLINI, Sara DI TROCCHIO
Fondazione FORMIT, Rome, Italy

Abstract: This paper aims to analyse the cybersecurity issue, taking into account the investment behaviour of operators managing ICT infrastructures and providing ICT services and trying to investigate which kind of actions must be implemented to increase their security level. The main finding is that information availability plays a key role in the cyber-risk assessment for ICT operators and is also critical for improving the cybersecurity behaviour of other ICT stakeholders. From the ICT operator perspective, lack of information affects the real perception of cyber-threat occurrence, the vulnerability of his system and the potential loss in case of cyber-attack. As ICT systems have to be regarded as a network of different actor categories, regulation efforts at the European level should focus on spreading information among all ICT stakeholders in order to reduce failures of the cybersecurity market. Virtuous behaviour of other ICT stakeholders may increase the level of cybersecurity also by reducing the current lack of information on cyber-attacks of ICT operators and pushing their investments.

Key words: cybersecurity, information lacking, risk assessment, investment behaviour, European cybersecurity policy.

The first years of the 21st century have been characterized by the appearance of brand new threats in the most developed western economies. Terrorist attacks such as those of New York 2001, Madrid 2004, London 2005, Mumbai 2006 and 2008 have illustrated the relevance of the issue of infrastructure security and citizens' safety [1]. In addition, the development of information and communication technologies (ICT) and their pervasiveness in everyday life have created new opportunities for malicious attacks with huge potential impact on social and economic services. The diffusion of computers among citizens throughout the globe and the

[1] Although security and safety are often used as synonymous, in this paper safety is strictly related to assets (such as infrastructures managed by operators) and their components (such as computer servers). Safety is intended as the preservation of health. Impacts of a terroristic attack in terms of security can be measured in economic losses and public effects, impacts in terms of safety through casualties. For a review of the different security and safety definitions see CAMBACÉDÈS & CHAUDET (2010).

automation of productive services have created a world-wide network in which all kinds of users operate. On the one side, a complex set of interconnected networks allows real-time data exchange thus increasing the efficiency of communications, but, on the other side, it increases the risk of accessibility to confidential information and to critical systems able to control physical assets. In particular, the importance and the need to protect information infrastructures have largely increased in the political debate of global security over the last decade. Because most critical infrastructure services rely on ICT systems remotely accessible via public networks that are vulnerable to cyber-attacks, the potential damages in terms of economic effects, public effects and casualties [2] may be amplified at the societal level.

The case of Stuxnet, a Windows-specific computer worm discovered in June 2010 able to spy and reprogram ICT systems of critical industrial infrastructure, shows that industrial processes controlled and monitored through Supervisory Control And Data Acquisition (SCADA) computer systems are affected by vulnerabilities that can be exploited. The specific targets of this particular cyber-attack were nuclear facilities in Natanz and the Bushehr Nuclear Power Plants in Iran, showing a narrow distance between virtual effects and potential physical damages (KEIZER, 2010). To this purpose, the necessity for prevention of and protection against cyber-crime has arisen once remotely-managed control systems have become a clear target for malicious attackers. The growing awareness about global cyber-threats has increased the need for accurate information about their features, ICT infrastructures vulnerabilities, cyber-risk management approaches and socio-economic effects of successful cyber-attacks.

The current European policy debate and the most advanced studies [3] on the economics of cybersecurity have recently included the issue of responsibilities of protection and the attribution of the associated costs (KOLFAL *et al*., 2010). To this aim, different actor categories with specific roles in cybersecurity can be identified: citizens, public bodies/authorities,

---

[2] Within the framework of the European Programme for Critical Infrastructure Protection (EPCIP), the Council Directive on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection qualifies which kind of impacts should be investigated. The policy focus is on economic effects (e.g. economic loss, degradation of services) and social effects (e.g. potential number of fatalities, disruption of daily life, loss of public services).

[3] For example, the study for the "Development of a Methodology and Research of Quantitative Data on the Economics of Security and Resilience in Critical Communications and Information Infrastructures – CIIS", (CAVALLINI *et al*., 2010) carried out for the DG Information Society and Media of the European Commission.

ICT operators, operators of other critical infrastructures. Citizens, intended as general private end-users, carry the social interest in using ICT infrastructures and services provided by other critical infrastructures. In the event of a cyber-attack on the mentioned infrastructures, the society, as the aggregation of all citizens, would suffer larger negative externalities since it has less direct capacity to contain cyber-crime effects. Public bodies and authorities have the main goal to protect the social interest and can directly support prevention, protection and reaction to cyber-attacks through regulation (top-down approach) [4] or action (bottom-up approach) [5] that encourage all stakeholders to bear part of the cybersecurity costs. ICT operators, intended as operators who directly manage Internet connections (such as Internet Service Providers and telecom operators), are directly involved in the cybersecurity issues and considered the most liable actors. Due to the fact that they manage ICT infrastructures and connected services, in the case of a successful cyber-attack, they would suffer the most direct consequences, but wide damages would also affect the rest of society. Operators of other critical infrastructures in the cybersecurity framework have a double damage-spreading role that has recently increased their responsibilities. On the one hand, if an operator of a critical infrastructure affecting ICT operators (e.g. an electricity provider) becomes a cyber-crime target, its failure may cause a large disruption of ICT services. On the other hand, if an ICT operator suffers a cyber-attack cascading effects on other critical infrastructures (e.g. hospitals) might be spread to the entire society with relevant impacts for non-ICT users.

