COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 31.5.2006
SEC(2006) 656

COMMISSION STAFF WORKING DOCUMENT

Annex to the

COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

A strategy for a Secure Information Society – "Dialogue, partnership and empowerment"

{COM(2006) 251 final}

IMPACT ASSESSMENT

Lead DG:

Information Society and Media

Other involved services:

Relevant services have been consulted in the process of preparation of the Communication.

An inter-service impact assessment steering group has been established. Representatives of the following services were invited: SG, DG COMP, DG DIGIT, DG EAC, DG ECFIN, DG ENTR, DG JLS, JRC, DG MARKT, DG RTD, and DG SANCO.

Commission Legislative Work Programme reference:

2006/INFSO/002

EXECUTIVE SUMMARY

The present report accompanies a Communication that is being prepared as a response to a commitment voiced in its initiative "i2010 – A European Information Society for growth and employment" to coordinate efforts to build trust and confidence of businesses and citizens in electronic communications and services.

Network and information security should be understood as one of the crucial elements of the Information Society enabling smooth development and deployment of new systems, applications and on-line services. Its economic significance to the European economy cannot be understated. At the same time, security problems persist, as illustrated daily by reports of new incidents (whether technical failures, accidents or intentional attacks). In addition, an interesting change in the "threat landscape" is currently taking place: while traditionally attacks have been predominantly motivated by curiosity and a desire to show off technical virtuosity, many current threats are motivated by profit and often attempt to perpetrate criminal acts, such as identity theft, extortion and fraud.

Against this background, several available policy options for dealing with the complex issues of network and information security have been considered, including "business as usual" and a purely regulatory option. The potential (economic and societal) impacts of the options have been analysed. The former has been discarded as insufficient in view of the current and new challenges. The latter, in turn, was deemed insufficient, as the complex set of issues related to network and information security could not be effectively addressed through regulatory action only.

As a result of the analysis, a preferred policy option has been singled out: "coordinated action". This option would mean pointing a strategic way forward (with the involvement of Member States and other stakeholders, and ENISA, as appropriate), while simultaneously overcoming existing fragmentation, both at the level of Member States and other stakeholders and at EU level.

In particular, the coordinated option could add value with respect to the various on-going and planned activities within the European Commission which has traditionally approached network and information security from various angles, including the policy for electronic communications networks and services, privacy and data protection, and cybercrime. The European Union (as well as most Member States) has a long-standing tradition of handling those various aspects separately, but in a coordinated manner (e.g. the situation in 2001 where two communications, on network and information security, and on cybercrime, were prepared in parallel)[1].

This report commits only the Commission's services involved in its preparation and does not prejudge the final form of any decision to be taken by the Commission.

[1] Communications: "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime" - COM(2000) 890 (January 2001); "Network and Information Security: Proposal for A European Policy Approach - COM(2001) 298 (June 2001). See also the graphic representation of the relationships (and overlaps) between the related policy domains in Part 2 (p. 5 above).

1. PROCEDURAL ISSUES AND CONSULTATION OF INTERESTED PARTIES

1.1. Organisation and timing

Trust and security forms an integral part of the "**i2010 – a European Information Society for growth and employment**". This initiative recalls an urgent need to co-ordinate efforts in order to develop policies, regulations, technology and awareness, to build trust and confidence of businesses and citizens in electronic communications and services and announces a new Strategy to be proposed by the Commission.

In view of the broad scope and the cross-cutting nature of the subject matter at hand, an inter-service steering group has been established. The following Commission services were invited to participate: Secretary-General; Justice, Freedom and Security; Informatics; Enterprise and Industry; Joint Research Centre; Research; Internal Market and Services; Health and Consumer Protection; and Economic and Financial Affairs.

1.2. Consultation and expertise

Building upon the Commission's commitment to transparency and evidence-based policy making, long before the draft Communication proposal is presented, a wide stakeholder consultation process has taken place. The general principles and minimum standards for consultation[2] have been respected.

Informal consultations were held, in particular with ENISA, as well as other Commission services. Some discussion have been taking place in the context of other specific activities of the Commission which are (at least partly) relevant to the proposed Communication (e.g. within the Inter-Service Sub-Group on Critical Infrastructure Protection).

In addition, a series of meetings with information security experts from the 25 Member States was organised by the Commission to take stock and discuss existing and future challenges for network and information security, and in particular the security and stability of the Internet, and define the way forward. The first meeting took place on 18th January 2005 and resulted in a set of issues agreed as the main challenges to the addressed in the development of a stable Internet[3]. The issues ranged from problems with core Internet infrastructure and protocols, through availability and reliability of information concerning threats and vulnerabilities, through lack of coordinated network and information security policy in the Member States, through awareness raising and education. The results of this meeting served as input of the European Union to the WGIG process[4]. The second meeting on 26 April 2005 started from this list of identified challenges and investigated possible responses, in particular the role that public authorities could play in securing information systems and networks, including the

---

2 As set out in the communication "General principles and minimum standards for consultation of interested parties by the Commission" - COM(2002) 704.

3 Proceedings from this meeting are available at: http://europa.eu.int/information_society/newsroom/cf/itemlongdetail.cfm?item_id=1687

4 Working Group on Internet Governance, in the WSIS context

Internet. The present document builds to a considerable extent on the results of this exercise.

On 9 February 2006, the Commission services jointly with the Austrian Presidency organised an international High-Level Research Seminar "Trust in the Net"[5]. This event constituted an important step in consultation process. It brought together a wide range of stakeholders, including Member States governments, research community, representatives of consumer protection organisations, and civil liberty groups. The main conclusions of the seminar have been taken into account in finalising the impact assessment process[6].

2. PROBLEM DEFINITION

Launching the partnership for growth and jobs as a new start for the Lisbon strategy, the 2005 Spring European Council called knowledge and innovation the engines of sustainable growth and stated that it is essential to build a fully inclusive Information Society, based on widespread use of information and communications technologies (ICT) in public services, SMEs and households. **To that end, the new initiative for the next five years should focus on ICT research and innovation, content industry development, security of networks and information, as well as convergence and interoperability in order to establish a seamless information area[7].** The need for a new, coherent approach was recognised most recently in the i2010 initiative which set as one of its objective the creation of a Single European Information Space offering affordable and secure high bandwidth communications, rich and diverse content and digital services.

Network and information security can be understood as the ability of a network or an information system to resist, at a given level of confidence, accidental events or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems[8]. Network and information security policy in the European Union should be seen in the context of the existing policies for electronic communications networks and services, privacy and data protection, and cybercrime, as illustrated by the following diagram[9]:

---

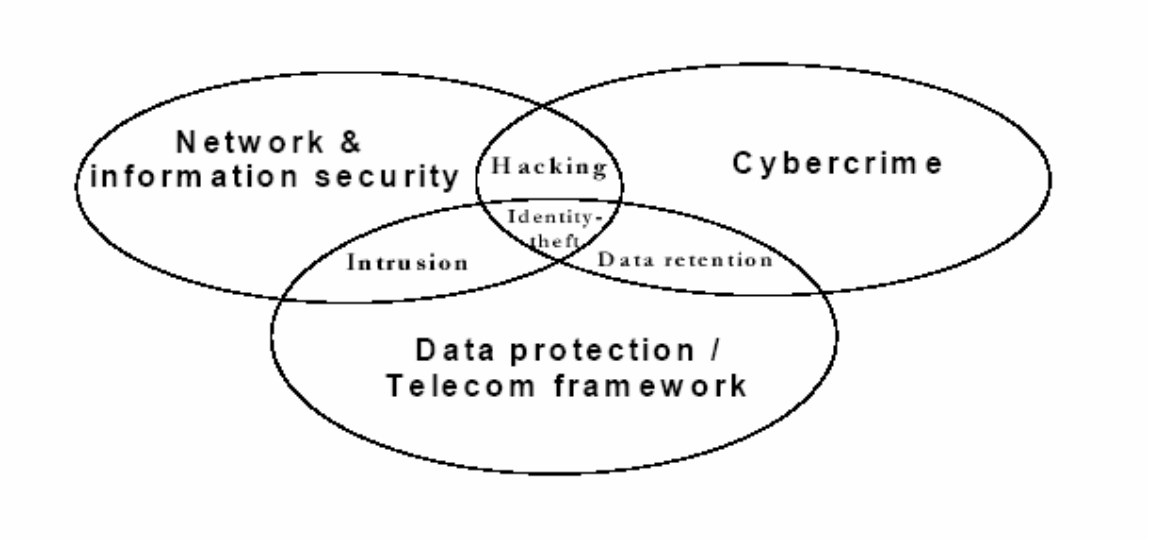
5 See "Trust in the Net" website: http://www.eu2006.at/en/Meetings_Calendar/Dates/February/0902TrustintheNet.html

6 See below, chapter 2.4.

7 European Council, Brussels, 22-23 March 2005, Presidency Conclusions, 23/3/2005 (English) Nr 7619/1/05 REV1.

8 Communication from the Commission "Network and Information Security: Proposal for a European Policy Approach" - COM(2001) 298.

9 *Ibidem*, p. 3.



Network and information security is a key enabler for the further development of the Information Society in Europe and beyond. Indeed, reliable electronic communications networks and services have gained an enormous economic and societal importance as they underpin more and more many critical aspects of our economy and society.

At the same time, the progressing liberalisation of electronic communications networks and services markets and the resulting multiplication of actors involved, and the technological developments (to mention but two major elements) have, on the one hand, boosted competition, economic and business growth and, on the other hand, rendered the management of networks a very complex task and the division of responsibilities of various actors involved rather unclear. This is further discussed in section 2.1 below.

A lot has been done since the adoption of the 2001 Communication (see also the description of recent and on-going EU initiatives related to network and information security in the Annex). However, a lot remains to be done since security problems still persist on electronic communications networks and new developments bring about new threats and disclose previously unknown vulnerabilities. Section 2.2 below briefly sketches the current state of affairs.

2.1. The economic significance of information security

Network and information security is a far-reaching and global issue which has become increasingly important in the society based on information and knowledge. Consumers, companies and governments rely to a great extent on communication networks and information technologies. Such networks include not only the Internet, but all communications infrastructures, whether IP-based, traditional telephony or data exchange, as well as mobile networks.

Users of such electronic communications networks expect reliable networks functioning without severe disruptions or interceptions and high-quality software protecting them

against malicious attacks, spam, viruses and other forms of malware[10]. They also expect a high level of protection of confidential or personal information.

Information and Communications Technologies play a vital role in Europe's continuing modernisation. The e-communications services sector continues to represent the largest segment of the overall ICT sector, accounting for 44.4% of the total value, up from 43% last year. The sector was worth €614 billion in 2005, €273 billion of which derived from e-communications services. Overall revenue growth continued strong at estimated levels of between 3.8%4 and 4.7%5. The production and use of ICT account for around 40% of productivity growth and one quarter of overall growth in Europe[11].

It is a highly innovative sector, responsible for more than a quarter of total effort in European R&D effort and capable of creating growth and jobs. Achieving the Lisbon strategy – that is, the goal to create a competitive, sustainable and a socially inclusive Europe – largely depends on the take up of secure and dependable ICT across all sectors.

Trade indicators tell a similar story. In 2004, total imports of ICT goods and services into the EU Member States amounted to more than 450 billion euro[12]. Much of this investment is going into information systems that are critically dependent on security-related performance criteria and stability requirements. Large parts of the EU economy are now either producing ICT-related goods and services or depending on them to execute their own business activities or to deliver their own ICT-based services.

ICTs also play an essential role in managing change in industry and the service sector – from health to inclusion, from regional development to the protection of our environment and promotion of cultural diversity. ICTs also play an essential role in meeting the demand for health and social care and in supporting the state-of-the-art and innovative provisioning of essential public and private services such as education, learning, security, energy, transport and environment.

In the EU-25, electronic communications networks and services are increasingly being deployed and used for a variety of purposes, including e-commerce, e-business and e-government applications. Enterprises invest in ICT for different reasons, e.g. to increase sales and market share; to improve efficiency of internal business processes or to reduce costs through e-procurement.[13]

The following figure[14] shows the percentage of enterprises using ICT applications[15]:

---

10 "Malware" stands for "malicious software".

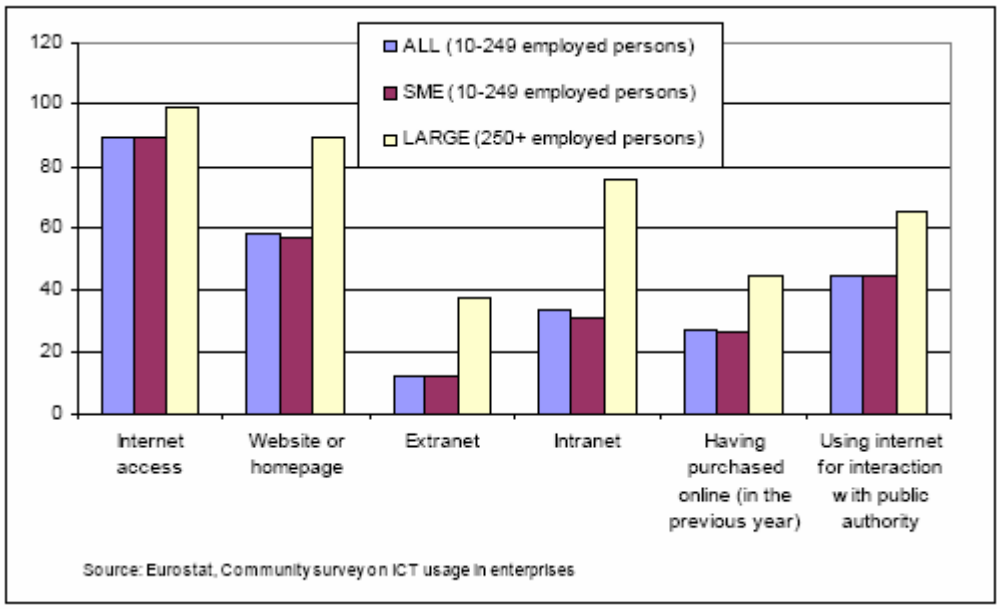
11 European Electronic Communications Regulation and Markets 2005, 11th Implementation Report - COM(2006) 68.

12 OECD "Key ICT indicators" 2005.

13 Source: Information Society Benchmarking Report, 2005, available at: http://europa.eu.int/information_society/eeurope/2005/all_about/benchmarking/index_en.htm

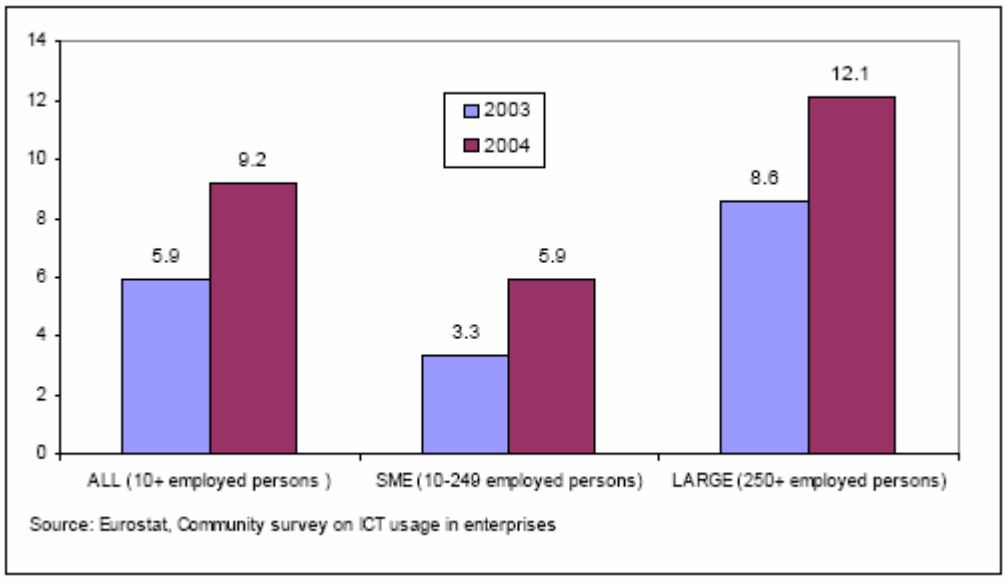
14 *Ibidem*

15 Please note that the legends for the category marked "ALL" should read: "10-250+ employed persons".



Even though most firms in the EU-25 (89 %) have an Internet connection, the other indicators show that other uses of networks (such as maintaining a website, or interactions with public authorities) are far less popular. The report also concludes that there is no evidence of growth in the use of ICT, which suggests that a large section of the business community is only beginning to exploit the potential of ICT[16].

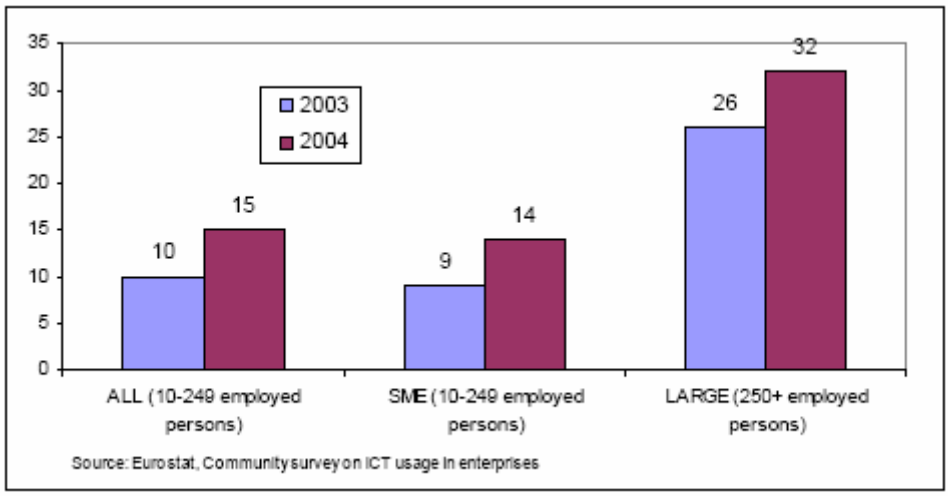
In terms of e-commerce revenue, an average growth from 5.9 % to 9.2 % has been noted between 2003 and 2004, with a faster growth rate for SMEs than for large enterprises, as illustrated below[17]:



16 *Ibidem*, p. 14.

17 *Ibidem*. The data covers EU15 only. Please note that the legends for the category marked "ALL" should read: "10-250+ employed persons".

At the same time, the proportion of enterprises selling on-line also grew[18]:



At the same time, results from the *e-Business W@tch* show that the use of advanced e-business solutions for automating business processes (such as enterprise resource planning; supply chain management; and customer relation management) is generally still low (and strongly correlated to company size). For instance, in 2005, 27 % of large enterprises use a supply chain management system (compared to 8 % of small and 14 % of medium enterprises[19].

In the same way that ICTs can generate value-added beyond the initial economic investment, failure in ICT-based information systems can also generate a negative impact that exceeds the economic value of the systems themselves. Potential impact values will vary according to the nature and extent of the failure concerned, but will inevitably increase in general in direct proportion to the deployment and dependency of information and network systems in the economy as a whole.

Both the 2003 WSIS Declaration of Principles[20] as well as the recent Tunis Agenda for the Information Society confirmed that confidence and security are the main pillars of the Information Society. Therefore, there is a need to promote, develop and implement a global culture of security. From a historical point of view, concerns about information security (with a slight difference in meaning, also referred to as "cybersecurity", "information assurance", or "critical information infrastructure protection") are not a new phenomenon. For instance, viruses and worms have been part of cyberspace since its early days[21]. However, the issue has gained more political impetus as communication

---

18 Please note that the legends for the category marked "ALL" should read: "10-250+ employed persons".

19 *Ibidem*, p. 18.

20 Declaration of Principles "*Building the Information Society: a global challenge in the new Millennium"*, document WSIS-03/GENEVA/DOC/4-E dated 12 December 2003; and Tunis Agenda for the Information Society, document WSIS-05/Tunis/doc/6(Rev.1)-E dated 18 November 2005.

21 E.g. the "Morris worm" distributed as early as 1988, see http://en.wikipedia.org/wiki/Morris_worm.

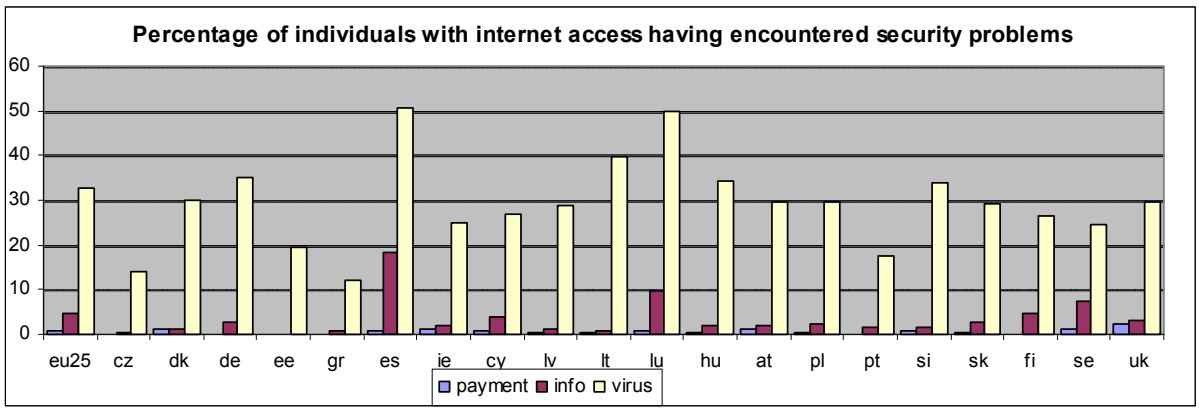
networks and information systems have become an essential factor in economic and societal development.

Information, predominantly in digitalised form, processed and transmitted over electronic networks, including the Internet, has become a strategically important, integral part of everyday economic and social life. ICT and communications networks are now becoming ubiquitous utilities in the same way as electricity or water supply already are, underpinning many functions of the society, but also introducing unknown interdependencies. The security of electronic communications networks and information systems, in particular their availability, is therefore of increasing concern to EU citizens.

2.2. Current trends in information security

A mere look at statistics and general surveys conducted in the area of network and information security indicates that the goal of secure and reliable networks and sufficient protection of information carried on them is still far away. Despite efforts undertaken at various levels, network and information security problems persist[22].

The following data from Eurostat[23] shows the percentage of citizens and businesses with Internet connection having encountered security problems during the year 2004. The graph shows that the most important security problem which EU citizens are confronted with is the presence of viruses. More than 30 % of EU citizens reported a virus in their computer.

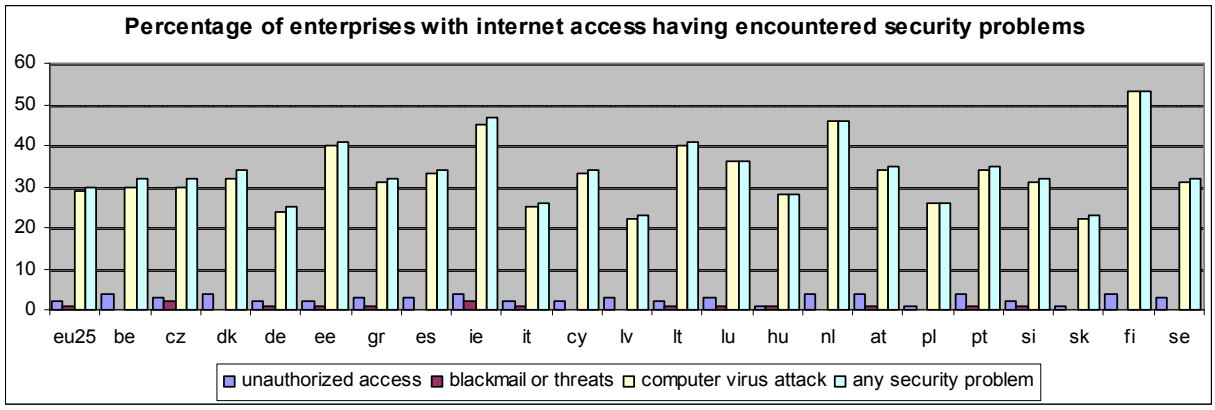


The same situation holds for enterprises: around 30 % of EU enterprises with Internet access were attacked by a virus in 2004. 2 % of them reported unauthorized access.

---

22 One of the difficulties in preparing the present report was obtaining reliable quantitative data about the current situation in Europe with respect to the number of security incidents, their costs for businesses, etc. The information easily available is often US-centred or gives a global overview, without indicating the state of the affairs in Europe (not to mention the even smaller scale of the EU). In addition, it is often provided by industry with clear financial interest in presenting security-related information in a way that suits their marketing strategies. This does not necessarily mean that such data cannot be trusted, of course, but it raises doubts and undermines the value of such data as a support for policy making.

23 The data can be accessed at: http://epp.eurostat.cec.eu.int/



Reportedly, a new computer connected to the Internet without firewall and virus protection will be taken under control by hackers within a few minutes[24]. Citizens who are not aware of the seriousness of various threats related to the usage of network can become not only victims of a computer attack but also a source of one. For instance, a computer - typically connected to the Internet via a broadband connection and without security software to protect it - might become infected by a Trojan horse or other malicious code and become a "zombie", i.e. used remotely to send spam, mount denial-of-service attacks, or other online crimes.