This paper faces the issue of the relationship between security investments and costs suffered as consequence of cyber-attacks. Starting from the analysis of the cybersecurity investment behaviour of ICT operators, the paper aims at proposing effective actions to public decision makers able to overpass potential market failures related to the security market of the cyber-world. The proposed model concerns the lack of information that characterizes ICT operators' investments in cybersecurity and provides indication on policy actions that may improve the cybersecurity level involving all the identified actor categories.

---

[4] An important aspect of the governments' response to cyber-crime is the development of laws and rules focused on the improvement of security provisions, the readiness in dealing with catastrophic incidents and the capacity to assure prompt recovery after incidents.

[5] A bottom-up approach relies on the initiative of each single actor to protect himself from cyber-attack effects. Governments can indirectly support this process, defining and setting up a clear liability framework and assigning negative externality costs to the specific categories of involved actors.

The next Section describes the economic framework of cybersecurity and how ICT operators would behave in terms of optimal investment behaviour with complete information on cyber-attacks. The following Section depicts the effective investment behaviour of ICT operators who assess cyber-risk with a lack of information. The Section after briefly summarizes the current institutional and regulation framework at the European level for increasing the availability of cybercrime-related information and provides suggestions to European policy makers on how cybersecurity could be increased not only directly involving the ICT operators. The concluding remarks summarize the main findings and suggest new investigation areas for the economics of cybersecurity.

■ The theoretical framework: the optimal level of cybersecurity

In recent years, with the spreading of information and communication services and the emergence of related threats and vulnerabilities, cybersecurity has evolved from a valuable economic good to a societal need. Business users, public authorities and citizens demand secure information systems, and ICT operators have set up investment strategies in order to provide ICT services at a suitable level of security. In the theoretical framework, the societal demand of cybersecurity provides an indication to ICT operators of their costs in terms of losses related to the lack of security and, consequently, the needed amount of investment. For an ICT operator, the optimal level of investment in cybersecurity is the level providing a protection that minimizes its expected costs in case of cyber attack events. This optimal solution occurs when marginal security investments equal the expected marginal costs that the operator would sustain. Nevertheless, market failures may impede the pursuit of the optimal level of investments and the consequent optimal level of security (BRUCK *et al*., 2006,).

Approaching a similar issue, GORDON & LOEB (2002) defined a model to determine the optimal amount of investment needed to protect a given set of information. Considering the vulnerability of an information system, the main finding is a biased behavior on the part of the operator: a firm spends only a small fraction (approximately 37%) of the potential loss that would result in case of a breach occurrence. According to this model, the level of cybersecurity investment of the ICT operator can be defined on the basis of the expected loss *E(L)* associated with its available information set, with *L*

representing the incurred loss in case of cyber-attack. The expected loss *E(L)* is the result of the probability of the threat occurrence, *t*, times the vulnerability of the system, *v* (which is the probability of threat effectiveness), and the potential loss due to the threat realization, λ [6]. In order to avoid huge unexpected losses, the ICT operator sets up a level of security *S* as a function of the implemented security investments I_s and of the level of vulnerability of the system *v*.

To illustrate the investment choice of Gordon and Loeb's model, the relationship between of the optimal investment choice of the ICT operator and loss can be drawn (Figure 1) with the level of investment in security I_s on the x-axis and with the expected loss *E(L)* on the y-axis. As common sense suggests, a lower level of investment corresponds to a higher expected loss in case of cyber-attacks and vice-versa. The ICT operator chooses the level of cybersecurity investment according to his risk attitude and his risk assessment. In fact, the level of chosen investment depends on the operator's risk propensity: if the operator is risk adverse, he would prefer a lower level of expected loss increasing current costs; otherwise, if the ICT operator is risk loving, he would accept a high risk situation increasing of current benefits (e.g. reduced security costs).

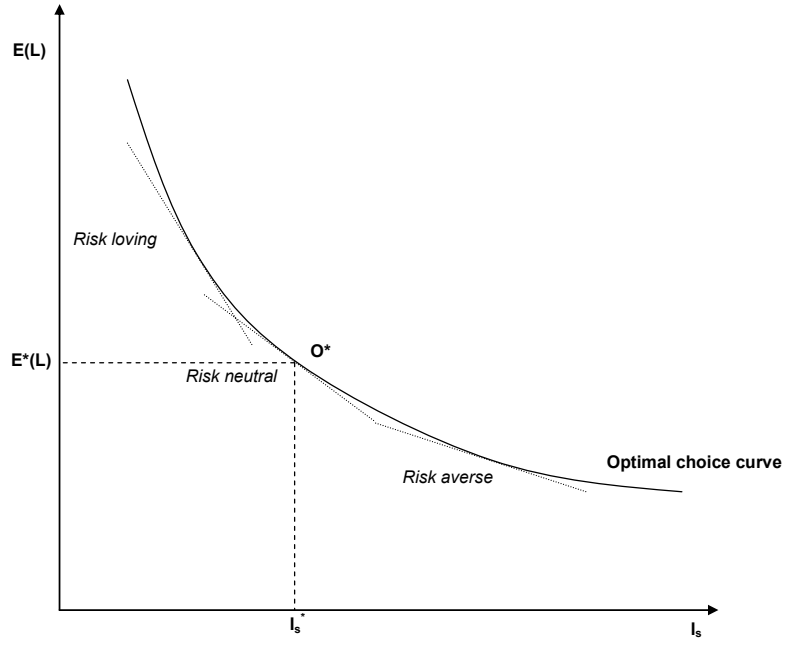
The assumption adopted in this paper is the risk neutrality of the operator [7]. Risk neutrality implies that the value of the level of cybersecurity investment is equal to the value of the expected loss, so that the optimal investment level chosen by the operator is represented by the intersection point between the optimal choice curve and the tangent representing the risk attitude of the agents. In Figure 1, the intersection point is *O**, the optimal cybersecurity choice, with a level of implemented investment I^*_s and consequent expected costs *E(L)** for cyber attacks.