Not only the Internet, but all electronic communications networks are vulnerable to security threats. For instance, spam, and increasingly malware, is also being distributed from one mobile phone to another (via SMS, MMS or through bluetooth connections). In addition, even if a large-scale, major global failure in a communications network has yet to happen, there have been examples of severe disruptions in several European countries in the past years[25]. This raises questions about the appropriate risk analysis and contingency planning by European operators, as well as whether adequate safeguards have been put in place by the Member States to prevent, or minimise impact of, similar failures[26].

Networks and information systems are vulnerable not only to attacks or security threats but also to an increasing number of vulnerabilities in the software that are due to the an unsatisfactory quality of the software and may range from flaws in operating systems, through Web applications vulnerabilities, through security holes in Web browsers. Such inherent and very often unknown software vulnerabilities may either lead to unexpected failures or be exploited for malicious attacks. This applies in particular to vulnerabilities in critical and ubiquitous software systems or applications, such as Web browsers, internet protocols, operating systems, etc. But vulnerabilities are unfortunately present in

---

24 See e.g. results of an experiment conducted in the US in 2004 available at: http://www.freerepublic.com/focus/f-news/1291394/posts.

25 E.g. the failure of the Norwegian mobile network operated by Netcom for several days in June 2005; earlier, similar problems have been reported in France.

26 It should be noted that provisions of the current regulatory framework for electronic communications concerning integrity of networks and access to emergency communications apply only to the "public telephone network at fixed locations" (Article 23 of the Universal Service Directive).

all sorts of software applications, including e-mail clients, file sharing applications, and even backup and anti-virus software[27].

The Symantec Internet Security Threat Report[28] monitoring computer and network vulnerabilities periodically every six months documented the highest number of new vulnerabilities in the first half of 2005 ever since the Symantec started monitoring. 59 % were found in Web application technologies. 97 % of these vulnerabilities were highly or moderately severe. For instance, the number of denial-of-service attacks (DoS) grew by more than 600 % compared to the previous period. Symantec reports also a strong increase in the number of variants of viruses and worms.

The scope of security threats is already very wide and is expected to widen even further with new technologies arriving on the market, such as wireless technologies, voice-over-IP (VoIP), etc. In addition, there are indications that security problems associated with mobile computing (the use of laptops, PDAs, smartphones, etc.) might become the most important information security issues over the next few years. A recent study points out that one-third of professionals who use mobile devices do not protect the data they contain with passwords or any other type of security measure. 30 % use the devices to store PINs, passwords and other sensitive corporate data, including customer contacts. 22 % of those surveyed said they had lost a mobile device; of those, 81 percent had not encrypted the data on the device[29]. Clearly, not all organisations have sufficiently addressed these issues in their security policies.

According to the OECD[30], a number of factors are likely to contribute to continuing vulnerability in the coming years. These include:

- The introduction of entirely new and potentially more destructive forms of malicious code and cyber attacks;
- The proliferation of new web applications, often with easy-to-exploit remote accessibility;
- The spread of instant messaging and peer-to-peer applications;
- The growth of mobile devices with always-on connectivity and remote access to critical sensitive data.

The study concludes that "as the vulnerability of information systems persists and evolves, demand for information security – both for physical security and access control (e.g. biometrics, encryption login) and for operational security (firewalls, anti-virus software etc.) – is expected to grow"[31].

---

27 For an overview of the most frequent security vulnerabilities related to the use of the Internet, see e.g.: http://www.sans.org/top20/.

28 Symantec Internet Security Threat Report, Volume VIII, cited above.

29 Pointsec's Mobile Usage Survey, 2005.

30 "The Security Economy", OECD, 2004.

31 *Idem*, p. 30.

Spam, or unsolicited commercial communications, remains a serious problem. Symantec reports that in the first half of 2005, spam made up 61 % of all e-mail traffic (a slight increase from 60 % in the previous 6-month period). In addition to infringing individuals' privacy, consuming bandwidth and creating avoidable costs for consumers and businesses (an estimated $20 billion worldwide[32]), spam is increasingly a vehicle used for distribution of viruses, spyware[33] and other forms of malware, as well as in *phishing* scams.

In addition, an interesting change in the "threat landscape" is currently taking place[34]. A couple of years ago, most security problems were reportedly caused by viruses and worms, to a lesser extent by unauthorised entry to internal networks, manipulation of software applications, identity theft or online fraud[35]. Traditionally, attacks have been motivated by curiosity and a desire to show off technical virtuosity, many current threats are motivated by profit. They often attempt to perpetrate criminal acts, such as identity theft, extortion and fraud. This phenomenon is sometimes summarised as a shift from a "hack for fun" to a "hack for money". Another particularly worrisome trend is the increase in malicious code that exposes confidential information, to 74 % of the top 50 malicious code samples reported to Symantec (up from 54 % during the previous reported period). This is very alarming, as threats to confidential information can result in significant financial loss, particularly if credit card information or banking details are exposed.

In this context another relatively recent phenomenon must be mentioned. *Phishing* is a form of social engineering aimed at fraudulent acquisition of sensitive information, such as passwords and credit card details. The fraudster masquerades as a trustworthy person or business in an apparently official electronic communication, such as an e-mail or an instant message, which tricks users into giving away their account information by "confirming" it at the *phisher's* linked website (a link to which is typically included in the message). According to Symantec, between 1 January and 30 June 2005, the volume of *phishing* messages grew from an average of 2.99 million attempts a day to 5.7 million. Gartner estimates 57 million Americans have received phishing e-mails costing victims $1.2 billion in just one year[36].

As indicated above, the revenue from e-commerce has been increasing steadily over the past years, despite the persistent security-related problems. One of possible explanations would be that a significant proportion of actors active in the sector have responded to security threats by implementing security measures.

---

32 Business Software Alliance, September 2005.

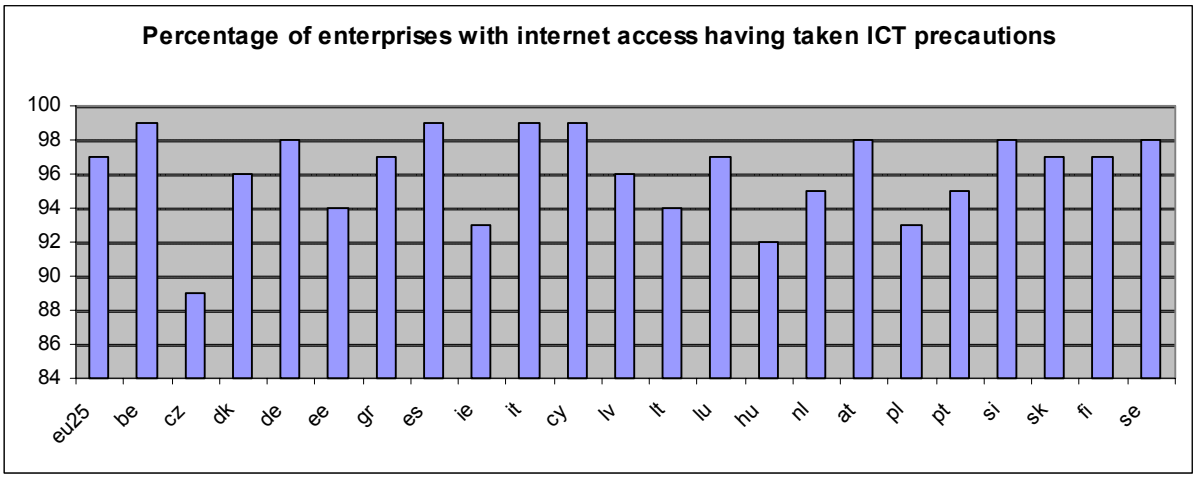
33 The Working Report issued on 27 October 2005 by the Anti-Spyware Coalition defines "spyware" in its narrow sense as tracking software deployed without adequate notice, consent, or control for the user. In its broader sense, the term covers all potentially unwanted technologies deployed without appropriate user consent and/or implemented in ways that impair user control over: (i) material changes that affect their user experience, privacy, or system security; (ii) use of their system resources, including what programs are installed on their computers; and/or (iii) collection, use, and distribution of their personal or other sensitive information. See http://www.antispywarecoalition.org/documents/definitions.htm

34 Symantec Internet Security Threat Report, Volume VIII, trends for January 2005 – June 2005, published in September 2005.

35 The RAND 2003 survey, cited above.

36 *Idem*

Indeed, available data illustrate the readiness of consumers and enterprises respectively to respond to security threats, as shown by the following graphs. Most enterprises (97 %) in the EU-25 take precautionary measures as a reaction to security threats (although the statistics does not reveal whether these measures were effective and sufficient).



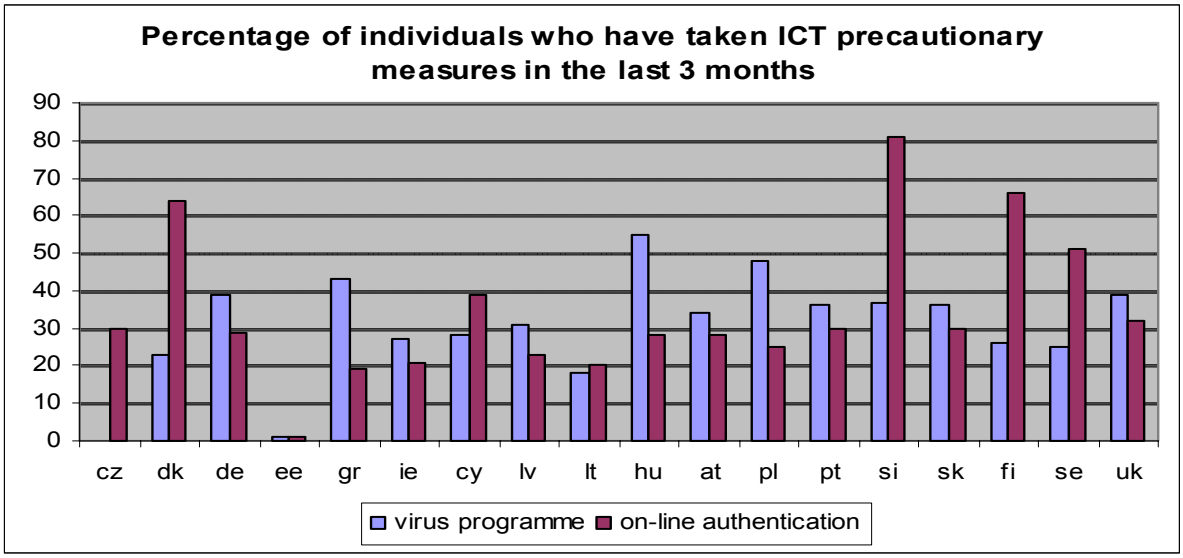
Also a recent European Commission's *e-Business W@tch*[37] indicates that basic components (such as firewalls and secure servers, if required) are already highly deployed by European enterprises. Three quarters of employees working in enterprises of all sizes are already equipped with firewall technology. The second most commonly implemented ICT security control is the drafting of a disaster recovery plan. On the other hand, there is still a lot to be done as far as other methods for countering risks are concerned. For instance, implementing an IT security policy comes third on the list, but at a surprisingly low level: less than half of European employees (48 %) work in enterprises with a security policy in place (23 %). This is despite consensus across security professionals that such a policy is an essential first step to ensuring adequate protection from growing security threats[38]. A lower still percentage of enterprises reports that they train their staff in security awareness (15 %), carry out risk assessment (15 %) or have put a security management system in place (19 %).

The percentage of individual users who have recently installed an anti-virus programme or used on-line authentication is still fairly low across the EU. The data show that there are still a relatively high number of unsafe, unprotected computers connected to the Internet.