---

[6] The random effect of the exogenous factors affecting the model structure could be addressed inserting an uncertainty variable into the model. The most likely uncertainty factors would be the probability of threat realization t and the potential loss λ. Both of them affect the expected value of loss due to the lack of information randomly affecting the ICT network actors. Assuming that the uncertainty variable would be inserted in the form of white noise, with zero average value independent and identically distributed, (which implies no autocorrelation), expected value of this uncertainty would not affect the final outcome of the model. For reference, see GREENE (2007).

[7] An agent is risk neutral when he/she is indifferent to sustaining current expenses in order to implement cybersecurity provisions or to bear the same expected expenses in the future to recover the losses caused by a cyber-attack. The idea of the risk aversion/propensity could be linked to inter-temporal choice, but it is crucial to consider the presence of a choice between certain and uncertain choice and not only between current options and future option. For reference, see KREPS (1991) and MAS-COLELL *et al*. (1995).

Figure 1 – The optimal level of investment in cybersecurity



■ The optimal cybersecurity choice with lack of information

The described optimal choice in the cybersecurity framework relies on the assumption that the ICT operator possesses complete information on cyber-crime effects and makes a proper assessment of cyber-attack risk. In fact, the expected loss and the following investment choice are defined as the result of the proper estimation of the probability of threat occurrence (t), of effectiveness in breaching the information system (v) and economic consequences of their impact (λ).

In the real world, complete information on cyber-attacks and related risk is not available to ICT operators, first of all, because cyber-attack techniques evolve rapidly and are becoming increasingly sophisticated. In addition, ICT operators targeted by cyber-attacks are reluctant to publicly communicate and report to the authorities any disruption in services, the causes, frequencies and costs. This operator behavior can be ascribed to the concern of suffering reputational damages, breaking confidentiality

obligations and being addressed on grounds of liability. Moreover, the particular sensitivity of information on cybersecurity incidents makes information sharing a particularly risky issue, hindering the development of a confident and fruitful environment [8]. In fact, from the perspective of a single operator, there are no immediate advantages in sharing information on past attacks [9], although all ICT operators and other critical infrastructure community members would gain from better information on cyber-attack framework.

The reluctance to share information about cyber-attacks experienced entails a biased knowledge on cyber-risk, leading to an under-estimation of cyber-attack probability and impacts. These circumstances influence the extent of implemented security provisions and the realized security investment: because ICT operators are not properly aware of the real extent of cyber-risk, the chosen level of investment is lower than that which would be desired by the operator himself.

These assumptions are supported by the results of a leading study on information sharing by GAL-OR & GHOSE (2004). The analysis made in the article "The Economic Consequences of Sharing Security Information" investigates the competitive implications of information sharing on breaches and the level of investment dedicated to security. The main conclusion is that market characteristics affect incentives for information sharing among competing firms, but information sharing encourages additional security investments.

---

[8] In this work the antitrust concerns related to information sharing are not discussed. However, speaking about information sharing, juridical criticalities that can arise in most of the western countries have to be mentioned. Due to confidential information flows among firms operating in the same market competitive issues may arise. For example, art. 101 and 102 of the Maastricht Treaty (respectively ex art 81 and 82 of the treaty establishing the European Union, generally known as the Treaty of Rome) pursue the goal of ensuring a competitive environment in the European union's markets prohibited "all agreements between undertakings, decisions by associations of undertakings and concerted practices which may affect trade between Member States and which have as their object or effect the prevention, restriction or distortion of competition within the internal market". Information sharing, characterized by restricted disclosure of sensitive information, could be misinterpreted by an enforcement agency or used to hide the flow of information for anticompetitive purposes.
For a general overview of the antitrust issue in information sharing, among the main reference works there are "Information Exchanges Among Firms and their Impact on Competition" by KÜHN & VIVES, "Overcoming impediments to information sharing" by AVIRAM & TOR and "Information sharing, innovation, Antitrust" by TEECE.

[9] In the perspective of the operator, the immediate advantages of sharing information are not enough to overcome the potential risk of reputation loss coming from breaches or improper disclosure.