---

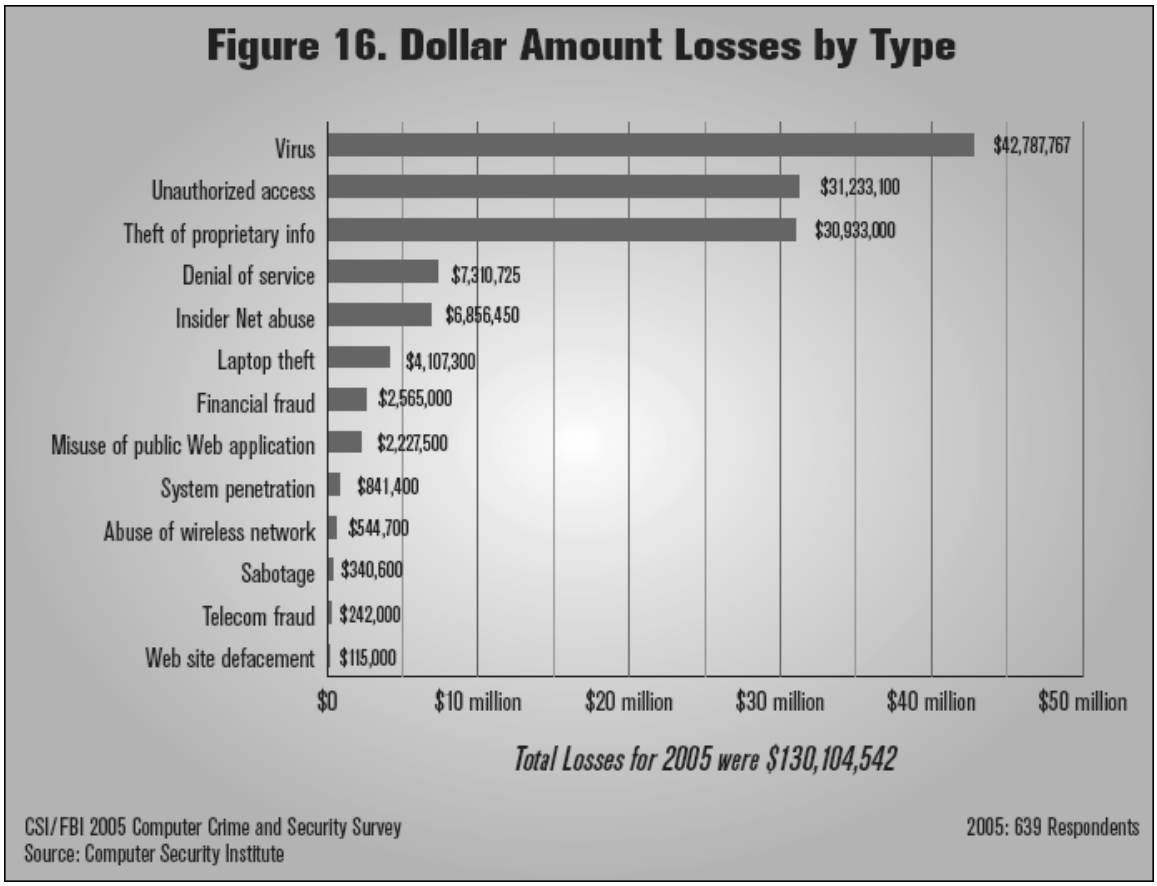
37 The European e-Business Market Watch "*ICT security, e-Invoicing and e-Payment Activities in European Enterprises*", Special Report, September 2005. The European Commission's e-Business W@tch monitors the adoption, development and impact of electronic business practices in different sectors of the economy in the enlarged European Union.

38 *Ibidem*, p. 40.



The ability (or the lack thereof) of both business and consumers to adequately respond to network and information security threats can have significant financial impact, as illustrated by the following data.

The recent CSI/FBI 2005 Computer Crime and Security Survey[39] gives the following estimates of financial losses caused by various types of security incidents:



[39] 10th Annual CSI/FBI Computer Crime and Security Survey 2005.

The cost of disruption to business processes is difficult to quantify. Impact may range from nuisance (employee's productivity hindered for a few minutes) through more serious disruptions (e.g. when a corporate network is closed for repair; this is particularly harmful for organisations that rely on permanent availability of the networks 24 hours a day, 7 days a week) through loss of business opportunities[40]. One study has grouped the types of risks an enterprise faces into six major categories, with average risks per year, average IT staff hours devoted to each security incident, and average collateral damage. Keeping track of security incidents and related costs can help justify security funds and predict the probability of future incidents[41]:

Typical Threats	Avg. Risk of Breaches per Year (per 1,000 users)	Avg. IT Staff Hours per Breach (Respond, Resolve and Forensics)	Avg. Business and Collateral Damage per Breach
Virus / Worms / Trojans	2	4 hours per infected asset	$24,000
Denial of Service	2 serious incidents	32 hours per system	$122,000
Data Destruction / Damage	1	120 hours	$350,000
Physical Theft Disclosure	1 in 4 former employees leaves with assets	2 hours	$5,000
Information Theft and Disclosure	1	180 hours	$250,000
Policy Violation	30	2 hours	$20,000
Errant User Behavior	15	2 hours	$20,000

Denial-of-service can be particularly nefarious for businesses relying on the Internet as they effectively aim at disconnecting networks or shutting down websites. Reportedly, this type of attack is increasingly used as an element of organised extortion schemes and has become the 4th most expensive form of computer-related crime in 2005, after virus, unauthorised access, and theft of proprietary information[42].

Another problem increasingly associated with computer security breaches may have very serious consequences both in terms of financial losses and societal impacts. Identity theft (ID theft) means the deliberate appropriation of another person's identity, usually to gain access to their finances (and for instance obtain loans and buy goods in the victim's name)[43]. Techniques for obtaining identification information range from the crude, such

---

40 "Security Breaches and the Cost of Downtime", a report by Endforce Inc., 2004.

41 *Ibidem*, quoting a report "Is There a Business Case for Security?" by Alinean, available at http://www.alinean.com/Newsletters/2004-3-March.asp

42 10th Annual CSI/FBI Computer Crime and Security Survey 2005.

43 http://en.wikipedia.org/wiki/Identity_theft. On the other hand, Assuming a false identity with the knowledge and approval of the person being impersonated, such as for cheating on an exam, is not considered to be identity theft. The UK Home Office Identity Theft Steering Committee proposes the following definitions: *Identity Crime* as a generic term for Identity Theft, creating a False Identity or committing Identity Fraud (a *False Identity* being either fictitious (i.e. invented) or a genuine identity that has been altered to create a fictitious identity); *Identity Theft* occurs when sufficient information about an identity is obtained to facilitate Identity Fraud, irrespective of whether, in the case of an individual, the victim is alive or dead; *Identity Fraud* occurs when a False Identity or someone else's identity details are used to support unlawful activity, or when

as stealing mail or rummaging through rubbish ("dumpster diving" in the US), stealing personal information from computer systems and networks, to infiltration of organizations that store large amounts of personal information.

Until recently, the term "identity theft" seems to have been more widely used in the United States than in Europe[44]. One reason could be that ID theft is usually the result of serious breaches of privacy whereas processing of personal data and protection of privacy is covered appropriately by European legislation. Another reason could be the widespread use of publicly available data (e.g. social security number or driver licence details) for identification in the United States[45]. However, governments like the United Kingdom now claim that ID theft is the fastest growing offence when using electronic communication services. It is estimated that more than 100 000 people are affected by identity theft in the UK each year, costing the British economy over £1.3 billion annually[46]. ID theft is also gaining an additional dimension in the light of the fight against illegal immigration, terrorism, and organised crime.

It is important to note that identity theft and related crime are not exclusively, or even predominantly, related to the use of the Internet or involve the use of computers. The US Federal Trade Commission reported in 2002 that only 13 % of victims of ID theft identified "transactions" as the mechanisms leading to the crime – and this covers both on-line and off-line transactions. On the other hand, it seems safe to assume that at least part of the cases is linked to attacks on computer systems and networks.

It is difficult to fully quantify the extent of *real* ID theft and consequently it is difficult to compile sound statistics. On the one hand, ID theft is often followed by other crimes such as fraud; on the other hand, it is hard to detect because personal data is not stolen physically but is "just" copied. Nevertheless, with the growing deployment of e-commerce, e-business and e-government services more and more personal data is transferred via electronic communications networks. This in itself could increase the risk of ID theft if the data is not sufficiently secured. In addition to eavesdropping during transmission or unauthorised access to information systems storing the data, *phishing* also carries threat of ID theft. Carefully designed and correctly implemented identity management solutions could provide a remedy. Of course, EU legislation in the field of data protection and cybercrime is likely to contribute to reducing the risk of ID theft. In particular, the recently adopted Framework Decision on Attacks against Information Systems requires Member States to criminalise illegal access to information systems

---

someone avoids obligation/liability by falsely claiming that he/she was the victim of Identity Fraud.

44 A 2003 survey by the US Federal Trade Commission showed that over a one-year period nearly 10 million people – or 4.6 % of the adult population of the country – had discovered that they were victims of some form of identity theft. See "Identity Theft Survey Report", September 2003, available at: http://www.ftc.gov/os/2003/09/synovatereport.pdf. Similar statistics for Europe are not available.

45 In the US, knowing the SSN of a person is often treated as sufficient identification that you are that person. The widespread use of both official and private databases which hold SSN opens the door to large-scale identity theft. In addition, geography and commercial habits in the United States have led to long-distance transactions being much commoner than in most of Europe, which may at least partially explain the spread of identity theft in the US. See "*Identity Theft. A Discussion Paper*", European Commission, JRC, 2004

46 Source: Home Office Identity Theft Steering Committee, http://www.identity-theft.org.uk/

which often constitutes an important element of ID theft-related crimes. In addition, Article 4(2) of the ePrivacy Directive (2002/58/EC) provides that the electronic communications service provider must inform the subscriber of a particular risk of a breach of the security of the network.

2.3. Justification for public intervention

Given the scope of security threats, a need to tackle these threats still persists. Moreover, the present trend towards convergence of networks and information systems puts current systems security solutions under more pressure and urges new solutions to be found.

The principal issue when designing an appropriate public intervention is first to ask whether there is a reasonable justification for public policy action (of regulatory or non-regulatory nature) or whether the security problems outlined in the previous section could be solved by market forces more effectively then by any public intervention. Only then it is reasonable to assess what kind of public intervention would bring best results at the lowest cost possible and also, whether it is desirable to proceed with actions at the EU level or leave the initiative to the Member States.

The reasons for public intervention are in this case both economic (market imperfections) and social (discouragement of some groups of users and lower take-up of ICT). As stated already in the previous Commission Communication on Network and Information Security [COM(2001) 298] and as it is also widely recognised in economic literature[47], there are market imperfections preventing the market itself from solving some of the security problems and causing these problems to persist or even grow bigger in time. The following text discusses the most common market imperfections, which can be encountered in relation to network and information security.

The first problem identified lies in the incentives of ICT systems producers including software developers to produce reliable systems and software with good security features. The speed of technological change encourages the highly competitive industry of equipment and software to launch new goods and services very quickly, whereas a thorough quality check including security tests would make the time-to-market much longer and costly. First-comers often win the whole market and the vulnerability of their goods and services is often discovered only after they are already well-established on the market. Typically, software producers would advertise new and additional features of their software to appeal to consumers, rather than security and robustness.

Secondly, there certainly exists a problem of asymmetry of information between users on one side and the ICT industry on the other side. Companies and even more consumers are often not fully aware of all the potential security risks because the systems and networks get more and more complex and the market does not reveal all the potential vulnerabilities and risks related to the systems or software. Many new services and applications have attractive features and can be easily accessed (e.g. downloaded) but while the benefits are visible to consumers, the security risks are not and they are usually only discovered later (if at all). Asymmetry of information (typically in the software

---

[47] See e.g. Ross Anderson, "*Why Information Security is Hard. An Economic Perspective*"; Hal R. Varian, "*Managing Online Security Risks*"; and other materials available at Ross Anderson's Economics and Security Resource Page at http://www.cl.cam.ac.uk/~rja14/econsec.html

market) could therefore sometimes lead to preference to more attractive, cheaper and less secure alternatives.

Companies and consumers generally invest less than an adequate amount in security measures making their computers and networks more vulnerable and prone to cybercrime, malicious attacks and other sorts of network disruptions.

The general problem of companies (and to lesser extent also consumer) is that they are not able to assess very precisely the security risks and the return on investment (ROI) in security. The problem with most information security investment is that the expected financial returns are very difficult if not impossible to predict. Designing strong security measures into the information system architecture of an enterprise can reduce its overall operational costs by enabling cost-saving processes, such as remote access and customer or supply-chain interactions, which could not occur in networks lacking appropriate security[48]. Therefore, there is a need to raise awareness of businesses and public administrations that they can benefit from increasing their level of information security.

Consumers do not have a strong incentive to invest in security measures. The problem is similar to the decision-making of companies. The user has to compare potential risk of a security problem with the time, effort and money devoted to security measures. The reasons for not taking any security measures can be twofold. The first reason is rather practical and awareness-related: the market for technologies and software changes very quickly and many individual users are not able or ready to keep pace with so many updates and changes. Some users are simply not aware that their ill-protected machines or systems can make vulnerable not only their system but the whole network or they do not know how to tackle the security problems. The second reason could be the "free-rider problem" when all users want to have a satisfactory level of security but not everybody is willing to pay the price since they are not entirely responsible for the consequences of their security behaviour (such as damage to other users' systems).