In cybersecurity management, availability of information guarantees proper risk-assessment essential for an efficient protection strategy. For the single ICT operator, any security investment choice depends on the evaluation of the balance between potential costs due to disruptions and benefits arising from a proper risk evaluation as a result of the assessment of threat probability, of its vulnerability and of potential threat damage. Limited information on cyber-attack potential damages may lead to underestimate the effective risk lowering desired investments. In addition, a large amount of literature, starting from the seminal contribution of DIXIT & PINDYCK (1994), regards the uncertainty of market conditions (for example, the probability of occurrence of threats) as a costly condition in case of investments. An ICT operator investing in security in a specific moment loses the possibility to wait for better market conditions, thus bearing higher costs. Empirical studies highlighted that there are situations where such costs are very high and particularly affected by the market uncertainty degree, leading to a remarkable security underinvestment compared to the theoretically optimal level [10].

The effect of lack of the adequate operator's awareness on cyber-risk is represented in Figure 2 with the *perceived* optimal choice curve under the optimal choice curve. The threat probability and the cyber-attack impact, which contribute to the shape of the optimal choice curve, are biased by the absence of a proper level of information and are perceived by the operator equal to $t^p<t^*$ and $\lambda^p<\lambda^*$ [11]. Assuming the ICT operator risk neutral, the resulting optimal level of investment (I^{**}_s) is lower than the previous (I^{*}_s) implying an expected cost $E^{**}(L)$ according to the operator's perception. Considering the real level of threat probability (t^*) and the real cyber-attack impact (λ^*) for a level of investment I^{**}_s, the expected loss that operator would sustain is $E^{*}(L)'$ which is higher than that estimated.

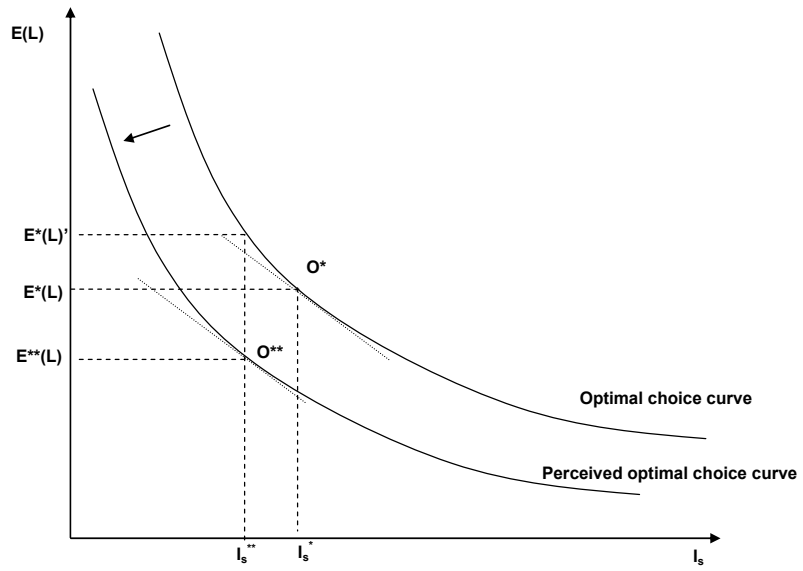
This analysis shows that the lack of information on cyber-attacks may cause an inadequate awareness of related risk (represented in the position of the perceived optimal choice curve) which leads each ICT operator to

[10] On this topic interesting articles have been written by CABALLERO (1991) and ABEL & EBERLY (1999).

[11] The vulnerability variable, v, composing the expected loss, is considered constant at least in the short term. In fact, it is assumed that the vulnerability of the ICT operator is a technological concern linked to the variability of the cybersecurity environment, where dangerousness and frequency of cyber-attacks change only in the long-term. In this study, vulnerability is considered constant as "protective capacity" and can be effectively modified in the mid-term only through current security investments implemented by the ICT operator.

invest in cybersecurity in a suboptimal way, with a level of implemented security provision insufficient not only for social demand but also for the ICT operator's preferences.

Figure 2 – The effect of lack of information on the optimal level of investment in cybersecurity



In this context, cyber-attacks cause greater economic damages than expected by the ICT operators themselves, with amplified consequences on other critical infrastructure operators, public authorities/bodies and citizens.

■ The improvement of information availability on cyber-attacks: potential measures at European level

The strategic role of ICT services in the current European economies is increasing the policy makers' interest towards protection against cyber-attacks and towards possible measures to reduce related market failures.

One of the possible regulation solutions is suggested by GARCIA & HOROWITZ (2007) in "The potential for underinvestment in internet security: implications for regulatory policy", where incentives and obstacles to security provisions in the Internet market are investigated. Their model confirms the security underinvestment (from a social perspective) by Internet providers:

the social value derived from Internet largely exceeds potential and actual revenues associated with the telecommunication companies. GARCIA & HOROWITZ sustain appropriate, at least in the long term, the implementation of regulatory instruments focusing on a standardized security risk analysis for Internet companies even if there are difficulties due to the inability to measure the current level of security, the evolution of cyber-attackers' tools, the implementation of homogeneous security tools, the capacity of ranking security risks and the different organisations' financial readiness and technological profile to support security of the internet infrastructure.