Network and information security is not only an issue of economic incentives and costs and benefits for those who are already using ICT. Our society is equally concerned with widening the ICT uptake, bridging the digital divide and achieving the highest possible level of eInclusion. There is of course a number of reasons for low ICT uptake in some groups of the society; however, reliable networks, secure systems and software and an adequate level of protection of information can contribute significantly to wider usage of ICT goods and services, which in turn brings also positive economic and social benefits for the society as a whole[49]. Concerns about security and low protection of data while using ICTs can discourage users from using new services and create a barrier for new, less knowledgeable and less experienced users with low awareness of ICT security issues.

Raising the general awareness of ICT security issues (and in particular of available countermeasures and best security practices) could also go a long way towards creating incentives. This applies in particular to individual users and consumers. The importance of raising security awareness has long been recognised among the Member States, as

---

48 See e.g. the US government "*National Strategy to Secure Cyberspace*", 2003.

49 For example in terms of broadening the possibilities for eGovernment and eHealth services .

well as at EU level. ENISA with its ad-hoc Working Group on awareness raising has an important role to play in this respect[50].

The above-mentioned examples of market imperfections and inclusion issues show that market in many cases fails to provide an appropriate level of network and information security and that this can also affect the ICT take-up by the general public. There is certain scope for public policy action which should not necessarily involve only regulatory measures.

Public policy action should always respect the principles of proportionality, creating the lowest possible burdens on economic actors and the overall effectiveness of the public intervention compared to the situation created purely by market forces. This Impact Assessment considers three main policy options the cost and impacts of which will be assessed more thoroughly in Section 5.

2.4. Is there a need for EU action?

The European Union has been active in the field of network and information security for many years now. The most important initiatives are briefly presented in the Annex to this report.

The potential for economic growth made possible by the technology revolution has not yet been fully realised. One of the reasons is reportedly the deterrent effect of security risks which not only affect transactions, but also jeopardize intellectual property, business operations, infrastructure services and consumer trust. The lack of coordination and co-operation in the field of network and information security results in fragmentation of security policies in different Member States, heterogeneous application of rules and solutions and ultimately low and diversified level of protection across the EU. So far there has not been a significant transfer of know-how between Member States as far as network and information security is concerned and it is a genuine interest of the Community to encourage the knowledge exchange and co-operation between governments, ICT industry and users concerned.

Cybersecurity or information security is approached from various angles by national governments and at international level, i.e. either as an IT security issue (strong focus on Internet security; implementation through technical means such as firewalls, anti-virus software, or intrusion detection software); as an economic issue (business continuity); as a law enforcement issue; or as a national security matter. It seems that, at present, the cybercrime / law enforcement approach has gained significant political momentum. The protection of critical information infrastructures is also high on political agenda[51]. In the European Union the network and information security concerns have traditionally been approached as an important internal market issue.

Internal market measures (including the existing regulatory framework for electronic communications) often require different forms of technical and organisational

---

[50] For the first deliverables, see the results of ENISA workshop on "Good Practice in Awareness Raising" available at: http://www.enisa.eu.int/deliverables/index_en.htm

[51] M. Dunn, *A Comparative Analysis of Cybersecurity Initiatives Worldwide*, a report prepared for the ITU WSIS Thematic Meeting on Cybersecurity, Geneva, 28 June 2005.

applications by the Member States and the Commission. These are technically complex tasks with no single, self-evident solutions. The heterogeneous application of these requirements can lead to inefficient solutions and create obstacles to the internal market[52].

The existing regulatory framework for electronic communications and data protection already provides for legal obligations for operators and service providers to ensure a certain level of security in communications and information systems. In order to maximise their effectiveness, these legal provisions need to be applied as consistently as possible across the Member States. A common understanding of the underlying security issues and the specific measures to be taken is a necessary prerequisite. Carefully designed policy measures can reinforce the existing market processes driving investments in security solutions and at the same time improve the functioning of the legal framework[53].

In order to respond to such challenges through ensuring an appropriate and effective level of network and information security for the benefit of the citizens, consumers, private and public sector organisations of the EU, thus contributing to the smooth functioning of the internal market, the European Network and Information Security Agency ENISA was established[54].

Due to the dynamic nature, challenges for the security of networks and information systems exist and new dangers seem to appear every day, in spite of the efforts already made. These include spam, spyware and other forms of malware, illegal content, and on-line fraud, including *phishing* and identity theft. Threats, both real and perceived, undermine consumers' confidence in Information Society and hamper its recognised potential for flourishing.

The conclusions of the recent High Level Research Seminar "Trust in the Net"[55] also indicated that there is a room for action at EU level to enhance network and information security in Europe. The participants called for coherent, multi-stakeholder discussions and actions, including research, certification and standardisation, regulation and **general policy strategies**, aiming at a true culture of security in the Information Society. Specifically, the following areas have been identified for further examination[56]:

---

52 There is evidence suggesting that network and information security markets have indeed remained confined to national boundaries of the Member States, see e.g. a recent report prepared for the French government "*La sécurité des systèmes d'information. Un enjeu majeur pour la France*", 26 November 2005, p. 76.

53 See also Commission Communication "Network and Information Security: Proposal for a European Policy Approach" - COM(2001) 298.

54 See Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency - OJ L 77, 13.3.2004, p. 1.

55 Organised by the Commission services jointly with the Austrian Presidency on 9 February in Vienna.

56 Report on the International High Level Research Seminar on "Trust in the Net", Vienna, Austria, 9 February 2006, available at: http://www.eu2006.at/en/Meetings_Calendar/Dates/February/0902TrustintheNet.html

A thorough societal debate is needed aiming at a balance between security, freedom and protection of human rights, including privacy;

The role of software manufacturers concerning their responsibility to produce, deliver and maintain secure and fault-tolerant software;

The role of ISPs with respect to the creation of trust in the Internet and the services they provide; and

A public-private partnership, including industry, research communities and public authorities to ensure the right balance between technology development, regulations and policy measures.

Network and information security are global issues that require concerted international efforts. Due to significant cross-border effects, most security threats cause negative cross-border externalities which cannot be effectively dealt with only at a national level. Instead, there is a need for closer cooperation at global level to improve security standards and information exchange, and promote a common global approach to network and information security issues, thereby contributing to the development of a culture of network and information security. European Union can play a significant role in fostering efficient cooperation with third countries and the global community. In addition, an orchestrated EU approach is necessary to avoid creating barriers to the internal market through deployment of non-harmonised security solutions.

3. OBJECTIVES

Security should be understood as one of the crucial elements of the Information Society enabling smooth development and deployment of new systems, applications and on-line services. More secure Internet and networks in general will then result in more citizens using Information Society goods and services. This in turn will contribute significantly to the Lisbon agenda objectives. In this context, the Commission initiative should create more awareness among the general public both about the potential of wide deployment of ICT and electronic communications networks, as well as about the potential security risks associated with their operation and use.

In order to successfully tackle the problems described above, the main objective to be pursued should be to raise awareness both on the opportunities and risks associated with the use electronic communication networks as well as on how the available security technologies, standards and processes could help to cushion the risks and seize the opportunities. To this purpose, there is a need to foster and enhance a culture of network and information security[57] for the benefit of consumers, businesses and public administrations. Moreover, the importance of network and information security and roles and responsibilities of all stakeholders in ensuring sufficiently high levels of network and information security in Europe should be emphasised and articulated, also by overcoming the diversity and fragmentations of existing approaches and keeping in mind the global dimension.

---

[57] A culture of security as promoted among others by the *OECD Guidelines for the Security of Information Systems and Networks.*

Achieving this objective would lead to more and wider knowledge on how to tackle the security problem, as well as more readiness of all stakeholders to take up their responsibilities. In particular, suppliers and vendors of software and ICT equipment and providers of electronic communications networks and services would have take up more responsibility for the quality and security features of the goods/services they offer. For instance, the banking world nowadays demonstrates that, despite the potential security problems in transmission networks it is possible to achieve consumer confidence by applying state of the art authentication and security mechanisms. These applications typically go through extensive testing before being released to customers.

In addition, the business community at large would understand better the potential benefits of investing in security. To this end, however, policy makers need to be sensitive to presenting security as a virtue and an opportunity, rather than as a liability and a cost. Security should always be perceived as a competitive advantage for businesses and as an essential quality for public sector service providers.

As a further result, we would expect the level of investments in security to rise, in particular in technologies for reliable and robust electronic communications networks, and in software and hardware security products. This, in turn, would certainly contribute to a yet wider take-up of ICT services and goods by citizens (eInclusion) and indirectly to achieving the objectives of the Lisbon agenda.

4. POLICY OPTIONS

The following available options for dealing with the complex problems set out above have been considered:

Policy option 1: "business as usual"

Choosing the option "business as usual" would mean a continuation of on-going activities in the area of network and information security.

In the first place, ENISA would continue to operate. It would pursue its activities on the basis of yearly work programmes. The Commission (alongside the European Parliament as well as certain national bodies) would continue to have the possibility to issue formal request to ENISA (based on Article 10 of ENISA Regulation).

The R&D programmes related to network and information security would be carried out, as planned[58]. The same would apply to other activities, whether of regulatory nature or not, that might currently be under consideration, both at EU level or within Member States.

However, all these activities would be pursued in isolation, without further attempts to identify possible overlaps and/or synergies that could be exploited at EU level.

[58] See also description of current EU activities in the Annex.

Policy option 2: coordinated action

This option would mean pointing a strategic way forward by providing an "umbrella" for the various processes already under way at various levels (including among Member States and other stakeholders, as well as within the European Commission).

It would involve an open dialogue that would result in a clear set of priorities and enable a result-oriented, coherent, European approach in partnership with all stakeholders while leaving the door open to both possible "soft law" measures, as well as to legislative action (such as the one that may result from the 2006 review of the regulatory framework for electronic communications.

Policy option 3: purely regulatory

Choosing this option would mean taking a radical, purely regulatory approach in order to create (or improve) some incentives to achieve increased network and information security through legislative measures only.

To invigorate the debate, the legislative process would commence with a Communication. Depending on the outcomes of the Communication, and in particular of the subsequent discussions with the other Institutions, the Commission would decide on further legislative action (which could take the form of recommendations or even directives).

5. ANALYSIS OF IMPACTS

The main impact sought is enhancing security of networks and information systems in the long run, thus improving the reliability of ICT that are so critical to the quality of life and economic wellbeing of modern societies.

In the short term, the action should result in better awareness of the public in general, and policy makers in particular, of both the benefits and opportunities offered by increasing use of electronic communications services and networks, including the Internet, as well as the associated risks and effective methods to address them. This in turn would contribute to the establishment of a true "culture of security" across the European Information Society.

Below the major economic and societal impacts of each of the considered options are briefly set out. Given the subject matter of the proposal, there are no likely environmental impacts to consider.

5.1. Policy option 1: "business as usual"

In the short term, the "business as usual" option seems neutral in terms of impacts on competitiveness, trade and investment flows. However, it is possible that negative consequences for competitiveness would appear in the long term. In the first place, choosing this option would imply that no specific response is sought to the currently observed change in the "threat landscape", as well as to new and emerging security

threats. Such an approach could result in exacerbated security challenges in the future that could adversely impact European businesses and users.

In addition to the shift towards increasingly serious security threats (such as targeted attacks of criminal nature, as described above in 2.2), there are also other changes that risk to undermine the feasibility of continuing the current approach to network and information security. In particular, the advent of ambient intelligence (or "ubiquitous computing"), using technologies like RFID, is likely to pose new risks and challenges. Also, convergence of networks and services together with a growing number of actors on the electronic communications markets (result of the progressing convergence) pose additional challenges for policy makers and call for adapted response.

Continuing the current approach would also be unlikely to alleviate the risk of fragmentation of the internal market. Reportedly, such fragmentation exists already and is likely to persist if Member States continue to take differing approaches to network and information security. As a side effect of such a fragmentation, the European security services and goods markets are likely to remain dominated by a limited number by non-European players. This would leave the European ICT security industry (coping with divergent national rules and requirements) at a disadvantage compared to their non-European counterparts (who would be able to impose de facto standards anyway). It is also likely to be detrimental to the overall competitiveness of the EU as a whole.

The truth that network and information security "is only as good as the weakest link" applies also to the European, multi-nations situation. At present, network and information security issues are high at the political agenda in many Member States. However, some other Member States are less prepared (or not so well equipped) to give these issues the attention they deserve. There might be many reasons for that, ranging from insufficient awareness among the public and/or policy makers, through lack of adequate resources (that need often be devoted to other issues of "higher priority"). Unfortunately, as a result of such discrepancies, the EU as a whole becomes weaker and more vulnerable, as threats and risks – just as modern ICT networks - do not respect national boundaries.