For this purpose, the starting point of institutional efforts against the spread of this threat at the European level is the Convention on Cyber-crime, composed and signed by the Council of Europe in November 2001 in Budapest [12]. It represents the first recognition of the necessity to protect society, industry and citizens' life from cyber-crime by harmonizing national laws, improving investigative techniques and increasing cooperation among nations.

In addition, the Communication on "Network and Information Security: Proposal for a European policy approach" [13] stimulated a structured approach to the Information system protection. In recognition of the ever growing importance of the issue, the European Commission revitalized its 2001 approach and developed a new strategy for a secure Information Society which was adopted on May 31, 2006 [14].

In 2009, the European Commission adopted the Communication on Critical Information Infrastructure Protection [15], which develops a structured European policy on prevention, preparedness and awareness and defines a plan of immediate actions to strengthen the security and resilience of CIIs.

---

12 Convention of Cybercrime, Budapest, 23 November 2001.

13 COM (2001) 298 Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Region. "Network and Information Security: Proposal for a European policy approach".

14 COM (2006) 251. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Region. "A Strategy for a secure information society - Dialogue, partnership and empowerment".

15 COM (2009) 149 final. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection – "Protecting Europe from large scale cyber-attacks and disruption: enhancing preparedness, security and resilience".

More recently, the Communication on "A digital agenda for Europe" [16] aimed at delivering sustainable economic and social benefits from a single digital market. Particular attention is addressed to reinforcing Network and Information Security Policy in the Chapter on Trust and Security. The communication suggests an intervention to modernize ENISA [17] and to set up a Computer Emergency Response Team (CERT) specifically for EU institutions.

All the regulatory initiatives against cyber-attacks undertaken at the European level are focused on the critical role of information on cyber-crime and on the network nature of information systems and its consequence on security. Most of the proposed measures aim to increase the social awareness of cyber-attack effects and to reduce the biased optimal choice behaviour of ICT operators, targeting with policy indications also the other actor categories as stakeholders able to impact directly on the security provisions.

In order to improve cybersecurity, an incentive framework can be set up by policy makers for:

- Sharing technical information through a bottom-up approach essentially involving ICT operators and other critical infrastructure operators to better assess the cybersecurity risk at the organization level
- Sharing technical information through a top-down approach essentially involving ICT operators and public authorities/bodies to set up measures to prevent cyber-attacks and to better assess cybersecurity risk at the social level
- Spreading information on the cyber-crime phenomenon, increasing the knowledge for each category of ICT stakeholder (ICT operators, other critical infrastructure operators, public authorities/bodies and citizens)

16 COM (2010) 245. 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".

17 The renewal of the mandate of ENISA and its modernization have been regulated through the "Proposal for a regulation of the European Parliament and of the Council amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration" (COM (2010) 250 final) and by the "Proposal for a regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA)" (COM (2010) 251 final).

The following paragraphs review potential actions at the European level able to reduce the lack of information on cyber-attacks and to increase the cybersecurity level not only through the higher investments of ICT operators.

How information sharing on cyber-attacks may raise security investment

ICT stakeholders' active interaction is necessary to exchange information on experienced incidents and breaches in order to be effective in increasing the level of knowledge and control of cyber-attacks. A positive impact on the improvement of Network Information Security and on the minimization of the potential disruption effects is given by the sharing of information on threats, vulnerabilities, risk assessment and response best practices (e.g. including investment strategies) among ICT operators and other critical infrastructure operators (ENISA, 2007).

Institutionally, important steps have been taken at the European level to facilitate information sharing. The Resolution 2007/C68/01 of the European Council of 2007 invited Member States to "encourage where appropriate in co-operation with ENISA, effective exchanges of information and co-operation between the relevant organizations and agencies at the national level" referring in particular to Network Operators, service providers and rest of the private sector [18].

To this purpose, introduction of circles as platforms and forums to share information enhances preparedness and resilience. These circles are groups of ICT operators and other critical infrastructure operators (at national or international level) available to spread information on cybersecurity within the restricted group. Participation is subject to compliance with requisites set by the circle: trust among members, value and concreteness of the content of the information sharing, absence of biased and of competitive behaviors, and guarantee of non disclosure.

Information sharing circles may be led by government bodies and/or authorities and in most of the cases can be considered voluntary and

[18] According to the "Good Practice Guide for Information Sharing" (ENISA 2009a), "an Information Exchange is a form of strategic partnership among key public and private stakeholders. In the NIS field, these can sometimes be referred to as 'Network Security Information Exchanges' (NSIEs) although it is recognised that alternative names can also be used."

bottom-up initiatives. Although information sharing circles may include informal and formal groups, recent evidence in the European context has been driven towards the latter option [19], organizing information circles as "trusted forums" or "trusted platforms" in which operators and stakeholders meet regularly. Formal structures with the participation of public entities and a mixed composition (e.g. ICT operators and other infrastructure operators) guarantee a regulated framework around information sharing circles avoiding an untrustworthy atmosphere hampering valuable exchange of information and good practices [20]. Information sharing circles may represent one of the most efficient tools to solve limitations related to the lack of information and data on cybersecurity for the ICT operators and partially for other critical infrastructure operators. At the organization level, the improvement of cybersecurity related information allows a better assessment of the risk of disruptions and supports more effective investment choices both to improve preparedness and to respond to emergencies.