Network and information security is borderless and in essence a global issue. However, if discussions at international level are to be fruitful, it is essential to establish a common position at EU level so that the Community interests could be defended as appropriate. Lack of coordination at EU level could lead to weakening of the EU position in international fora dealing with information security issues. In view of the global nature of cybercrime and other threats, carrying on isolated (national) approaches to network and information security could also result in increased vulnerability to external attack on EU information infrastructures and systems.

As indicated earlier, the current state of network and information security risks to undermine the already fragile trust and confidence of users of electronic communications networks and services. No significant (positive) change in this respect could be expected if no change in policy were made. This in turn would result in the continuing exclusion of some user groups from the use of ICT and the Internet in particular (and deprive them of related benefits), at least partly due to lack of trust and lack of understanding of security issues.

Indeed, choosing the first option would amount to stating that the level of network and information security in the EU is satisfactory and no further public action is needed. This would be in contrast with the problem description in Chapter 2 above. The growing importance of information systems and networks in daily life of our society results in more and more valuable information (personal data, trade secrets, financial information) being available on computers and networks, thus rendering them an attractive target for criminals. In addition, most of what can be called "critical information infrastructure" is currently in private hands. Inadequate security measures taken by private owners could cause serious problems to other network users. Moreover, it seems that the market does not at present provide sufficient incentives to stimulate adequate security measures. This can be partially due to underreporting of security incidents by organisations and companies that fear damage to their reputation, loss of customers or revenue or political repercussions. A carefully considered government action might seem justified to remedy these problems.

For these reasons, the "business as usual" option seems undesirable, given in particular the social and economic issues at stake (the new Lisbon agenda), as well as the associated risks of market fragmentation at EU level. In addition, it might put at risk the potential benefits from the Information Society.

5.2. Policy option 2: coordinated action

Should the second option be chosen, network and information security issues would be put firmly on the European policy agenda. Coordinated approach to network and information security at EU level (within the Commission and with Member States) would allow developing significant synergies and avoiding potential overlaps.

In this scenario, the role of the European Commission as a representative of the Community interest would be to establish a basic set of rules to be respected by all the actors, bring the actors together, discuss the most efficient strategies for security management and provide an effective liaison with the rest of world. Such a dialogue could take form of a (series of) public consultation(s) organised by the Commission. The consultation process would lead up to a consensus on a list of clearly defined priorities and actions to be taken at various levels (i.e. EU, national level, regional level etc.) and involving the various stakeholders as well as ENISA. Through this type of coordinated action a true culture of network and information security could be promoted in Europe.

It goes without saying that ENISA would have an important role to play in this quest towards a culture of security. As an independent Agency, it would pursue its activities, as defined in the ENISA Regulation 460/2004, as well as in its work programme adopted every year (which should be consistent with the Community's legislative and policy priorities in the area of network and information security[59]). In addition, the Commission might use its right to issue a formal request to ENISA for advice and assistance, in accordance with Article 10 of the ENISA Regulation 460/2004, as appropriate. This would allow for the Agency to reaffirm its role as the centre of expertise on the one hand, and provide added value through greater coherence in policy making at EU level

[59] Article 6(8) of the ENISA Regulation 460/2004.

Moreover, the Commission activities in the field of anti-spam, cybercrime, protection of critical information infrastructure would be pursued in a coordinated manner. This is of paramount importance due to the growing complexity of the issues at stake and push of the convergence of the communication technologies and networks that has changed the landscape of market sectors with blurring boundaries.

Importantly, the coherent approach would encompass the on-going and planned legislative actions at the EU level, such as the 2006 review of the regulatory framework for electronic communications. This would enhance the visibility of the provisions of the regulatory framework related to network and information security and highlight the importance of these provisions and of their correct transposition and effective application in Member States' domestic legal systems.

It cannot be excluded that, as a result of the broad consultation process described above, a need arises for more specific action to be taken at EU level. The Commission might then consider the possibility of using alternative methods of regulation, such as co-regulation and self-regulation[60]. Soft-law instruments, such as recommendations, could also be considered. Recommendations could be based on relevant provisions of the EC Treaty[61] or, alternatively, on provisions of the regulatory framework for electronic communications[62].

In addition, regulatory measures considered necessary as part of the strategic approach to security in electronic communications would be pursued in the context of the upcoming review of the regulatory framework for electronic communications (including the ePrivacy Directive 2002/58/EC.

In particular, Article 4 of the Directive on privacy and electronic communications imposes on providers of publicly available electronic communications services an obligation to take appropriate technical and organisational measures to safeguard security of their services[63]. Moreover, Article 23 of the Universal Service Directive covers

---

60 As defined in the Interinstitutional Agreement on better law-making of 16 December 2003 - OJ C 321, 31.12.2003, p.1.

61 E.g. Articles 249 or 211 EC Treaty (Commission recommendations); Article 157 EC Treaty (recommendations from the European Parliament and the Council).

62 Pursuant to Article 19 of Directive 2002/21/EC on a common regulatory framework for electronic communication networks and services (Framework Directive), the Commission may issue recommendations to Member States on the harmonized application of the provisions in the Framework Directive and the specific directives (including Directive 2002/58/EC on privacy and electronic communications) in order to further the achievement of objectives set out in Article 8 of the Framework Directive, such as *ensuring the development of consistent regulatory practice and the consistent application* of the Framework Directive and the specific directives.

63 As for network security, an analogous obligation rests upon providers of public communications networks. Security measures taken in accordance with this provision must ensure a level of security appropriate to the risk presented, having regard to the state-of-the-art and the cost of their implementation. In addition, service providers who offer publicly available electronic communications services over the Internet are obliged to inform users and subscribers about particular security risks, as well as about measures they can take to protect the security of their communications (for instance by using specific types of software or encryption technologies). The requirement to provide information does not discharge a service provider from the obligation to take, at its own costs, appropriate and immediate measures to remedy any new, unforeseen security risks and recover the normal security level of the service. On the contrary, the information obligation does not cover situations where a breach of security actually occurs.

requirements with respect to the integrity of the public fixed telephone network and its availability in the event of a catastrophic network breakdown or *force majeure*. As a result of the 2006 review it would be appropriate to consider whether additional security requirements should be imposed on electronic communications service providers and network operators. In particular, consideration would be given to: more specific technical and organisational measures to be taken by service providers; provisions dealing with the notification of security breaches; and specific remedies and penalties regarding breaches of obligations.

In the area of EU cybercrime legislation, the latest development was the adoption of the Framework Decision on attacks against information systems in February 2005. This third-pillar instrument addresses the most common forms of criminal activity against information systems and provides a comprehensive framework of common definitions and criminal sanctions. Member States have to transpose the provisions of the Framework Decision into their national legal systems by 16 March 2007.

Moreover, a coherent approach would enable Member States and other stakeholders, including industry, civil society and public administrations to better understand their responsibilities. This in turn would allow them to better fulfil their duties and seize the opportunities offered by more secure and flourishing electronic communications networks and services.

If successful, i.e. adopted by the Member States and followed up by a set of coherent policy actions in specific areas (such as prevention of security incidents, information infrastructure resilience, business continuity etc.), this option would likely have significant positive economic impact, in particular in terms of increased competitiveness and productivity, as well as research and innovation. In addition, a positive societal impact is expected, as citizens' confidence in the use of ICT in general grows and the benefits offered by these technologies are finally fully exploited.

All in all, the "coordinated action" option seems to offer a promising perspective and added value through bringing more coordination and coherence to the many activities and processes under way in the area of network and information security.

5.3. Policy option 3: purely regulatory

Given the description of problems and analysis of the need for public intervention (market imperfections and eInclusion), some might argue for a radical, command-and-control approach that would attempt to change the incentives of individual market players through binding regulatory provisions. Theoretically, this could be done through defining and assigning some sort of responsibility to different actors in the hope of creating the right incentives and the right level of security for all. Legislative action can range from imposing some security-related obligations, e.g. on entities processing personal data, up to radical solutions such as making both users and ICT suppliers liable for their security products, behaviour and breaches.

It should be kept in mind that, as indicated above, many legislative processes are already under way at EU level in areas related to network and information security. One example is the 2006 review of the regulatory framework for electronic communications which might result in amendments to the security-related provisions of the ePrivacy Directive

2002/58/EC or the Universal Service Directive 2002/22/EC. Finally, the Commission issued proposals for directives that would bring network and information security more firmly within the remit of corporate governance responsibilities[64].

Against this background, any new legislative proposal would need to ensure that no potential conflict arises with the processes already under way. In addition, economic and societal impacts of new regulatory provisions would need to be carefully assessed.

Moreover, regulatory action could be considered in other areas, not covered by the policy initiatives indicated above. However, it is not yet clear at this stage what exactly form could such regulatory action take. Further consultation with all stakeholders would be needed in order to gather supporting evidence and clearly defined the regulatory options available. For this reason, the analysis of impacts of the purely regulatory option in the present report can only be of a very preliminary character.

Generally speaking, purely regulatory approach does not seem the most efficient way to reinforce the culture of network and information security. Experience shows that the real difficulty often lies in correct implementation and effective enforcement of regulatory provisions in the Member States. New legislative measures as such could risk exacerbating that difficulty.

On the other hand, regulatory measures accompanied by some form of coherent approach aiming at better implementation and more uniform application of regulatory provisions across the Member States could provide great added value. This is generally true both for existing and new regulatory initiatives. In any case, regulation seems to produce the best

---

64 Recent high-profile scandals involving publicly listed companies in the US and in Europe have resulted in new regulatory requirements on businesses, such as the Sarbanes-Oxley Act in the US and the new banking regulation arising from the Revised International Capital Framework, also known as Basel II. Such regulations make Boards of Directors responsible for, among other aspects of corporate governance, managing key risks to their business, including information risks. At the same time, while "traditional" risks (like credit or market risks) are usually well understood and managed, the more recent and dynamic risks are posing a bigger challenge to organisations. According to Ernst & Young most recent global information security survey, compliance with regulations such as Sarbanes-Oxley Act has become a primary driver or information security. Under Section 404 of the Sarbanes-Oxley Act, an annual report of a US-listed company must include an "internal control report". The report not only has to state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting, but must also contain an assessment of the effectiveness of the internal control structure and procedures. Chief Executive Officers (CEOs) and Chief Financial Officers (CFOs) are individually responsible to the company, its shareholders and third parties for the accuracy of their company's financial statements (and thus also for the internal control report). In the European Union, the Commission proposed recently that all EU-listed companies should provide a corporate governance statement in their annual report. In addition, the new draft 8th Directive on Statutory Audit will require audit firms that carry out statutory audit(s) of public interest entities to publish on their website an annual transparency report that includes, among others, "a description of the internal quality control system of the audit firm and a statement by the administrative or management body on the effectiveness of its functioning". Both directives are likely to be adopted in the course of 2006 [see Proposal for a Directive of the European Parliament and of the Council amending Council Directives 78/660/EEC and 83/349/EEC concerning the annual accounts of certain types of companies and consolidated accounts - COM(2004) 725; and Proposal for a Directive of the European Parliament and of the Council on statutory audit of annual accounts and consolidated accounts and amending Council Directives 78/660/EEC and 83/349/EEC - COM(2004) 177].

results when it is part of a "package" rather than attempting to constitute the "silver bullet", stand-alone solution to a complex set of issues.

According to the Commission's "better lawmaking" approach, legislative activities may only be undertaken when sufficient evidence of failure of other less interventionist options is in place. At present, there seems to be insufficient evidence that the security problems could be adequately addressed by a new legislative initiative at EU level at this stage. Instead, it seems that maximising the effectiveness of existing legislation by ensuring its consistent application across the Member States could be an advisable first step (without precluding the possibility of amending or adjusting the existing regulatory measures, if necessary)[65].

The table 1 below sets out the main likely impacts arising from each of the three policy options.

[65] It need to be stressed that nothing in the present report should be interpreted as precluding the outcome of the processes currently under way at EU level which might result in amendments to existing rules or even in new regulation with implications for network and information security (e.g. the 2006 review of the regulatory framework for electronic communications; the work on critical infrastructure protection, or combating cybercrime).

	Options		
Impacts	(1) "Business as usual"	(2) Coordinated action	(3) Purely regulatory
Economic			
Competitiveness & investment	Neutral, no big changes in a short term, however, could bring more security challenges in the future if only the existing framework and activities are preserved (e.g. security challenges related to wireless technologies, Voice over IP, emerging technologies etc. might not be covered) ➔ possible negative consequences on competitiveness in the long term; Risk of fragmentation of security efforts, different approaches in different MS leading to obstacles to the internal market and loss of competitiveness of the EU as a whole; Widening of differences between well-equipped countries and those where security risks are ignored, not enough attention paid to security in some countries ➔ possibility of spreading the risk to other countries as cybercrime is borderless; Low incentives of the private sector to invest in security	Increased investment in security in the public and private sectors through raising awareness of security issues; Appropriate mix of self-regulation, co-regulation and cooperation to deal with agreed priorities; Potentially also increased competitiveness if security risks are properly assessed, security challenges dealt with and harmonised approach to security fostered (including through standardisation and certification); Potential economies of scale and increased effectiveness resulting from a coherent approach rather than inconsistent initiatives of individual actors (e.g. wider adoption of security standards, etc.)	Additional regulatory burden on enterprises (in terms of higher administrative and compliance cost) could have a negative impact on competitiveness of EU industries; Positive: if properly enforced, could create incentives for companies to invest more in security and help raise awareness of security problems;
Innovation and research	No significant transfer of know-how between governments; exchanges made more on a reciprocal basis; which	Co-operation efforts will bring more attention to R&D and innovation of security goods and services. It will be easier to incorporate	More legislation could stifle innovation and create market distortions;

	Options		
Impacts	(1) "Business as usual"	(2) Coordinated action	(3) Purely regulatory
	does not help reduce disparities; Cooperation in the development of government security products is rare, lack of coordination = non-interoperability in the supplied security goods/services, in terms of both relationships with suppliers who are in a position of quasi-monopoly and support for the development of open-source software Possibly less incentives to provide more inside into the future challenges resulting from the complexity of networks and information systems;	security aspects in every stage of design and deployment of network infrastructure, applications and software; Security industry will become a fast growing market e.g. with faster roll-out of secure versions of IP and electronic signatures	On the other hand, it could stimulate the market for assessing risks and transferring them to insurances; Some claim that there's not enough incentive from the market to stimulate adequate security measures;
Administrative and compliance costs for businesses, citizens and public authorities	No significant change	Compliance costs could increase in some cases for businesses (e.g. standardisation or certification); There is some additional administrative cost incurred in coordination (organising public awareness campaigns, coordination meetings with stakeholders and exchange of best practices between Member States). However, this cost is likely to be significantly lower than the administrative and regulatory burden imposed in the case of legislative action.	Likely higher administrative and compliance costs for businesses if required to report every security breach + higher administrative costs related to the legislation already in the pipeline (a corporate governance statement required by the corporate governance legislation, annual transparency report required by the new draft of the directive on Statutory Audit); Citizens could be economically affected in terms of companies passing (some of) the additional administrative and compliance costs on to them; Increase in

	Options		
Impacts	(1) "Business as usual"	(2) Coordinated action	(3) Purely regulatory
			administrative burden for public authorities by having to transpose the new legislation and ensure its proper enforcement.
Citizens and consumers	Negative side-effects for consumers due to different security standards, products and law enforcement in different countries, different level of awareness of security issues among consumers from different countries;	More awareness of security issues, benefits from using more secure technology, greater choice of security goods and services; Increased confidence in ICT	More attention paid to security of services, applications, networks and goods but only if new security legislation properly enforced. Prices of goods and services could go up in the short-term as companies pass a part of their increased cost to the consumer
Overall impact on companies	Different approaches to security will provoke different reactions in companies with a tendency to invest less in security and not to reveal security problems (fears of loss of consumers' confidence, etc…), additional cost of compliance with different approaches in different MS Continuing problem of low incentive of companies (especially SMEs) to invest in security, limited promotion of the "culture of security" outlined in the OECD guidelines in the private and public sectors.	More awareness and more economic incentives to invest in security EU-wide; Encouragement of co-operation and self-regulatory, voluntary efforts; Open discussion about future challenges in security and risk management.	Possible positive impact on companies producing security goods and services (enhancing demand); Higher cost for companies investing in security (especially for SMEs), however, positive impact in the long term as the increased security starts paying off (increased reliability, customer's confidence)
The macroeconomic environment	No significant change in the short term, but potentially negative impact on the economy as a whole as new security challenges emerge and are not	If coordination action properly conducted, the overall level of network and information security will be enhanced, which may have a positive impact on take-up of ICT services, increase in	Even if well enforced, the new legislation would solve the problem only partially – imposing additional burden on businesses and thus encouraging them to

	Options		
Impacts	(1) "Business as usual"	(2) Coordinated action	(3) Purely regulatory
	being tackled in a coherent way.	productivity (also due to reduced number of security breaches) and ultimately on economic growth; Risks of lowering the positive effects of coordination actions if stakeholders are not sufficiently committed to achieve the proposed goals or if the Commission does not achieve sufficient coordination of actions internally and externally.	invest more in security. However, it solves neither the issue of security flaws in software, ICT equipment and networks, nor the underinvestment and low awareness of consumers. Therefore, the impact on ICT take-up, productivity and growth is likely to be minimal.
Social			
Employment, labour markets	Heterogeneous and interoperable environment might become a disadvantage (in the short term) compared to Asia-Pacific and US. Missed opportunities might be a disadvantage (in the long run) due to latency in a very dynamic and global market.	Potentially more employment in the area dealing with security goods and services and in the area of multilateral coordination of security efforts	Might have positive effects on employment in companies producing security goods and services
Social inclusion	No significant impact. Some groups of the society will remain excluded from use of ICT systems and services, partly due to lack of trust in ICT and lack of understanding of security issues.	Culture of security promoted and fostered through coordination will result in higher confidence of citizens in the use of ICT and higher awareness, which in turn can have positive impact on eInclusion.	Legislative measures targeted principally at companies are not expected to have direct impact on social inclusion. They may improve the awareness of consumers of security issues and their implications for privacy and data protection.
Privacy/personal data	No standardisation of electronic authentication and ID management techniques, less interoperability and coherence of IDM in different MS, low deployment of electronic	Positive impact because of a stimulated market for security technology, a promoted security culture and the provision of privacy enhancing technologies.	Positive impact if existing legislation is better enforced.

	Options		
Impacts	(1) "Business as usual"	(2) Coordinated action	(3) Purely regulatory
	signatures;		
Crime, terrorism, State security	Cybercrime and terrorism are global problems, therefore a not answered need for concerted efforts and international/global cooperation to tackle the increasing complexity and vulnerability instead of an isolated national approach might result in an increased attack potential.;	More awareness, increase in the exchange of best practices in security and risk management; lower rate of incidents/higher rate of emergency response if efforts coordinated not only at EU level but also internationally/globally	New regulatory measures tackling problems of security of networks (especially security of network infrastructure) can improve resilience and robustness of networks
Environment	N/A	N/A	N/A

6. COMPARING THE OPTIONS

As a result of the analysis, the first option ("business as usual") has been dismissed as inadequate to the challenges at stake and unlikely to efficiently contribute to the achievement of the set objectives.

Firstly, choosing this option would amount to de facto admitting that the present level of network and information security in the EU is considered to be satisfactory and that the existing measures do not necessitate further public policy action at EU level.

On the other hand, in spite of the new trends depicted in earlier sections (and in particular the noticeable change in the threat landscape) it is unlikely that – without a Commission initiative to this end - an adequate response to the existing and new challenges would be sought (or developed) at EU level. In particular, there is no evidence that the first option would lead to better alignment of national security policies or to any attempts to establish common priorities and actions to be taken at EU level.

Similarly, choosing the purely regulatory approach (option 3) would not be likely to produce positive results. The main reason for this is the complexity of the issues at stake which are unlikely to be resolved through legislative measures only. Rather, as already acknowledged by various fora (including the OECD), fostering a true culture of network and information security requires a set of coherent actions ranging from raising awareness, through research and developments, through creating an adequate policy framework, including – but not limited to – regulatory actions. In addition, as indicated above, a number of processes are currently under way at EU level which could result in new (or amended) legislation with network and information security implications. Proposing new regulatory measures at this point, without awaiting the outcome of the on-

going processes would therefore require careful consideration, in particular in view of the "better regulation" approach of the Commission. At the very least, proposing any new legislation at this stage would require careful consideration in order to avoid any potential conflicts with these on-going processes.

The description of the trends in information security (section 2.2), as well as the analysis in section 2.3 above suggest that, at present, market forces alone fail, in many cases, to provide an appropriate level of network and information security. There is certainly scope for public policy action, the scope of which would take into account the nature and scale of the problem as well as the types actors involved.

As indicated above, many processes are under way that may influence the status of network and information security in the EU. These issues are, however, difficult to understand and address for several reasons, perhaps most notably because of the sheer size, complexity and interconnectedness of the information infrastructure and associated technology, applications and services. Therefore, there can never be a "silver bullet", a single "one-size-fits-all" solution, no single answer to all open questions. Rather, there is a need for a more structured approach with clearly set priorities. The Commission has already taken such an approach in dealing with specific security-related issues such as spam[66].

This is a compelling argument in support of the second option which calls for a more structured approach with clearly set priorities ("coordinated action"). Choosing this option would provide an adequate response to the complexity of the problems related to network and information security through coordination of activities at various levels.

The first level of coordination to consider is between Member States. Alignment of network and information security policies between Member States would, in the first place, allow for exploring possible synergies. In addition, it would help avoid fragmentation of the EU internal market for security.

Secondly, coordination should be sought among the various stakeholders, including industry, public administrations, and citizens/users (e.g. represented by civil society groups). Such coordination would hopefully result in a set of common priorities, which in turn is a prerequisite to efficient and effective building of a culture of security. In addition, if an approach to network and information security is to be successful, all stakeholders (including public and private sectors, as well as representatives of civil society) would need to recognise and take up their responsibilities.

To this purpose, there is a need to establish a structured process of consultation and dialogue with relevant stakeholders. More coordination of stakeholders should be achieved. This is due to the fact that all actors are co-responsible for creating (or failing to create) a culture of security. A true culture of network and information security can only be achieved with a strong participation of the parties concerned – consumers, enterprises, organisations, producers of security equipment and public administrations.

---

66 See COM(2004) 28.

Network and information security is a broad policy area that has traditionally been approached from various angles and which should be seen in the context of the existing policies for electronic communications networks and services, privacy and data protection, and cybercrime. The European Union (as well as the Member States) has a long-standing tradition of handling those various aspects separately, but in a coordinated manner (e.g. the situation in 2001 where two communications, on network and information security, and on cybercrime, were prepared in parallel)[67].

It is of utmost importance that these initiatives are carried out in a coherent way. This coordination would be provided by an "umbrella" Communication provisionally entitled a "strategy for a Secure Information Society". This would allow the Commission to convey to the public a coherent message while addressing the various aspects of network and information security, i.e. the regulatory framework (including anti-spam activities and the protection of personal data and privacy), as well as cybercrime.

7. MONITORING AND EVALUATION

In order to measure progress of the security strategy or even in order to decide whether a stronger legislative measure would be appropriate, it is necessary to put in place an efficient and comprehensive evaluation and monitoring system. European policy in the information security field is often articulated in terms of "trust" and "confidence". Even though these issues are crucial for the effective uptake of new technologies and the development and growth in the Information Society, they are very difficult to measure. "Trust" in particular has many aspects, often not possible to define in a measurable way. Due to its multidimensional character it is not a viable indicator for the assessment of policies.

Although there are some data being collected on information security (for example within the framework of eEurope 2005), there is not a systematic monitoring of key security performance indicators in individual Member States. One way of helping Member States and other stakeholders co-ordinate their efforts and learn from each other would be comparative benchmarking exercise, comparing a set of key indicators[68] and revealing best practices across Member States. The proposed key indicators will be periodically collected, analysed and published.

A list of specific performance indicators that would allow for effective monitoring and evaluation of the impact of the proposed policy initiative could be one outcome of the broad multi-stakeholder dialogue, including public consultations, that would be outlined in the proposed Communication. The indicators should take into account the specific needs of each of the stakeholders groups (i.e. citizens, businesses and public administrations) and the particular challenges they are facing.

---

67 Communications: "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime" - COM(2000) 890 (January 2001); "Network and Information Security: Proposal for A European Policy Approach - COM(2001) 298 (June 2001). See also the graphic representation of the relationships (and overlaps) between the related policy domains in Part 2 (p. 5 above).

68 ENISA could play an important role in developing a set of adequate indicators. A relevant request to the Agency could be issued by the Commission to this effect.

The following preliminary set of key indicators could be considered[69]:

- *Percentage of individuals with Internet access having encountered security problems;
- *Percentage of enterprises with Internet access having encountered security problems;
- Percentage of public administrations with Internet access having encountered security problems;
- Financial losses due to security breaches (mainly for companies);
- Presence and type of security policies;
- *Percentage of individuals, enterprises [and public administrations] having taken ICT security precautions (defined separately for consumers and enterprises) within the last 3 months;
- Awareness of security features of websites;
- Concerns regarding on-line security;
- Propensity to report incidents (with or without assurance of anonymity);
- Importance of security features of websites on consumers' propensity to shop on-line;
- Number of secure servers per million inhabitants (OECD source);
- Investment in security – as % of enterprises' total investment;

** Indicators marked with an asterisk are already collected by Eurostat as part of the eEurope 2005 benchmarking exercise*

Some of these indicators are collected by Eurostat on a regular basis, others have to be collected by means of an ad hoc study or public survey (commissioned by the Commission). A formal request for assistance to ENISA could also be considered.