The exchange of information may increase security awareness of ICT circles' members and result in benefits for individual stakeholders and for the network security of the society as a whole. Applied to the model described before, reduction in the lack of information has the immediate effect of diminishing the distance between the perceived level of damage of cyber-attacks (λ^p) and the actual (λ^*) and the mid-term effect of increasing the ICT operator's awareness of its vulnerability v, bringing the perceived optimal choice curve closer to the actual and pushing I_s^{**} towards I_s^*. Information sharing circles provide information for short-term intervention in the event of emergencies and for long-term perspective reducing costs of potential disruptions with a benefit for all other mentioned ICT stakeholders through an increased level of cybersecurity on the part of ICT operators.

[19] Within the project "Availability and Robustness of Electronic Communications Infrastructures - ARECI", formal approaches for sharing information seem to be the most effective to improve protection of infrastructures critical to the reliability of telecommunications services.

[20] The National Computer Emergency Response Teams (CERTs), which are regulated by public entities, contribute effectively to dissemination of security information. For example, an integrated platform among national contexts would also permit prevention actions of potential disruption and effective management of cyber-attacks at European level. For further details on a concrete realisation, see the project "National and European Information Sharing and Alerting System - NEISAS".

How disruption reporting may reduce cyber-attacks effects

The increase of shared information on threats, vulnerabilities and incidents among CIIs operators' and main stakeholders may refine the risk assessment activity on which security and resilience investment rely. Among the several ways to address the lack of information issues, one solution is the implementation of homogenous practices for disruption reporting, allowing competent authorities to have a complete overview of the emerging threats and related vulnerabilities and to collect significant data for the social risk evaluation.

Through the Telecommunications Regulatory Package (article 13.a.3 of the amended Directive 2002/21/EC) a strong indication has been already provided to Member States in order to:

> "[…] ensure that telecom operators notify the competent national regulatory authority of a breach of security or loss of integrity that has had a significant impact on the operation of their networks".

The telecommunication sector in particular is led by universal service provision rules and Member States have to ensure all users minimum service level provisions according to the current development of technology at an affordable price, irrespective of their geographical location.

As per the ENISA's study on "Good practices on reporting security incidents" (ENISA 2009b):

> "Reporting plays an important role in these efforts as it contributes in improving stakeholders' knowledge of the actual security problems at stake. An effective incident reporting system contributes to the collection of reliable and up-to-date data on information security incidents and ensures: a) quick dissemination of information among interested parties, b) a coordinated response, c) access to a wide pool of expertise about such incidents, d) that national authorities can follow up with the infrastructure managers in a regulatory capacity, e) threat analysis; and f) identification of good practices".

A key-element for overcoming lack of information at European level is therefore a common strategy for collecting detailed data and widening reliable sources (e.g. main ICT stakeholders). In spite of the effort made by the European institutions and bodies to adopt appropriate measures to harmonize incident reporting procedures, existing practices at Member States level remain extremely heterogeneous reducing the effectiveness of

the collected information. [21] Consequently, appropriate reporting schemes and data shared at the European level may impact positively on security and resilience disclosing the effective extent of the cyber-threats. Apart from the effects similar to information sharing, reporting activity [22] of ICT operators to public authorities/bodies may reduce the distance between the perceived probability of cyber-threats (t^p) and the real probability of threats (t^*) spurring the implementation of adequate actions against potential cyber-attacks (e.g. imposition of security standards, cooperation at international level). The entire society would benefit from an increase of cybersecurity sustained by additional investments by ICT operators (towards I_S^*) and other critical infrastructure operators.

How competence may increase cybersecurity level

The consistent development of ICT networks, as well as the technological pervasiveness in all the socio-economic activities, requires a continuous update of technological skills. Education in security is needed to prevent, to face and to react to cyber-crime attacks. Due to the network features of ICT systems and the presence of the weakest link, the development of baseline security technological skills for the largest part of the population may improve the overall security of the ICT systems and those strictly connected. Filling the gap in terms of technological skills with the aim of increasing cybersecurity would mean setting up different education measures for citizens according to their potential user role: home user, ICT professional and worker.

The creation of a cybersecurity culture implies the involvement of society as a whole. Mass actions to communicate essential information on the potential impacts of cyber-attacks ranging from the individual perspective to the public one may represent an effective tool to spread awareness on security issues (ENISA 2009c). In the USA, the National Cyber Security Awareness Month (NCSAM), conducted every October since 2004, is a national public awareness campaign to encourage everyone to protect their computers and the USA's national critical cyber-infrastructure. According to

[21] According to the report "Good practices on reporting security incidents" (ENISA 2009b), differences in incident reporting exist between countries especially in terms of objectives such as emergency response, incident response, incident prevention, legal rectification.

[22] Incident reporting may add value to all the parts involved in the process. Efficient and fast access to valuable information is one of the main benefits for the reporting organizations.

the Department of Homeland Security (DHS), the National Cyber Security Alliance (NCSA) and the Multi-State Information Sharing and Analysis Center (MS-ISAC), cybersecurity requires constant action to coordinate what home users, businesses and governments need to do in order to protect themselves against attacks. [23]

As technology is involved at every level of life, professional ICT education on security issues is essential. Most education systems in Europe have developed ICT skills among future professionals. This awareness should move to encompass security because it is not efficient to divide ICT and security specialists. The need for e-skills certification and e-skills is a moving target modeled after the market. Within this area, specific skills pertaining to ICT security have long been identified but little training effort is currently devoted to security and resilience in the large panel of e-skills certifications throughout Europe. At present, ICT operators and other critical infrastructure operators lack qualified security professionals and academic courses on ICT security represent a preliminary answer to this need of competence.

In addition, it is fundamental for companies and their employees to understand ICT threats, vulnerabilities and risks able to damage their business. For this reason, "training on the job" and "learning-by-doing" are necessary tactics to better protect the employee's daily work from cyber-attacks. Employees tutored through training courses in order to become aware of cyber attack risks and mitigation strategies may avoid severe consequences also due to unintentional internal actions. A provision of constant training (typically in house, i.e. within companies and government agencies) can be conceived at the European level through lifelong learning programmes in which ICT may constitute the core support to reduce potential impacts of cyber-disruptions (both malicious and caused by human error). According to the theoretical representation, the creation of a cybersecurity competence through different channels (awareness of citizens, creation of ICT security professional profiles and cybersecurity training on the job) reduces the gap between the perceived probability of cyber-threat (t^0) and the real probability of threats (t^*). Furthermore, in the mid-term, an increase in cybersecurity competence is advisable to reduce the real probability of threats (t^*). In fact, cyber-threats due to involuntary human errors (and not to malicious attacks) may be consistently reduced through education [24].

---

[23] The USA National Cyber Security Awareness Month, http://www.staysafeonline.org/ncsam.

[24] GORDON & LOEB (2002) mention this effect also in their model.

■ Concluding remarks

Cyber-attacks are gaining in the ranking of global threats for their potential devastating socio-economic impact. Together with cyber-crime fighting, measures to increase the general level of cybersecurity have to be adopted by all relevant stakeholders related to ICT networks. At the European level, regulation efforts are supported by bottom-up actions aimed at reducing market failures of the security-market. In addressing the investment behavior of ICT operators, improvement of their cybersecurity level can be obtained by reducing the current lack of information on cyber-attacks.

An effective cybersecurity investment relies on information on the probability of the threat occurrence, the vulnerability of the system and the potential loss due to the threat realization. Lack of information generates a biased cyber-risk assessment and an underestimation of the potential loss.

Furthermore, increased cybersecurity can be obtained through more efficient behaviour of the other main ICT stakeholders. Formal information sharing practices, homogeneous breach-reporting procedures at the European level and the improvement of the social cybersecurity competence may positively affect the structural conditions in which ICT operators make their cybersecurity investment choice.

Additional research on the cybersecurity topic is needed to deeply investigate the network nature of the ICT world, the related security behaviours of its main actor categories and the extent of the effect of each analysed measure to increase information availability on cyber-attacks to ICT operators.

References

ABEL A.B. & EBERLY J.C. (1999): "The impact of uncertainty on capital accumulation", *Journal of Monetary Economics*, Vol. 44, pp. 330-377.

ACOCELLA N. (2000): *Foundations of Economic Policy. Values and Techniques*, Cambridge Press.

Alcatel-Lucent's Bell Labs and professional services (2007): "Availability and Robustness of Electronic Communication Infrastructures - ARECI", Final Report of the ARECI project supported by DG Information Society and Media of the European Commission.

ANDERSON R. (2001): "Why Information Security is Hard – An Economic Perspective", *Proceedings of the 17th annual Computer Security Application Conference*. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=991483.

ANDERSON R. & MOORE T. (2006): "The Economics of Information Security", *Science*, Vol. 314 no. 5799 pp. 610-613.

ARTHUR S. & SHEFFRIN S.M. (2003): *Economics: Principles in Action*, Pearson Prentice Hall.

AVIRAM A. & TOR A. (2004): "Overcoming impediments to information sharing", Harvard Law school discussion paper, *Alabama Law Review*, Vol. 55.

BORG S.

- (Forthcoming): *Cyber attacks. A Handbook for Understanding the Economic and Strategic Risks*, US – CCU.
- (2005): "Economically complex cyber attacks", *IEEE Security and Privacy*, Vol. 3.
- (2009): "The Economics of Loss" in *Enterprise Information Security and Privacy*, edited by C. Warren AXELROD, Jennifer L. BAYUK & Dainel SCHUTZER.

BRUCK T., KARAISI M. & SCHNEIDER F. (2006): "A survey of the economics of security", NEAT Economics of Security working paper 1.

CABALLERO R.J. (1991): "On the sign of the investment-uncertainty relationship", *American Economic Review*, Vol. 81, No. 1, pp. 279-288.

CAMBACÉDÈS L.P. & CHAUDET C. (2010): "The SEMA Referential Framework: Avoiding Ambiguities in Security and Safety Issues", presentation at the 4th Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, Fort McNair, Washington, DC, USA, March 14-17, 2010.

CAVALLINI S., DI TROCCHIO S., BISOGNI F., TANCIONI M. & TRUCCO P.C. (2010): *Study for the Development of a Methodology and Research of Quantitative Data on the Economics of Security and Resilience in Critical Communications and Information Infrastructures – CIIS – SMART-SEC*, Final Report of the SMART-SEC project supported by DG Information Society and Media of the European Commission.