In order to achieve better enforcement of the EU security legislation, security experts from individual Member States will meet regularly to discuss and exchange views on *inter alia* national strategies for NIS, including non-regulatory measures taken to raise awareness, priorities for EU action (coordination with ENISA, etc.) in specific domains of security, etc.

With regard to legislation, the Commission is reviewing in 2006 the existing regulatory framework for electronic communications, including the security-related provisions of

---

[69] An attempt to identify viable indicators that could be used to measure progress in the area of trust and information security was made by SIBIS, a project funded by the European Commission under the IST Programme (1998-2002).

Directives 2002/58/EC and 2002/22/EC. ENISA has been requested to collect from Member States information on measures adopted by service providers to comply with the requirements bearing on providers of electronic communications services to implement technical and organisational measures to safeguard the security of their services (including measures to fight against spam, spyware and other forms of malware). The results of this survey are expected to provide an overview of the current overall status of the implementation of existing legislation and indicate whether steps need to be taken to improve enforcement of European legislation at Member States level.

Meetings with stakeholders should help promote as well as get commitment of key players in private sector to a culture of security by raising awareness, encouraging standardisation and certification and promote best practice at company-level.

ANNEX

Brief description of recent and on-going European Community initiatives related to network and information security

Network and information security is an extremely complex and continually evolving area. The EU has been active in the field for a number of years now. The most important recent initiatives are briefly described in the following paragraphs.

In 2001, the Commission issued a Communication "Network and Information Security: Proposal for a European Policy Approach"[70]. It recognised the growing importance of security in a world where communication and information have become a key factor in economic and societal development and the society is increasingly relying on data and services supported by communications networks and information systems. As everybody, including consumers, businesses and public administrations, want to exploit the possibilities of communications networks, security has become a prerequisite for further progress. The Communication proposed a series of actions to improve security of networks and information systems, including relevant provisions in the regulatory framework for electronic communications and new cybercrime legislation.

EU activities specifically in relation cyber-crime include the January 2001 Communication on "creating a Safer Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime"[71] which was the first comprehensive EU policy statement on the issue and proposed the establishment of an EU Forum on Cyber-crime and a regulatory proposal to deal with attacks against information systems. In February 2005, the Council adopted the Framework Decision on attacks against information systems[72], thus successfully concluding a legislative process of three years. The Framework Decision is a third-pillar instrument[73] that addresses the

---

70 COM(2001) 298.

71 COM(2000) 890 creating a Safer Information Society by improving the Security of Information Infrastructures and Combating Computer-related Crime.

72 Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems - OJ L 69, 16.3.2005, p. 67.

73 It should be noted that, following a judgment of the European Court of Justice of 13 September 2005 (Case C-176/03 Commission v Council) concerning the choice of legal basis for criminal sanctions, the legal basis of the Framework Decision will have to be changed, see the Communication from the Commission on the subject - COM(2005) 583.

most common forms of criminal activity against information systems, such as hacking (under the heading "illegal access to information systems"), denial-of-service attacks ("illegal system interference"), virus attacks, website corruption, and spreading of Trojan horses, worms and other malware ("illegal data interference"). It provides a comprehensive framework of common definitions and criminal sanctions for offences, provided that they are committed "intentionally" and "without right". Aggravating circumstances include committing the offence within the framework of a criminal organisation or offences that have caused serious damage or affected essential interests. On the contrary, actions of recklessness or even gross negligence, but no intent, are not criminalised.

In order to enhance the capability of the Community, the Member States and consequently the business community to prevent, to address and to respond to major network and information security risks, the European Network and Information Security Agency (ENISA) was established in 2004[74]. On 1 September, 2005, a new chapter started in the life of ENISA: the Agency moved to its new headquarters in Heraklion and newly hired staff took up their duties. ENISA now has 38 staff and can be considered fully operational.

The Agency will build on national efforts to enhance security and to increase the ability to prevent and respond to major network and information security problems. It should be able to provide assistance in the application of EU measures relating to security, for example to the Computer Emergency Response Teams (CERTs) of the Member states. This will help ensure interoperability of information security functions in networks and information systems. The activities of the Agency will consist primarily in advisory and co-ordinating functions. It will ultimately serve as a centre of competence where both Member States and EU Institutions can seek advice on matters relating to security. To date, the Agency established a Permanent Stakeholders Group comprising 30 members from industry, consumer organisations and the academic world, as well as 3 ad-hoc Working Groups (on Awareness Raising; CERT (Computer Emergency Response Teams) Cooperation and Support; and Risk Assessment and Risk Management). The Agency has also participated in and co-organised a number of conferences, workshops, and seminars dealing with network and information security issues.

The Commission communication in June 2005 entitled "i2010 – A European Information Society for growth and employment" also identified the need to take additional steps to ensure trustworthy, secure and reliable ICT which are crucial for a wide take up of converging digital services. This would include the need to help ensure a safer Internet, dealing effectively with fraudsters, combating harmful content and to increase trust amongst investors and consumers.

Several legal acts of the European Community address also issues relevant to network and information security. For instance, when the 1995 Data Protection Directive[75] was drafted, it recognized the importance of security measures for the protection of personal

---

74 Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency - OJ L 77, 13.3.2004, p. 1.

75 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data - OJ L 281, 23.11.1995, p. 31.

data. Article 17(1) introduces a legal obligation to ensure state-of-the-art-security of information systems and networks used to processing of personal data. Pursuant to this provision, the person or entity responsible for the processing must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be processed.

The Directive on electronic signatures[76] provides a legal framework for electronic signatures and other certification services. Its main objective is to create a Community framework for the use of electronic signatures, allowing the free flow of electronic signature goods and services cross-border, and ensuring a basic legal recognition of electronic signatures. All 25 Member States have now implemented the general principles of the Directive. However, the effective use of advanced or qualified electronic signatures has found a very slow take-up. On the other hand, many other electronic signature applications have become available that use the simpler form of electronic signature, mainly in relation to e-government and personal e-banking services. Nevertheless, the Directive introduced legal certainty with respect to the general admissibility of electronic signatures. It is expected that the need for secure electronic means of identification to access and use public services is essential for citizens and businesses and will promote the use of electronic signatures[77].

Network and information security provisions also form part of the regulatory framework for electronic communications.

In particular, Article 4 of the Directive on privacy and electronic communications[78] imposes on providers of publicly available electronic communications services an obligation to take appropriate technical and organisational measures to safeguard security of their services. Article 5 of the same Directive affirms the principle of confidentiality of communications and the related traffic data which must be ensured by national legislation[79]. In addition, Article 5(3) regulates issues like cookies, spyware and other technologies that might be deployed without appropriate user consent or implemented in ways that impair user control over their computers. Accessing any user's equipment like a PC or a mobile phone, or storing information on that equipment is only allowed if,

---

76 Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures - OJ L 13, 19.1.2000, p. 12.

77 See also the Ministerial Declaration approved in Manchester during the Ministerial e-Government Conference "Transforming Public Services", 24 November 2005.

78 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 - OJ L 201, 31.7.2002, p. 37.

79 In particular, listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data may only take place when legally authorised, for purposes including State security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences (see Articles 5 and 15 of Directive 2002/58/EC).

firstly, the user is given clear information about the purpose of any such activities and secondly, the user is offered the right to refuse it[80].

Article 13 of the Directive contains regulation of unsolicited commercial messages, which when transmitted by e-mail are often called "spam". It introduces the principle of consent-based marketing by electronic communications to natural persons (or opt-in) and complementary safeguards. The regime covers not only email but also fax, SMS, MMS, etc. In January 2004, the Commission presented a Communication identifying a series of actions to complement the Directive and make it as effective as possible. These include: effective enforcement by Member States, technical and self-regulatory solutions by industry, consumer awareness. International cooperation is another essential component of this policy, since most spam comes from outside the EU and European efforts much be echoed in other regions of the world.

The Commission has also set up a Contact Network of Spam Authorities (CNSA) that meets regularly and uses online facilities to exchange best practices and cooperate on enforcement across borders. The upcoming review of the regulatory framework for electronic communications should serve to determine whether any additional regulatory initiative is needed in this area.Moreover, Article 23 of the Universal Service Directive[81] covers the integrity of the public telephone network and its availability in the event of a catastrophic network breakdown or *force majeure*, as well as access to emergency services.

Misleading or aggressive spam activities are also banned under the provisions of the recent Directive on Unfair Commercial Practices[82] because it is misleading or deceptive (e.g. "scams"), or under the Framework Decision on illegal attacks against information systems.

Cooperation on the large amount of spam that breaches consumer protection law is also to be considerably enhanced by the implementation of the Regulation on Consumer Protection Cooperation[83]. This regulation creates a formal network of public authorities responsible for the protection of consumer economic interests and empowers and obliges them to stop traders that breach consumer protection laws, including through spam, in cross-border situations. The Regulation will also boost the ability to cooperate

---

80 In this context, it should be noted that ENISA has been requested to collect from Member States information on measures adopted by service providers to comply with the requirements bearing on providers of electronic communications services to implement technical and organisational measures to safeguard the security of their services (including measures to fight against spam, spyware and other forms of malware). The results of this survey are expected to provide a good overview of the current overall status of the implementation of existing legislation and indicate whether steps need to be taken to improve enforcement of European legislation at Member States level.

81 Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services - OJ L 108, 24.4.2002, p. 51.

82 Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market - OJ L 149, 11.6.2005.

83 Regulation (EC) No 2006/2004 of the European Parliament and of the Council of 27 October 2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws - OJ L 364, 9.12.2004.

internationally to stop spam that breaches consumer protection laws as it provides for international agreements on cooperation with third countries.

Trust and security take an important place in the European Community research and development activities. By way of example, in the first part of the 6th Framework Programme, 17 projects[84] (6 Integrated Projects, 3 Networks of Excellence, 6 Targeted Research Projects and 2 Coordination Actions) were launched with a total Community funding of about 75 M€ (and an overall budget of ~130 M€). These activities cover advanced and sophisticated research and provide strong links with policy developments in trust and security, i.e. in multimodal and secure biometrics; identity and privacy management; electronic authentication; secure digital assets management; virtualisation of security resources for advanced and seamless security. More recently, as a result of the IST Call 4, 19 new projects on security and dependability are under negotiation for an overall Community funding of about 70 M€ (and a total overall budget of ~115 M€). This set of new projects would strongly extend the technical coverage in this domain. It includes activities on the development of knowledge and technologies to manage and control complex and interdependent networks and systems, so as to enhance security and resilience in the Information Society infrastructure; provision of interoperable and open trusted computing platforms; advanced mechanisms and models for security, privacy and trust in mobile environments; and sophisticated technologies to fight malware on the Internet.

Crisis management actors belong to important users of security technologies. In order to address their needs, risk management R&D activities in the 6th Framework Programme are making an intensive use of advanced trust and security technologies. It is estimated that more than two third of the projects are addressing security issues. They cover the following fields of applications: Command, Control Coordination systems ("C3"), and public safety communications (which includes communication from and to the authorities early warning and alert systems and emergency telecommunications). This represents 5 integrated projects, 15 targeted research projects and one support action with a Community funding of about 60 M€ and an overall budget of 110 M€.

In addition, the European Commission is funding security-related research projects in the Preparatory Action for Security Research (2004-2006), and has planned more substantial activities in the area of security research within the 7th Research Framework Programme with a view to the establishment of a coherent European Security Research Programme (ESRP) starting in 2007.

Security-related activities carried out by the European Standardisation Organisations provide a good example of concerted international efforts. Further to the 2001 Communication[85] and the Council Resolution of 28 January 2002 "On a common approach and specific actions in the area of network and information security", CEN and ETSI collaborated on the production of a report that addresses standardisation activities and standardisation requirements with respect to network and information security. This report was approved both in CEN and in ETSI and was published as ETSI SR 002 298

---

84 The list of on-going projects with links to their web home pages is available on http://www.cordis.lu/ist/trust-security/projects.htm

85 COM(2001) 298.

v.1.1.1 (2003-12). Its content might be partly out of date due to the continuous evolution of the technology; however, it will be updated in the course of 2006. The ICT Standards Board[86] created in March 2004 the Network and Information Security Steering Group[87] to ensure appropriate coordination of the European standardisation activities in the security domain.

[86] ICTSB: http://www.ict.etsi.org/Home.htm
[87] NISSG: http://www.ict.etsi.org/NISSG_home.htm