CHOI J.P., FERSHTMAN C. & GANDAL N. (2004): "Internet Security, Vulnerability Disclosure, and Software Provision", 4th Workshop on the Economics of Information Security, Harvard University, Cambridge.

European Parliament:

- COM (2001) 298. Communication from the Commission to the Council, the European Economic and Social Committee and the Committee of the Region, "Network and Information Security: Proposal for a European policy approach".
- COM (2006) 251. Communication from the Commission to the Council, the European Economic and Social Committee and the Committee of the Region, "A Strategy for a secure information society - Dialogue, partnership and empowerment".
- COM (2009) 149 final. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the

Committee of the Regions on Critical Information Infrastructure Protection – "Protecting Europe from large Scale Cyber-Attacks and Disruption: Enhancing Preparedness, Security and Resilience".

- COM (2010) 245. 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".

- COM (2010) 250 final. Proposal for a regulation of the European Parliament and of the Council amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration

- COM (2010) 251 final. Proposal for a regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA)

Council of Europe:

- (2001): Convention of Cybercrime, Budapest, 23 November. http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm

- (2008): Directive 2008/114/EC, 8 December, "On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection".

- (2002): Directive 2002/21/EC of the European Parliament and of the Council, 7 March, "On a common regulatory framework for electronic communications networks and services" (Framework Directive).

DIXIT A.K. & PINDYCK R.S. (1994): *Investment under Uncertainty*, Princeton University Press.

ENEA (2011): "National and European Information Sharing and Alerting System - NEISAS", project supported by the Prevention, Preparedness and Consequence Management of Terrorisms and Other Security Related Risk Programme of the European Commission's Directorate Home Affairs.

ENISA:

- (2007): "Examining the feasibility of a data collection framework", ENISA Report.

- (2009a): "Good Practice Guide for Information Sharing", ENISA Report.

- (2009b): "Good Practices for Reporting Security Incidents", ENISA Report.

- (2009c): "The growing requirement for information security awareness", ENISA Report.

FORMIT (2009): "The Vulnerability of Information Systems and its iInter-sectoral, Economic and Social Impacts – VIS", project supported by the Prevention, Preparedness and Consequence Management of Terrorisms and Other Security Related Risk Programme of the European Commission's Directorate Justice, Freedom and Security.

GAL-OR E. & GHOSE A. (2004): "The Economic Consequences of Sharing Security Information", *Advances in Information Security*, Vol. 12.

GARCIA A. & HOROWITZ B. (2007): "The Potential for Underinvestment in Internet Security: Implications for Regulatory Policy", *Journal of Regulatory Economics*, Vol. 31.

GORDON L.A. & LOEB M.P. (2002): "The Economics of Information Security Investment", *Advances in information security*, Vol. 12.

GREENE W.H. (2007): *Econometric Analysis*, Prentice Hall.

HAUSKEN K. (2006): "Returns to Information Security Investment: The Effect of Alternative Information Security Breach Functions on Optimal Investment and Sensitivity to Vulnerability", *Information SystemsFrontiers*, Vol. 8, no. 5, pp. 338-349.

KANNAN K. & TELANG R. (2005): "Market for Software Vulnerabilities? Think Again", *Management Science*, Vol. 51, no. 5, pp. 726-740.

KEIZER G. (2010): "Is Stuxnet the 'best' malware ever?", *Infoworld*, 16 September. http://www.infoworld.com/print/137598

KOLFAL B., PATTERSON R. & YEO M.L. (2010): "Market impact on it security spending", Workshop on the Economics of Information Security, Arlington, USA. http://weis2010.econinfosec.org/papers/session1/weis2010_kolfal.pdf

KREPS D. (1990): *A Course in Microeconomic Theory*, Princeton University Press.

KÜHN K.U. & VIVES X. (1995): "Information Exchanges Among Firms and their Impact on Competition", Institut d'Anàlisi Econòmica (CSIC).

LIU D., JI Y. & MOOKERJEE V.M. (2005): "Information Security Investment with Different Information Types: A Two-Firm Analysis", *AMCIS 2005 Proceedings*.

MARKUSEN A.R. (2003): "The Case Against Privatizing National Security Governance", *International Journal of Policy, Administration and Institutions*, Vol. 16, Issue 4, pp. 471–501.

MAS-COLELL D., WINSTON M. & GREEN J. (1995): *Microeconomic Theory*, Oxford University Press

POWELL B. (2005): "Is Cybersecurity a Public Good? Evidence from the Financial Services Industry", *Journal of Law, Economics and Policy*, Vol. 1, pp. 497-510.

TEECE D. (2003): "Information sharing, innovation, Antitrust", in *Essay in technology management and policy*, World Scientific.

The USA National Cyber Security Awareness Month. http://www.staysafeonline.org/ncsam

VARIAN H.R. (2004): "System Reliability and Free Riding", in *Economics of Information Security*, Springer.

WILLEMSON J. (2006): "On the Gordon & Loeb Model for Information Security Investment", Workshop on the Economics of Information Security, Cambridge, England. http://weis2006.econinfosec.org/docs/12.pdf